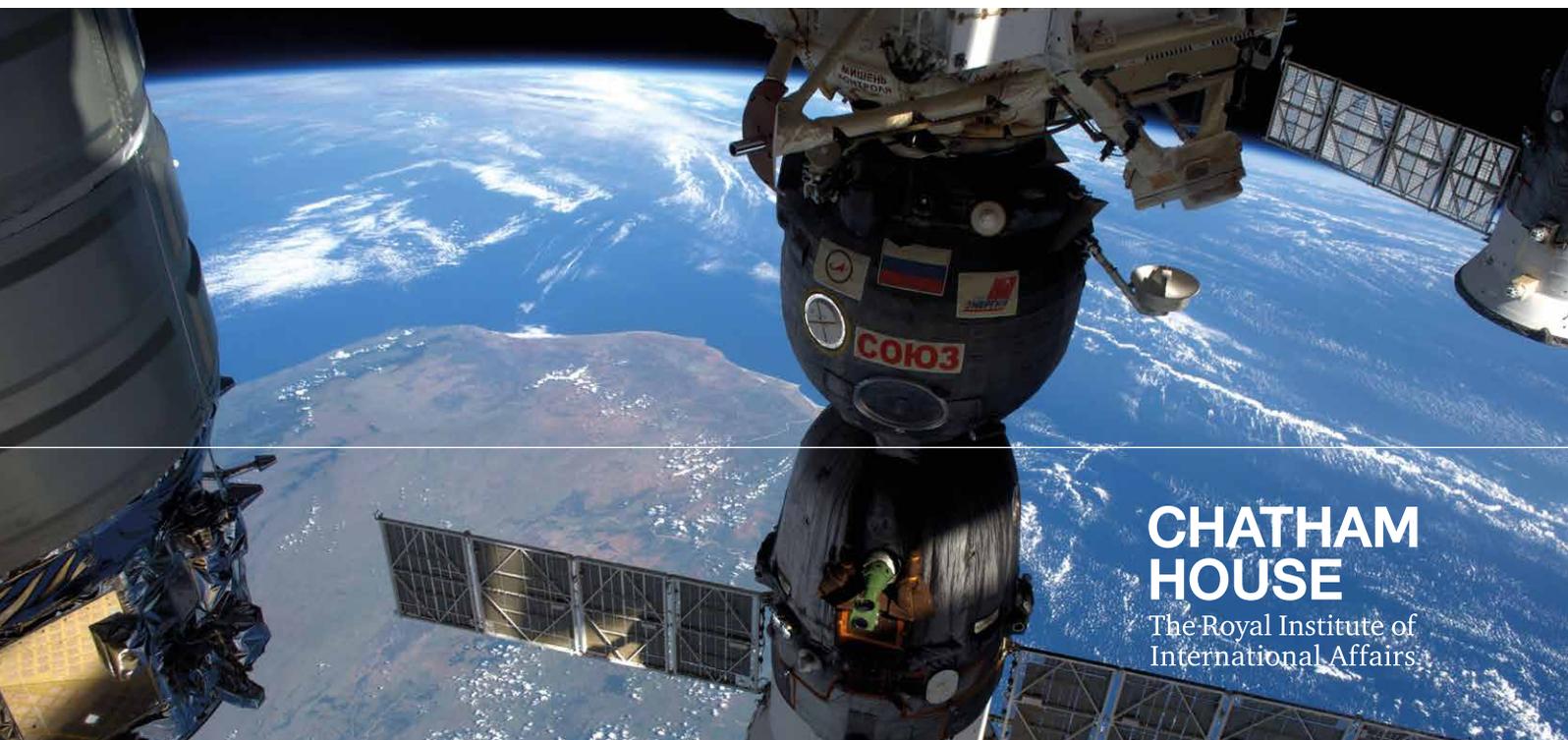


Research Paper

David Livingstone and Patricia Lewis

International Security Department | September 2016

Space, the Final Frontier for Cybersecurity?



**CHATHAM
HOUSE**
The Royal Institute of
International Affairs

Contents

	Summary	2
1	Introduction	3
2	Challenges	6
3	Threats, Risks and Trends	8
4	Technical Aspects of Cyberthreats to Satellites	16
5	Promoting International Cooperation and Other Policy Measures	24
6	Implementation of a Space Cybersecurity Regime	31
7	Conclusions and Recommendations	36
	Glossary of Terms	41
	About the Authors	43
	Acknowledgments	44

Summary

- Much of the world's critical infrastructure – such as communications, air transport, maritime trade, financial and other business services, weather and environmental monitoring and defence systems – depends on the space infrastructure, including satellites, ground stations and data links at national, regional and international levels.
- Satellites and other space assets, just like other parts of the digitized critical infrastructure, are vulnerable to cyberattack. Cyber vulnerabilities in space therefore pose serious risks for ground-based critical infrastructure, and insecurities in the space environment will hinder economic development and increase the risks to society.
- Cyberattacks on satellites can include jamming, spoofing and hacking attacks on communication networks; targeting control systems or mission packages; and attacks on the ground infrastructure such as satellite control centres. Possible cyberthreats against space-based systems include state-to-state and military actions; well-resourced organized criminal elements seeking financial gain; terrorist groups wishing to promote their causes, even up to the catastrophic level of cascading satellite collisions; and individual hackers who want to fanfare their skills.
- Space is changing from a selective preserve of wealthy states or well-resourced academia, into one in which market forces dominate. Current technologies bring space capability into the reach of states, international organizations, corporations and individuals that a decade ago had no realistic ambition in this regard; and capabilities possessed a few years ago only by government security agencies are now in the commercial domain.
- The pace at which technology evolves makes it hard, or even impossible, to devise a timely response to space cyberthreats. Humans too are affected by 'digital ageing' and legacy issues, and younger people use space-based and cyber communications in ways that make it difficult for older generations – and thus by implication some senior decision-makers – to fully understand the range of technologies and threats.
- Technology alone cannot provide the basis for policymaking on cybersecurity. Entirely or largely technological approaches do not have the breadth or depth to allow comprehensive participation, and would exclude many stakeholders who could otherwise contribute usefully to responses to the variety of threats propagated through the internet.
- Development of a flexible, multilateral space and cybersecurity regime is urgently required. International cooperation will be crucial, but highly regulated action led by government or similar institutions is likely to be too slow to enable an effective response to space-based cyberthreats. Instead, a lightly regulated approach developing industry-led standards, particularly on collaboration, risk assessment, knowledge exchange and innovation, will better promote agility and effective threat responses.
- An international 'community of the willing' – made up of able states and other critical stakeholders within the international space supply chain and insurance industry – is likely to provide the best opportunity to develop a space cybersecurity regime competent to match the range of threats.

1. Introduction

The vulnerability of satellites and other space assets to cyberattack is often overlooked in wider discussions of cyberthreats to critical national infrastructure. This is a significant failing, given society's substantial and ever increasing reliance on satellite technologies for navigation, communications, remote sensing, monitoring and the myriad associated applications. Vulnerabilities at the junction of space-based or space-derived capability with cybersecurity cause major national, regional and international security concerns,¹ yet are going unaddressed, apart from in some 'high end' space-based systems. Analysing the intersection between cyber and space security is essential to understanding this non-traditional, evolving security threat.

Cybersecurity and space security are inextricably linked. Technologies in satellites and other space assets are sourced from a broad international supply base and therefore require regular security upgrades. And the upgrades via remote connections could serve to make space assets vulnerable to cyberattacks.² In everyday life, satellites are regularly used to provide internet services and global navigation satellite system (GNSS) technologies which are increasingly embedded in almost all critical infrastructure.

Vulnerabilities at the junction of space-based or space-derived capability with cybersecurity cause major national, regional and international security concerns, yet are going unaddressed, apart from in some 'high end' space-based systems.

Because cyber-related technology is relatively new and is often multi-purpose and dual-use in nature, legislation lags behind. For example, two global utilities – the internet and GNSS – are driven by dual-use technology and are thus potentially deployable for military and civilian use. The United States, in particular, recognizes this and strives to cope with this challenge through its International Trafficking in Arms Regulations (ITAR).³ These utilities have a plethora of military and security applications, and are integral parts of critical national infrastructure. However, in the military context it is also hard to establish when they are used for defence or for offensive actions.

The United States has recently described the space environment as 'congested, contested and competed',⁴ and has developed a corresponding policy to 'deter, defend and defeat'. Russian defence policy states that the information domain is one of war,⁵ pointing to an urgent need for rules of engagement and rules of prevention and prohibition, which do not yet exist. Moreover, international cooperation can generate dependency risks, which could have a negative impact on national security interests; consequently, sound policy concepts do not readily translate into political will, and international rule-based solutions may be hard to develop.

¹ UK HM Government (2014), *National Space Security Policy*, UKSA/13/1292, p. 2, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/307346/National_Space_Security_Policy.pdf.

² *Ibid.*, p. 9.

³ FAS Space Policy Project (1997), 'International Traffic In Arms Regulations: Part 121 – United States Munitions List', <http://fas.org/spp/starwars/offdocs/itar/p121.htm#C-VIII>.

⁴ Schulte, Greg (2011), Deputy Assistant Secretary of Defense for Space Policy *Address to 27th National Space Symposium* and the Opening Keynote, Hosted Payload Summit, 4 October 2011, http://archive.defense.gov/home/features/2011/0111_nsss/docs/HostedPayloadsKeynote%20Schulte.pdf.

⁵ Geers, K. (ed.) (2015), *Cyber War in Perspective: Russian Aggression against Ukraine*, Tallinn: NATO CCD COE, p. 20.

For the insurance sector, the systemic risks are at once evident and potentially unquantifiable, as noted by one industry expert in 2014:

The challenge is that insurers have to contend with a new and potentially catastrophic class of risk, with limited historical loss data on the nature and severity of the threat. To some extent therefore it is a jump into an unknown world where criminal, business and political/strategic interests could be at play.⁶

Hackers, who represent the front end of the threat, currently constitute a major problem; their culture is entirely different from that of government or the military. Therefore, analysis of cyberattacks needs to take into account the fact that at a national level future attacks will be mostly generated by complex interests, from sources that are not immediately apparent to legitimate actors. To compound the problem, GNSS systems, which are now used by many stakeholders worldwide, are relatively insecure because until recently civil applications have not been designed with security in mind (although more modern systems such as the European ‘Galileo’ have secure technology).

In addition, the huge amount of data disseminated through satellites makes it possible for criminals to corrupt accuracy and reliability with a low probability of discovery. In particular, preventing spoofing (see section on technical aspects of cyberthreats to satellites, below) requires integrity checks in which large amounts of data are transferred between interested parties. In the maritime arena, space-based monitoring systems are regularly being jammed or spoofed by vessel operators entering false information in order to disguise their illicit activities. The need for integrity checks applies to many other aspects of the maritime domain such as distress calls, data and information. In principle, lack of integrity and availability can cause a great deal of damage to confidence in systems. However, proposed solutions are seen as expensive and are therefore unlikely to be adopted universally – unless there is a compelling reason such as legislation or a major incident, or new competition; in this context, perhaps the August 2016 launch of China’s ‘quantum satellite’, said to be ‘designed to establish ultra-secure quantum communications by transmitting uncrackable [i.e. hack-proof] keys from space to the ground’, will change the game.⁷

Project background

The International Security Department at Chatham House has undertaken a multi-year, multidisciplinary study of the intersection between cybersecurity and space security. In 2013–14, in partnership with Finmeccanica UK, it held a number of expert discussions and published a paper on the challenges.⁸ From 2015 Chatham House has partnered with the Sasakawa Peace Foundation to study the specific ways in which cyberattacks can be used to disable satellites and their functions, and the impact of such attacks on the military uses of satellites and international security.⁹ The project, on ‘Satellite Security – Vulnerability to Cyber Attack’, addresses:

- How cyberattacks can be used to destroy or impede the functions of satellites and other space assets, either by taking remote control of a satellite itself or by jamming its signals; and

⁶ Lloyd’s of London (2014), ‘The Space Industry Wakes Up to the Cyber Threat’, Q&A with Denis Bensoussan, Head of Space at Beazley, 7 July 2014, <https://www.lloyds.com/news-and-insight/news-and-features/market-news/industry-news-2014/the-space-industry-wakes-up-to-the-cyber-threat>.

⁷ Fernholz, T. (2016), ‘China’s new quantum satellite will try to teleport data outside the bounds of space and time’, Quartz, <http://qz.com/760804/chinas-new-quantum-satellite-will-try-to-teleport-data-outside-the-bounds-of-space-and-time-and-create-an-unbreakable-code/>.

⁸ Baylon, C. (2014), *Challenges at the Intersection of Cyber Security and Space Security: Country and International Institution Perspectives*, Research Paper, London: Royal Institute of International Affairs, https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20141229CyberSecuritySpaceSecurityBaylonFinal.pdf.

⁹ The Sasakawa Peace Foundation (2015), <https://www.spf.org/e/>.

- The way forward and potential solutions, including increased international cooperation requiring a blend of policy and technical inputs.

As part of the project, Chatham House held two expert roundtables in London, under the Chatham House Rule, in which over 30 participants from government, academia and the private sector participated, with the aim of fostering discussion on awareness of the mutual vulnerabilities of cyber and space assets, and potential policy solutions. In addition, in collaboration with the Synergia Foundation, Chatham House ran an expert high-level roundtable in Bangalore. The meeting was co-hosted with Toby Simons of Synergia Foundation,¹⁰ Bangalore, and co-chaired with Raji Rajagopalan of the Observer Research Foundation,¹¹ Delhi.

This paper identifies the key issues associated with the management of cybersecurity in the space supply chain across the world, and recommends appropriate actions to mitigate wide-ranging vulnerabilities in the space infrastructure.

¹⁰ Synergia Foundation (2016), <http://www.synergiafoundation.in>.

¹¹ Observer Research Foundation (2016), <http://www.orfonline.org>.

2. Challenges

Governments and global economic institutions are seeking to align the need to provide internet-based platforms for financial and business growth with the requirement for increased protection against an increasing number of sophisticated and well-resourced cyber-related threats from nation states, terrorist groups, organized criminal groups and individuals aiming to steal intellectual property, cash or sensitive personal data, or simply to cause damage.

Satellite services are potential targets for a range of cyberthreats, as space supports a growing and increasingly critical level of functionality within national infrastructure across the world, stimulating economic growth. One attack on a key node in the space sector could have the leveraged potential to affect critical national and international capabilities. This dependency on space is not unique to developed states; most countries will have similar vulnerabilities.

A recent Chatham House paper on space and cybersecurity points to the increasingly blurred line between ‘offensive’ and ‘defensive’ activities in cyber and space, given that, technologically, offence is easier and more cost-effective than defence.¹² More advanced countries are increasingly vulnerable to attack from less developed states, and from terrorist groups and other actors such as organized criminals. In addition, the technologies for the space sector are developed and sourced from all over the world; the space supply chain can therefore be considered a truly internationalized business environment that is not yet well regulated with cybersecurity in mind. While the overall approach of many governments to cybersecurity is becoming more effective, the paper warns that the conjunction of cyber and space remains vulnerable to exploitation in the context of complex and internationalized supply chains and space-related infrastructure.

Current responses

There is currently no coherent global organization with regard to cybersecurity in space. For example, the UK’s policy response appears to be confined to high-level and classified information-exchange groups comprising select, by-invitation-only entities that coordinate between civil and military agencies but which have only limited reach into the supply chain. This structure is generally replicated in other countries that are ‘space-enabled’, with few if any mechanisms for implementing cybersecurity controls down to the deepest levels.

This systemic challenge at the intersection of cyber and space security therefore requires a radical, innovative approach to build and maintain confidence in the use of the space domain. This in turn will catalyse growth in trade and the wider global economy, help reduce the costs of government, and support safe provision of cultural and recreational activity. The experience gained in resilient satellite communications (SATCOM) and navigation systems, and the development of smaller satellite technologies, mean that the international challenge at the intersection of space and cybersecurity could now be regarded as a strategic opportunity to enhance mission assurance for space assets. Although the value of the space cyber market-in-waiting still needs to be defined, it can be assumed to be large, with rewards accruing to early (and quick) market adopters on both the customer and the supply sides.

¹² Baylon (2014), *Challenges at the Intersection of Cyber Security and Space Security*.

New responses

Work is needed to systematically define and analyse each segment of a typical space mission and its supporting functions, and to develop mitigating strategies. Two cyber-related vulnerabilities of space missions are investigated in a later section of this paper: jamming and spoofing of satellite signals and associated data; and the remote takeover of satellite control through a cyberattack.

Development of a flexible international space and cybersecurity regime is urgently required; this arrangement should be managed initially by an international ‘community of the willing’ – a limited number of able states and other critical stakeholders within the international space supply chain and insurance industry. Such a regime would avoid the inevitable delays in agreement and implementation associated with any regulated, centralized and directive approach developed by an international body – the International Telecommunication Union (ITU) for example – that would give the advantage to attackers as latter are unencumbered by compliance with relatively time-consuming legislative controls. The new, agile regime would provide focus to rapid, active response mechanisms, and as a side benefit the body that coordinates and oversees it could also be tasked by the coalition to achieve market traction nationally and internationally for products and services related to cybersecurity in space. The regime could be implemented rapidly and cost-effectively, shifting risk-management activity to the less expensive and vital activities of education, training, exercises and providing situational awareness (understanding the status of people and systems) in the global space supply chain. Over time, the regime could be extended to a wider group of like-minded states.

The proposed regime would thus provide a vehicle for practical leadership in delivering enhanced security within the whole of the global space sector, upstream and downstream and at all levels of the supply chain. It would also act, *inter alia*, as an independent convener, providing oversight and guidance, and could undertake gap analyses for security processes, review concepts of operations and procedures, determine the roles of associate organizations, assist in insurance risk assessments, and secure funding for capability development projects. It would develop established and trusted connections with the space cyber community, including government agencies, academia and industrial concerns, as well as exploiting existing channels to provide access to commercial markets worldwide.

Initial work would include building on the structures already developed for national infrastructure, in particular the National CERTs (Computer Emergency Response Teams) – for example, in the UK, CERT-UK,¹³ the Cyber Essentials Scheme¹⁴ and the Cybersecurity Information Sharing Partnership (CISP); in Japan, JP-CERT and JP-CERTCC (Coordination Centre);¹⁵ in India, CERT-In;¹⁶ in Ghana, CERT-GH;¹⁷ and in the United States, US-CERT¹⁸ and the Comprehensive National Cybersecurity Initiative.¹⁹ Where possible, it would help, through ‘designing for security’, to resolve problems affecting satellites under construction. The regime would add further value by mitigating sector-specific concerns. This is particularly relevant within the current period of dramatic market-led change in the delivery of space-related goods and services and insurance.

¹³ CERT-UK (2016), ‘Useful documents and links’, <https://www.cert.gov.uk/resources/external-content/useful-links/>.

¹⁴ UK HM Government (2016), ‘Cyber essentials scheme: overview’, <https://www.gov.uk/government/publications/cyber-essentials-scheme-overview>.

¹⁵ Computer Emergency Response Team Coordination Centre Japan, <https://www.jpccert.or.jp/english/about/>.

¹⁶ Computer Emergency Response Team India (CERT-In) (2016), <http://www.cert-in.org.in>.

¹⁷ Computer Emergency Response Team Ghana (CERT-GH) (2016), <http://certgh-web.cert-gh.org>.

¹⁸ Computer Emergency Response Team US (US-CERT) (2016), <https://www.us-cert.gov>.

¹⁹ Executive Office of the President of the United States, ‘The Comprehensive National Cybersecurity Initiative’, <https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative>.

3. Threats, Risks and Trends

Cybersecurity threats and risks represent a systemic challenge to modern society. A system-level response is therefore the only viable approach, enabling the full set of agencies and organizations to work together in a synergistic and complementary manner. However, collectively harnessing the myriad national, regional and international agencies and organizations that characterize the space industry is not amenable to central organization and direction. What is required is a mutually agreed framework within which strategic and operational approaches can be networked so as to cross-fertilize information and foster an innovative, self-governing and accountable culture.

The intersection of space security and cybersecurity is not a new problem, but it has remained largely unrecognized as a potentially significant vulnerability. It thus remains unaddressed in practical mechanisms. This is despite the increasing dependence on the space-related goods and services to support modern communities as space becomes increasingly intrinsic to all elements of national and international infrastructure. Even outside the space domain, cybersecurity cultures across national and international communities are immature and inconsistent in their development.

The intersection of space security and cybersecurity is not a new problem, but it has remained largely unrecognized as a potentially significant vulnerability.

Although there is now a growing recognition of the problem, many national space security policies,²⁰ even those in countries where cybersecurity is more advanced, have been slow to identify the significant cyber risk to space-based assets. Moreover, very little is as yet being done to address cybersecurity at a system-of-systems level.²¹

The dialogue on cybersecurity in space cannot be confined to a broad but fragmented approach by individual states and international organizations, albeit each acting in good faith. National approaches in isolation will do little to mitigate harm already being experienced in space assets. So far, however, no international body has taken on the challenge, and so there is a gap in the international dialogue and plans for action. A lack of consistency in the internationalized domain addressing threat-response vulnerabilities has resulted in a failure to examine the range of risks. In common with other domains, such as the civil nuclear industry, the lack of documented or reported events in the space cyber domain leads to a false sense of security: little seems to be happening, little is likely to happen, and so what is the point in adopting any countermeasures? But the evidence suggests that imagining the risk to be small could be a fatal blunder.²²

²⁰ For example, in the UK Space Agency (2015), *National Space Policy*, p. 11, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/484865/NSP_-_Final.pdf; and in the UK HM Government (2015), *National Security Strategy and Strategic Defence and Security Review 2015*, p. 46, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf.

²¹ Note that at a recent meeting of the US House Permanent Select Intelligence Committee (HPSCI), Rep. Adam Schiff was reported to have said that a cyberattack on a US satellite could be considered an act of war; see Clark, C. (2016), 'Cyber Attack On Satellite Could Be Act Of War: HPSCI Ranking', *Breaking Defense*, 10 June 2016, <http://breakingdefense.com/2016/06/cyber-attack-on-satellite-could-be-act-of-war-hpsci-ranking/>.

²² See Baylon, C., Brunt, R. and Livingstone, D. (2015), *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*, Chatham House Report, London: Royal Institute of International Affairs, https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20151005CyberSecurityNuclearBaylonBruntLivingstoneUpdate.pdf.

Mapping the threats

Cyberthreats against space-based systems may be classified as follows:

- States setting out to create military advantages in space, or seeking to steal strategic quantities of intellectual property and having sufficient computing power to crack encryption codes, for example;
- Often well-resourced organized criminal elements seeking financial gain;
- Terrorist groups wishing to promote their causes, even up to the catastrophic level of satellite collisions with space debris including a cascade of collisions – called the Kessler Effect,²³ denying the use of space for all actors;
- Individual hackers who simply want to prove and fanfare their skills;
- Any combinations of the organizations and individuals above.

And their methods would be:²⁴

- Jamming, spoofing and hacking attacks on, for example, communication networks, by using space infrastructure;
- Attacks on satellites, by targeting their control systems or mission packages, perhaps taking control of the satellite to exploit its inherent capabilities, shut it down, alter its orbit (perhaps thereby ‘weaponizing’ it), or ‘cook’ or ‘grill’ its solar cells through deliberate exposure to damaging levels of highly ionizing radiation;
- Attacks on the ground infrastructure, such as satellite control centres, the associated networks and data centres, leading to potential global impacts (for example on weather forecasting systems, which use large quantities of space-derived data).

International cooperation will be crucial in any response to space-based cyberthreats, and is at the heart of current debates, for the following reasons:

- Large numbers of satellites orbit the Earth, traversing all territories, and their uplinks and downlinks are transmitted via ground stations from all around the world;
- These satellites are used worldwide, whether for communications, Earth observation or precise navigation and timing capabilities;
- Satellites are built with components from an internationalized supply chain.

Space is thus no longer a technological playground for the privileged few countries involved in sending humans to the moon, spying on others or putting communications leviathans into geostationary orbit.

For some states, there is still the simple allure of national prestige to be gained by entering the space race, with the successful launch of a sovereign vehicle being seen as a demonstration of technological achievement. More importantly, however, an ever increasing number of countries and private enterprises are commissioning satellites or buying timeshares in satellites for an

²³ Kessler, D. and Cour-Palais, B. (1978), ‘Collision Frequency of Artificial Satellites: The Creation of a Debris Belt’, *Journal of Geophysical Research*, 83(6): pp. 2637–646, <http://webpages.charter.net/dkessler/files/Collision%20Frequency.pdf>.

²⁴ Chatham House workshop roundtable, 16–17 July 2015, <https://www.chathamhouse.org/event/cyber-and-space-security-policy-solutions-technical-challenges>.

equivalent number of reasons; and market forces and technological advances are leading to lower-cost launches, smaller and more reliable satellites, and satellite constellations that can provide aggregated capability. As service providers become more aware of how space can be used, they are looking to satellites to deliver reliable, cheap and persistent capabilities that support commercial enterprises.

Factors such as these are now bringing space capability into the reach of states, international organizations, corporations and individuals that 10 years ago had no realistic ambition in this domain. The space market in both the upstream (the building of rockets and vehicles) and the downstream (goods and services enabled by space technology – i.e. the ‘applications’ market) is estimated to be worth £125 billion per annum today, and some £400 billion by 2030.²⁵ This suggests long-term double-digit growth. Entrepreneurship will create disruptive influences as the commercial opportunities provided by space become mainstream. Reductions in launch costs, miniaturization of payloads, standardization of data outputs and increases in capability are giving space mass market status, such that a wide variety of payloads can, and will, be put into orbit.

Space is thus developing from a domain for selective use by wealthy states or well-resourced academia, into one in which market forces dominate. Importantly, this will entail risk-management decisions on how much to spend on each mission’s security. Space-based offerings in the commercial domain now include capabilities possessed a few years ago only by government security agencies: Earth observation optical satellites seeing in 16 spectrum bands able to detect specific materials to a resolution of approximately 25 cm; radar satellites able to detect millimetric movements of buildings, terrain or vehicles; high-definition Earth observation CCTV, now being trialled in the International Space Station (ISS); commercial organizations rather than government agencies contracted to resupply the ISS, now using rockets that return to base and make a controlled soft landing.

To give some examples of the vulnerability of satellite systems, a draft report to the US Congress in 2011 recorded that at least two US environment-monitoring satellites had suffered interference four or more times in 2007 and 2008. A Landsat-7 Earth observation satellite built by NASA and managed by the US Geological Survey experienced 12 or more minutes of interference in October 2007 and July 2008. A NASA-managed Terra AM-1 Earth observation satellite suffered similar interference for two minutes or more on a single day in June 2008, and at least nine minutes on one day in October 2008.²⁶ The US National Oceanographic and Atmospheric Administration (NOAA) reported that its Satellite Data Information System was taken offline in September 2014 after a serious hacking incident; this denied high volumes of data to weather forecasting agencies around the world for 48 hours.²⁷

Figure 1 provides a general overview on future trends in space usage. This indicates that the global space-enabled economy is truly in a period of market-driven change.

²⁵ UK Space IGS (2013), *Space Innovation and Growth Strategy 2014–2030*, UK Space IGS, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/298362/igs-action-plan.pdf.

²⁶ Wolf, J. (2011), ‘UPDATE 1-China key suspect in US satellite hacks: commission’, Reuters, 28 October 2011, china-usa-satellite-idUSN1E79R1LK20111028; Wee, S.-L. (2011), ‘China denies it is behind hacking of U.S. satellites’, Reuters, 31 October 2011, <http://www.reuters.com/article/us-china-us-hacking-idUSTRE79U1YI20111031>.

²⁷ Livingstone, D. (2014), ‘The Intersection of Space and Cybersecurity is a Growing Concern’, Chatham House Expert Comment, 25 November 2014, <https://www.chathamhouse.org/expert/comment/16325>.

Figure 1: Satellite roadmap overview: Future trends in space usage, 2020–35

	2020	2035
 New Space		
Launchers	Rocket-based: semi-single use	Early tests for space planes, multiple air-launch solutions
	Microsat air-launch: up to 650 kg	Heavy air-launch: up to 6,000 kg
Nanosat constellations	Increasing constellations of various sizes	Targeted launch to bring low-capability microsats
	Larger constellations: up to 100s	Ubiquitous coverage and redundancy
COTS avionics technologies	Level-1 and -2 data product processing On-board reconfigurable computing and soft-core processor upgrades	RAD-Hard/MIL-SPEC computing processing capabilities equal to contemporary COTS
	Widespread use of MEMS for altitude control	System-on-a-chip avionics
Optics	Mechanized pointing	Aperture synthesis using nanosat constellations assemblies
	Miniaturized and compact optical arrays	Deployable structures to increase aperture
Micropropulsion	MEMS microthrusters	High-effort orbital manoeuvres
	Simple electric propulsion	High-effort orbital manoeuvres
 Satellite Communication		
Broadband	Performance: 2 MB/s	Performance: 200 MB/s
	Global capacity: 10 TB/s	Global capacity: 100 TB/s
Broadcast	100 million users, £50/month	1 billion users, £5/month
		Data-intensive media
Mobility	Enable users	Empower users
	1 million users, £200/month	1 billion users, £2/month
		Always connected
Network resilience services	Point-to-point link performance: n x 100 MB/s – microwave	Point-to-point link performance: 1 TB/s – optical
	Mobile backhaul: 10,000 nodes	Mobile backhaul: 1 million nodes
Internet of things and M2M	Internet of things	Autonomous system, self-optimizing
	1 million devices, £10/month	1 billion devices, £0.10/month
 Earth observation		
Resolution	0.25 metres	0.10 metres
	Several a day	Several an hour
Revisit time		GEO satellites and LEO constellations, HAPS and UAS
		Continuous surveillance
Processing method	Early on-board processing	Complex on-board satellite processing, e.g neurosynaptic chip
	Cloud computing, high-performance computing	New business models
Synthetic Aperture Radar	Ground-based InSAR capabilities	Near-real-time ability
		Multi-frequency
		Fully polarimetric
Spectral bands	16 spectral bands	50+ spectral bands high resolution

	2020	2035
 Position, Navigation and Timing		
Outdoor position accuracy with a mass-market device	1 metre	0.1–0.5 metres
Indoor position accuracy	0.5–2.5 metres	0.1–0.5 metres
Miniature atomic clock accuracy	Lose 2.5 picoseconds in 1 second	Lose 2.5 femtoseconds in 1 second
Time to first position fix for cm-level accuracy	15–300 seconds	1–20 seconds
Vulnerability protection on a mass-market device	Against multipath Against jamming	Against spoofing

Source: Satellite Applications Catapult, <https://sa.catapult.org.uk>.

To manage this appetite for space, the sector has to cater for increased demands in, for example:

- Satellite orbits that require deconfliction;
- Satellite constellations in which vehicles communicate with each other on an autonomous machine-to-machine basis;
- Data relay systems to reduce latency in delivering data;
- Satellite-based internet services involving a plethora of access points around the world;
- Supply chains of multinational corporations providing space-enabled goods and services, involving internationalization of the various tiers of suppliers.

The pace of change in space technology and the unregulated market forces that then demand development of space offerings are deepening to the extent that space is significantly interwoven with our daily life. In the near future, if it is not already the case, the space domain, including its ground elements, will be permanently embedded in the global infrastructure. This infrastructure, which accounts for trillions of data transactions every day, involving communications, precise navigation and timing, Earth observation (and the more niche space observation), means that space must now unavoidably be regarded as a constantly expanding and changing domain in which market applications are constantly developing at a pace that governments cannot control.

It is hard to map this change, even if segments or niches of space-related structure can be traced accurately. A chart of ‘how space works’ or ‘how space delivers’ can only be transiently accurate, a snapshot. Likewise, attempts at increased national-level regulation of the space sector to install structured approaches in the supply chain will bring resistance from powerful commercial organizations which constantly seek advantage through early adoption of quick-to-market offerings; regulation tends to be the antithesis of innovation and the exploitation of commercial opportunity.

Threat pathways

The threat pathways are hugely complex, but the main strands can be summarized as follows:

- Increasing numbers of individual satellites and constellations providing an ever-increasing number of entry points;
- Increasing connectedness through communications paths, and increasing connectedness of satellites while in orbit;
- Autonomous communications paths to billions of devices with little opportunity for humans to intervene;
- An international supply chain of satellite components, with the associated uncertainties about provenance and standards of production;
- The imperatives of speed to market, forcing designers and manufacturers to skip or pay only passing attention to important security controls;
- Security costs that are disproportionate to the costs of manufacture of smaller and cheaper satellites;
- Back-door holes in encryption and otherwise secure control systems.

But what are the likely consequences of cyberattacks on space infrastructure? There are many potential outcomes (suggesting that a response mechanism has to be flexible enough to cope with the unpredictable nature of attacks), but examples would include:²⁸

- Reduction in national security or defence capability;
- Reduction in capacity of communications, observation capability or navigation precision (perhaps through denial of service attacks);
- Corruption of communications, including precise timing systems, leading to lack of confidence;
- Denial of orbits following a contrived collision;
- Destruction of a space vehicle, or holding it to ransom;
- Destruction of a complete launcher and payload assembly, possibly during the launch phase, putting the uninvolved general public at risk;
- Corruption or deletion of data being transmitted from satellites;
- Interception of communications including sensitive intellectual property;
- Rerouting of communications to allow easier interception;
- Jamming of signals or spoofing of data (discussed in more detail below).

²⁸ Chatham House workshop roundtable, 16–17 July 2015, <https://www.chathamhouse.org/event/cyber-and-space-security-policy-solutions-technical-challenges>.

Mapping threats, assessing vulnerabilities

Discussion at the Chatham House expert roundtables concluded that traditional approaches in vulnerability assessment, with their origins in physical security methodologies, are no longer applicable to this problem. Space is changing from a domain where the development of technology, principally via academic research, was the determining factor, to one where market forces are driving an ever more rapid pace of change. For example, the market is increasingly hungry for bandwidth to satisfy the demand for internet-based services, for more precise timing and navigation systems to enable new capabilities such as autonomous vehicles, and for better provision of analysed data to provide better situational awareness of incidents on Earth and in outer space.

The life cycle of technology in satellites is completely different from that of most other technologies in the critical infrastructure. Many satellites – depending on their purpose, function and orbits – are designed to have very long lives. As a result, the technology installed in them and in some ground systems can become obsolete, creating serious legacy problems. The pace at which technology evolves makes it hard, or even impossible, to devise a timely response to space cyberthreats. Humans too are affected by different ‘digital ageing’ and legacy issues; younger people use space-based and cyber communications in ways that make it harder for older generations to understand the range of threats. But older people are often the senior decision-makers, and therefore need to understand the technologies far better than many currently do. This points to a need for ‘digital bridging’ between both human and hardware generations, in which both are updated and adapted to enhance system resilience.

Security is not simply created through agencies and operators; it is also achieved through coordination with manufacturers, software developers and operators. Numerous parties contribute to developing the integrated systems for typical satellite operations, and as with any complex technical architecture, the more parties are involved, the greater the vulnerability. Further problems arise as space becomes more cluttered. For example, there is a severe lack of available frequencies for space-based communications; orbit allocation is becoming increasingly problematic; and the amount of space junk is rising to critical levels.

Overall, the costs associated with cybersecurity – such as to guarantee the performance of each part of the various space missions – are high and rising. If the commoditized supply chain, constrained by the need to deliver profit to stakeholders, is not able to meet these costs, vulnerabilities will increase further. The problem becomes even more acute with low-cost space missions, where the commercial price of implementing cybersecurity measures rivals the value of the mission and makes little economic sense to the operator.

In addition, although standard-setting can reduce costs, in some cases standardization will serve to make some systems more prone to attack because the strength of the system is often only as good as the weakest point. Maximizing interoperability and efficiency could therefore inadvertently weaken the whole networked system by allowing threats to concentrate on the more vulnerable segments – most probably in the smaller and less expensive satellites where the cybersecurity components have been neglected on grounds of cost. Commercially attractive solutions are needed.

Secure encryption seems to be the most plausible response to cyberthreats to space assets, although it has its limits. Some security is better than no security – as long as the experts know what that security is capable of providing and what its limitations are. Part of the problem appears to be that neither the cyber community nor the space community understands the security requirements and vulnerabilities of each other’s domain. However, the cyber and space communities do not

just lack knowledge; they also need a wider understanding of the concept of security. The biggest limit to security might be the high costs that the different stakeholders are faced with; not all of them are prepared to spend a considerable amount of money to protect their systems.

Clearly there is a need to assess the level of vulnerability and manage the risk. How to ensure that introducing a solution does not inadvertently introduce a new, even worse problem is an important consideration. Solutions can never be a simple matter of technology but will always require a combination of different elements and approaches. The ‘market’ will not, for example, wait for long-winded security processes to be developed and imposed and for subsystems to be assessed for compliance. If such controls are imposed more rigorously in country A than country B, then systems integrators will simply switch allegiance from A to B. Thus the imposition of rigid controls to increase levels of cybersecurity assurance in the space market will be met with resistance on both the supply and the demand side, as such controls will be seen as impediments to innovation, market development and progress more generally.

Market trends

The market changes currently under way present problems in both analysis and delivery of solutions. Whereas a ‘technology push’ paradigm can force compliance with protocols such as ‘secure by design’, a ‘market-pull’ environment forces suppliers to speed up development and production in order to create competitive advantage. The temptation for these suppliers to cut corners in areas that are secondary to achieving the much desired early-adopter position, in which maximum financial returns are gained, becomes compelling; experience shows that those shortcuts are likely to include cybersecurity measures to a greater or lesser degree.

The controls required by a cybersecurity response to the threats that exist at the intersection of space and cyberspace are unlikely to cause problems where there is already a culture of regulatory compliance (such as in defence and intelligence). Elsewhere, however, where cash is king, the rules regarded as impediments to sales are much more likely to be circumvented; stakeholders will not become energized, cyber responses will become disjointed and allow plenty of opportunities for attack from those who wish either to jeopardize the space infrastructure or to use that infrastructure for destructive purposes.

The transition observed is truly towards the commoditization of space, a trend away from military and research, to one where ‘the market’ (in which there is a persistent need to innovate in a data-hungry world) holds sway. The pace of change can only quicken as launch systems become cheaper (through ‘low-cost access to space’ initiatives) and more reliable. In this unique environment, the world is on the cusp of a new dynamic in which the issue of cybersecurity has not even caught up with the old, just as a major change in market forces and corresponding supply chains is under way. What is becoming increasingly obvious is that there needs to be a radical review of cybersecurity in space. This more universal access now provides just such an opportunity for significant changes.

One of the key attributes of the new order must be an imperative to instil a *culture* of cybersecurity in the *commercial* supply chain that must be sympathetic to the fast-moving market and new technologies such as quantum computing, that allows (or even enables) innovation and that has a normative function. A lightly regulated framework should be selected as the default position, and the insurance industry could serve to create a level playing field and a set of incentives. Instead of the highly regulated and highly secure defence and intelligence segment driving policy, business interests would then become the principal driver of cybersecurity within the space sector.

4. Technical Aspects of Cyberthreats to Satellites

Jamming

Jamming is an attempt to degrade and disrupt connectivity by interfering with the signals that are the means for communication. It is normally associated with intentional interference in signal transmission and reception, and has been used for many decades by harnessing the deliberate use of radio noise and electromagnetic signals in an attempt to disrupt communications. A jamming device normally transmits electromagnetic energy in the same radio frequency bands as the desired transmitted signal, disrupting the ability of a receiver to accurately recover the transmitted signal. Simple jammers transmit ‘noise’ that takes no account of the signal or receiver characteristics and may be indiscriminate in action, while more sophisticated devices deploy techniques designed to take advantage of the properties of either the signal or the receiver, and can block specific types of networks on one or more frequencies simultaneously.

All wireless communication systems are susceptible to electromagnetic interference or jamming; the only consideration with regard to vulnerability is the degree of protection designed into the communication system to deal with particular interference or jamming scenarios. In the specific case of satellite services, signals can be jammed on the ‘downlink’ between satellites and receivers (termed ‘terrestrial’ jamming in this paper), or on the ‘uplink’ between transmitting ground stations and satellites (termed ‘orbital’ jamming here).

Terrestrial jamming affects the operating ability of receivers located in specific geographic regions, and is a well-known technique that has been used over many years by, for example, authoritarian governments attempting to prevent people from accessing unauthorized radio or television broadcasts. During periods of unrest and political control, radio and television reception has been blocked in several countries through electromagnetic terrestrial jamming for long periods of time, so that the governments maintained significant domestic controls over available information and mass communication. Terrestrial jamming of signals has also been used in more recent times to block access to mobile phone networks and the internet. This is sometimes called a wireless ‘denial-of-service’ attack and can take many forms.

Cases of mobile phone jammers have been documented with handheld units being able to block calls within a range of approximately 3 to 5 kilometres in urban areas. Higher-powered jammers, such as those used by military formations, can shut down service within a range of tens of kilometres.

Jammers may be inexpensive (some GNSS jammers can be bought on the internet for less than \$50) and are simple to use; they are also becoming smaller and easier to hide. The range of a jammer depends on its power, the atmospheric conditions, topography (for instance the level of reflective surfaces in the area), and the performance of receivers. In general, the jamming signal needs to be more powerful than the desired signal at the input to the receiver in order to

deny service or significantly degrade communications system performance. As an example, cases of mobile phone jammers have been documented with handheld units being able to block calls within a range of approximately 3 to 5 kilometres in urban areas. Higher-powered jammers, such as those used by military formations, can shut down service within a range of tens of kilometres. This is especially the case in rural areas, where terrestrial base stations are widely separated and where jamming power can be focused on very specific frequencies in order to avoid impact on 'friendly' frequencies while also achieving an advantage in terms of range.

Jammers of various types are readily obtainable through commercial sources. Sometimes they are used to block GSM connectivity in public spaces and thereby eliminate irritating mobile phone calls, but they can also be used for more malicious intent, denying access to communications to avoid alerting emergency services while another crime is being committed, for example. Other documented uses of jammers include the blocking of GNSS signals – thereby rendering ineffective surveillance techniques that are dependent upon reporting the position of a sensor. Terrestrial GNSS jammers have been known to interfere with emergency service response units' position reporting systems.

Orbital jamming interferes with the signal that is transmitted by a ground station towards a satellite. The jammer does not necessarily need to be in the vicinity of the transmitter, but could be located anywhere within the receiving beam of the satellite. (For certain types of satellite, this could be anywhere within the area on the Earth that the satellite covers – its 'footprint'.) The jamming signal degrades the quality of the wanted signal received at the satellite. For 'bent pipe'²⁹ satellites this results in the jamming signal being transmitted together with the wanted signal to overwhelm the terrestrial receivers, while for regenerative³⁰ satellites the jamming signal could result in failure of the satellite receiver to function correctly. The geographic extent of orbital jamming activity is not restricted to the physical location of the jammer, but instead affects the entire geographical region in which the satellite is intended to offer service.

In addition, depending on the nature of the jamming signal, there could be unintended collateral consequences if other signals being transmitted by the same satellite are also affected. For example, if a broadcaster for an Asian television channel is subject to an orbital jamming attack, then would-be viewers in North America are also unable to receive the broadcast signals. In addition, channels that are close in frequency may be affected if the bandwidth of the jammer is broader than absolutely necessary. For example, for several years, Iranian business entities, thought to be acting on behalf of the government, aimed signals of specific frequencies at the Telstar 12 satellite which was broadcasting Persian-language television from California. The jamming signals came initially from Cuba, and later (in 2005–06) from Bulgaria and Libya.³¹

Beyond physical cyberattacks

In recent years, it has become apparent that a new range of sophisticated methods is being developed, deploying cyber techniques to attack vulnerabilities in communications and navigation systems. Such vulnerabilities are particularly concerning, as they may not only be hard to detect and counter, but also have very significant consequences, ranging from wide-area denial of service

²⁹ In which uplink and downlink frequencies are different.

³⁰ In which satellites simply amplify and rebroadcast the incoming signal via a single frequency.

³¹ Small Media (2012), *Satellite Jamming in Iran: A War Over Airwaves*, London: Small Media, <https://smallmedia.org.uk/sites/default/files/Satellite%20Jamming.pdf>.

(equivalent to orbital jamming), to specifically targeted integrity failures (equivalent to spoofing), causing unsafe behaviour in satellite-based applications.

A significant fraction of all infrastructure requiring precise positional, navigation and timing (PNT) information to function effectively is becoming increasingly reliant on GNSS. In particular, the GNSS satellites contain very precise clocks and broadcast timing information to allow receivers to determine their location, and this timing signal is also used by a host of applications that are vital to day-to-day functions, such as the synchronization of terrestrial wireless and fixed communications networks. The signals from GNSS satellites operate over a narrow range of frequencies and are very weak at the input to a GNSS receiver, making them vulnerable to jamming attacks. Jamming attacks on the GNSS signals can degrade or (over time) deny mobile phone network service in a given geographical area.³² Over the past few years North Korea has conducted a series of coordinated jamming attacks that have affected GNSS signals in the Seoul area for up to a week at a time, leading to degradation of infrastructure, including mobile phone networks.³³

Public-service and military-grade GNSS receivers are less vulnerable to jamming as they use a range of techniques including:

- Receiving signals on multiple frequencies – for instance, military/civil global positioning system (GPS) and Galileo waveforms;
- Receiving signals from multiple GNSS systems – GPS/GLONASS/Galileo/BeiDou;
- Employing higher-specification receivers with more complex architecture;
- Deploying physical structures that mask signals received from terrestrial directions;
- Exploiting multiple receiving antennae and interference cancellation techniques.

Such techniques certainly improve the resilience of the GNSS receivers, but mission-critical systems must (and do) combine GNSS with other technologies such as inertial systems for positioning and local atomic clocks for timing, to mitigate the effects of any intermittent terrestrial jamming attacks.

Spoofing

Spoofing manipulates the information being exchanged in communications and hence reduces its integrity. Spoofing goes beyond jamming to distort or replace the wanted signal with a false signal. For spoofing to work, the receiver must continue to function correctly, and for a successful attack against a sophisticated receiver, the spoofing signals must both jam the wanted signal and be indistinguishable from it, containing *false* but *apparently true* information. A successful spoofing attack could potentially be used to target and directly damage critical infrastructure such as a national power grid by introducing erroneous timing signals, or cause indirect economic damage by, for instance, targeting high-frequency trading systems in the financial services sector.

One possible sophisticated attack scenario on a power grid might involve an attacker taking control of a wireless communications system and masquerading as a genuine controller, before creating a dangerous or destructive power surge by targeting distributed automatic power control systems devices that are used to accurately synchronize interconnected electrical grids. Potentially, this type of manipulation could trigger catastrophic overload currents, leading to cascading equipment

³² This occurs through the interruption of time division multiple access (TDMA) slots.

³³ BBC, North Korea 'jamming GPS signals' near South border, 1 April 2016 <http://www.bbc.com/news/world-asia-35940542>.

failures. Such events could trigger power grid blackouts over a sizeable geographic area, causing significant economic damage.

As with jamming, spoofing can be applied at both the receiver and the transmitter (satellite) end. In a dramatic demonstration in 2013, Dr Todd Humphreys, heading a team of scientists from the University of Texas, Austin,³⁴ used a lab-built device to broadcast counterfeit GPS signals that were slightly stronger than the real ones. Under controlled conditions, he took control of a luxury yacht's navigational system, resetting the vessel's satellite navigation system in a way that was not visible to the captain. The yacht's navigation system locked on to the fake signal, and the scientist hackers seduced the yacht's system to make it report that it was off course, although it was actually on the right track. The captain, not realizing that the GPS signal was incorrect, adjusted course so that the true track of the vessel was inaccurate by a few degrees. The implications of this form of attack, perhaps on a laden, very large crude carrier manoeuvring in confined waters, are only too clear.

Alternative attack scenarios might occur on banks and stock exchanges, with a conventional man-in-the-middle attack being employed to intercept and manipulate content to extract financial gain. A further sophisticated attack would not require the transmitted content to be manipulated, but would instead target GNSS timing functions in order to exploit the automated insertion of time-stamps on transactions for fraudulent purposes.

International incidents and awareness of vulnerabilities

In 1997 the prescient 20-person US President's Commission on Critical Infrastructure Protection stated that 'the most significant projected vulnerabilities are those associated with the modernization of the National Airspace System (NAS) and the plan to adopt the Global Positioning System (GPS) as the sole basis for radio-navigation in the US by 2010', and that 'exclusive reliance on GPS and its augmentations, combined with other complex interdependencies, raises the potential for "single point failure" and "cascading effects"'.³⁵ This analysis led to a thorough investigation of the threats and vulnerabilities associated with GPS deployment, and to Presidential Decision Directive (PDD) 63, Critical Infrastructure Protection,³⁶ which set out the roles, responsibilities and objectives associated with protecting US utility, transportation, financial and other critical infrastructure. PDD 63 focused on cooperation and intelligence-sharing within government agencies and with the private sector, and protecting individual sectors such as energy, banking and transport.

The GNSS networks currently available are the US GPS, Russia's Global Navigation Satellite System (GLONASS) and Europe's satellite-based augmentation system (SBAS), EGNOS and the new Galileo GNSS. China has developed a regional satellite navigation system, the BeiDou Navigation Satellite System (BDS), and is now developing a GNSS (BeiDou-2) with the aim of global operation by 2020. The seventh satellite in India's regional system NAVIC (Navigation Indian Constellation, formerly called IRNSS), IRNSS-1G, was launched in April 2016, and the system is set to become fully operational in the latter half of 2016. Japan is also developing a regional system, the Quazi-Zenith Satellite System (QZSS).

³⁴ Coutts, A. (2013), 'Want to see this \$80 million super yacht sink? With GPS spoofing, now you can!', Digital Trends, 30 July 2013, <http://www.digitaltrends.com/mobile/gps-spoofing/#ixzz429c2kQMH>.

³⁵ President's Commission on Critical Infrastructure Protection (1997), *Critical Foundations: Protecting America's Infrastructures*, http://permanent.access.gpo.gov/lps15260/PCCIP_Report.pdf.

³⁶ Presidential Decision Directive (NSC-63) (1998), *Critical Infrastructure Protection*, Washington, DC: The White House, <http://fas.org/irp/offdocs/pdd/pdd-63.htm>. The White House, Presidential Policy Directive (PPD -21) (2013), *Critical Infrastructure Security and Resilience*, Washington, DC: The White House Office of the Press Secretary, <https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>; Barack Obama, Executive Order (EO) (2013), *Improving Critical Infrastructure Cybersecurity*, Washington, DC: The White House Office of the Press Secretary, <https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.

One example of inadvertent mutual interference in GNSS systems occurred in early 2016 when 15 GPS satellites broadcast signals that were inaccurate by 13 microseconds, and telecom companies that are clients of the provider Chronos were hit by 12 hours of thousands of system errors. The GPS errors were also blamed for disturbances in BBC radio broadcasts.³⁷ The US Air Force, which manages the GPS satellite network, had earlier encountered problems in the GPS ground system software when decommissioning a satellite (SVN 23). This led to errors being transmitted to the GPS satellites, which negatively affected one signal from the satellite constellation, but the GPS core navigation messages and clock were not affected. The incident demonstrates several issues: that the software – as with all software – is vulnerable to error (or to a hack); that the 13-microsecond misstep had significant impact for several hours; that there is resilience in the GPS system, although infrastructure operators have apparently little knowledge of what to do in the event of a system degradation; and, more importantly, reversionary modes for infrastructure systems that rely on GNSS capability appear to be lacking.

Not all countries or government agencies have had the foresight or the resources to emulate the US in analysis of critical infrastructure vulnerabilities. However, until recently so much of the international system has been highly dependent on the US GPS. The advent of other GNSS satellite constellations helps to mitigate some of the risks, and is starting to raise awareness of the vulnerabilities beyond jamming and spoofing.

In these types of conventional electromagnetic attack, whether on communications systems or positioning systems, the jamming or spoofing device generally needs to be in the vicinity of the receiver, or in a position to intercept and manipulate communications between the transmitter and the receiver. The exception is orbital jammers, which, as noted above, need to be located within a satellite footprint but typically create disruption to communications services over a wide area. Organizations such as the Satellite Interference Reduction Group (IRG) coordinate the industry response to identifying, locating and responding to such attacks.

Military vulnerabilities

If left unattended, cyber vulnerabilities in the national and international critical infrastructure could be a conduit for attacks with highly dangerous consequences. Military technologies that provide situational awareness, observation and connectivity are increasingly dependent on cyber technologies. In the event of an escalation of an international crisis, cyber vulnerabilities could be exploited as part of diplomatic or military campaigns. Such attacks would increase the uncertainties in intelligence gathering and analysis and introduce uncertainties and delays in attributing actions and attacks to potential perpetrators, increase the risks of misperception, and thus further complicate decision-making at times of crisis.

Military strategic and tactical missile systems rely on satellites and the space infrastructure for navigation and targeting, command and control, operational monitoring and other functions. However, insufficient attention has been paid to the increasing vulnerability of space-based assets, ground stations, and associated command and control systems. Cyberattacks on satellites would undermine the integrity of strategic weapons systems, destabilize the deterrence relationships and obfuscate the originator of the attack without creating the debris problem that a physical

³⁷ Baraniuk, C. (2016), 'GPS error caused '12 hours of problems' for companies', BBC, 4 February 2016, <http://www.bbc.co.uk/news/technology-35491962>.

attack would cause. Because cyber technologies are within the grasp of most states (no matter how small or impoverished) and non-state actors, they level the strategic field and create hitherto unparalleled opportunities for small belligerent governments or terrorist groups to instigate high-impact attacks. As stated in the 2011 US International Strategy for Cyberspace, international approaches and cooperation are needed in order to address and mitigate the full range of cyberthreats to military systems.³⁸

Vulnerabilities in commercial satellite systems

In October 2014 a cyberattack on the US weather satellites system demonstrated the cyber vulnerabilities of strategic space-based assets.³⁹ While military satellites are generally well protected against such attacks (depending on their age, orbit and access), this is often not the case for commercial platforms, even though increasingly they are being used for military purposes. Both the complexity and availability of satellite technology are also growing through the development of small satellites in constellations – a trend that makes the space infrastructure even more vulnerable.

In general, complacency and misunderstandings about these vulnerabilities are widespread. A recent report by the US NOAA identified ‘significant security deficiencies’ in its own information systems, and a technical white paper from IOActive Labs provided what it asserted should serve as a ‘wake-up call for SATCOM security’.⁴⁰

There is a much higher potential for disruption than may be apparent from the direct mapping of cyber vulnerabilities to jamming (denial of service) and spoofing (malicious misdirection) scenarios. While electromagnetic attacks exploit physical vulnerabilities and may be characterized as ‘external’ to the systems under attack, cyberattacks that exploit non-physical vulnerabilities should be more closely characterized as ‘internal’ to such systems. Cyberattacks may have a deliberately delayed effect: latent threat vectors remain dormant within a system until activated at a critical juncture, when the level of damage they cause will be higher.

For a successful cyberattack to occur, the threat vector needs to be inserted within the system. This could take place during the manufacture, distribution or operation of the products and services that characterize the system. During the manufacturing and distribution phases, conventional physical security controls need to be applied to minimize the risk of cyberattacks. However, during operation, the conjunction of electromagnetic and cyber vulnerabilities becomes critical. As telecommunication systems integrate complex technology to improve performance, flexibility and efficiency, they are increasingly dependent on software that can be modified during operation rather than hardware or firmware that remains relatively unchanged once it has been designed and deployed. One example is the C-RAN (Cloud-Radio-Access-Network) concept being developed as part of the evolution of terrestrial mobile networks, and this type of software will be integrated into future satellite systems. Commercial tools such as SIM-toolkits are increasingly used to perform over-the-air provisioning and denial of service. Over-the-air software (both operating system and application) upgrades will be familiar to everyone using smart devices.

³⁸ The White House (2016), *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

³⁹ Flaherty, M., Samenow, J. and Rein, L. (2014), ‘Chinese hack U.S. weather systems, satellite network’, *Washington Post*, 12 November 2014, https://www.washingtonpost.com/local/chinese-hack-us-weather-systems-satellite-network/2014/11/12/bef1206a-68e9-11e4-b053-65cea7903f2e_story.html.

⁴⁰ Santamarta, R. (2014), *A Wake-Up Call for SATCOM Security*, IOActive Labs, http://www.ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf.

The ability to emulate a network, and to access, configure and control communications devices via wireless interfaces during normal operations also offers opportunities to an attacker to launch a large-scale cyberattack that remains latent within a system indefinitely, until activated at a time of the adversary's choosing.

There exists, therefore, a need to create infrastructure and procedures that allow full system vulnerability assessment to be undertaken and mitigation strategies to be developed, taking into account both electromagnetic and cyber techniques. Such facilities need to be available during the design, development and operational phases. As the internet has become near-ubiquitous, as devices become ever more interconnected and as critical infrastructure becomes more complex, vulnerability to cyberattacks is increasingly becoming the focus of network security, risk management, mitigation and resilience techniques. A multidisciplinary approach to vulnerability assessments and the design and implementation of mitigation strategies is required, while cybersecurity and wireless professionals alike require both greater awareness and sophisticated tools. Assuring the space-based capability must be the principal driver of the agenda. The industry needs to take stock of the GNSS vulnerabilities and develop pragmatic approaches to countering them,⁴¹ exploring and adapting new technologies, and building in redundancies.⁴² This will include ascertaining the prevalence of unintentional jamming and interference, and how jamming and spoofing play out in the realm of offensive state-initiated cyberattacks or may be used by terrorist groups.

Hijacking satellites to destroy or deactivate them

The technical challenges associated with cyberattacks that aim to take physical control of satellites, though great, are not insurmountable, and such a route may prove very attractive to attackers, who would most likely target industrial control systems (ICS), and specifically their vulnerable supervisory control and data acquisition (SCADA) systems. There are three components of SCADA systems: computers that control and monitor plant operations, and send signals that physically control the system; field devices such as programmable logic controllers, which control the sensors, motors and other physical components; and human-machine interface (HMI) computers, which display data on operations.⁴³ SCADA systems rarely have inbuilt cyber protection, and are vulnerable to a wide range of cyberthreats. Reports on the vulnerabilities of SCADA systems are well documented,⁴⁴ and states are actively developing the capabilities to be able take unauthorized remote control of satellites or other space-based assets with the purpose of destroying or deactivating them.

For example, it was reported in 2014 that Russian security researchers had found over 60,000 internet-connected exposed control systems with exploitable vulnerabilities that could allow malevolent actors to take 'full control of systems running energy, chemical and transportation systems'.⁴⁵

⁴¹ Spirent's GSS100D Detector, developed in collaboration with Nottingham Scientific Ltd, enables detection, characterization and analysis of real GNSS threats. GPS World staff (2015), 'New Spirent Test Framework Evaluates Threats to GPS', GPS World, 14 September 2015, <http://gpsworld.com/new-spirent-test-framework-evaluates-threats-to-gps-gnss/>.

⁴² For example, PNT that is independent of GNSS such as Long-Range Navigation (LORAN) systems. See <http://www.techweekeurope.co.uk/workspace/gps-jamming-elorlan-failover-109868>.

⁴³ Baylon, Brunt and Livingstone (2015), *Cyber Security at Civil Nuclear Facilities*.

⁴⁴ Zhu, B., Joseph, A. and Sastry, S. (2011), 'A Taxonomy of Cyber Attacks on SCADA Systems', published in the proceedings of the 2011 International Conference on the Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, http://bnrg.cs.berkeley.edu/~adj/publications/paper-files/ZhuJosephSastry_SCADA_Attack_Taxonomy_FinalV.pdf.

⁴⁵ Storm, D. (2014), 'Hackers exploit SCADA holes to take full control of critical infrastructure', Computer World, 15 January 2014, <http://www.computerworld.com/article/2475789/cybercrime-hacking/hackers-exploit-scada-holes-to-take-full-control-of-critical-infrastructure.html>.

The vulnerabilities of satellites to cyberattack include attacks that are aimed at ground stations. Most satellites launched in recent years rely on computers that are installed in the satellite themselves and that require regular upgrades through remote access. In addition, the technology is often off-the-shelf and, just as with all electronic devices, a ‘back door’ could be present in one of the many thousands of components in a single satellite, allowing cyberattackers hidden access. An attack could arrive via a ground station with the intent of causing a satellite to manoeuvre, ‘decaying’ or lowering its orbit so that it re-enters the Earth’s atmosphere and burns up. Even if there is no ‘back door’, current encryption is not always strong enough to deter determined, sophisticated attacks.

It is possible that a sophisticated attack could manoeuvre a satellite so that it collides with another satellite or space object. Alternatively, an attacker could activate all of the satellite’s solar panels, deliberately over-exposing them to highly energetic ionizing solar radiation causing irreparable damage.

States are actively developing these capabilities. As previously noted, two US government Earth observation satellites were hacked in 2007 and 2008.⁴⁶ The attackers gained entry into the system but stopped short of issuing commands. However, they are believed to have acquired ‘all steps necessary’ to do so. In March 2014 Russia accused Ukraine of attempting to decay the orbit of a Russian television satellite.⁴⁷ In the event of conflict, one country’s ability to disable or destroy one or more of another country’s satellites would give it a significant tactical advantage.

The dangers of cyberattacks that aim to take physical control of satellites have received far too little attention, even though such attacks would be of great global strategic importance. The main focus of concern has been the networks rather than the satellites. Consequently, experts and policymakers have not understood the full implications and the range of potential consequences of a satellite takeover.

Any satellite that can change orbit can be considered a space weapon. If the orbit changes so as to enter the pathway of another satellite then a collision will ensue, destroying one or both of the satellites and creating space debris that will continue to pose severe risks for other satellites far into the future. In addition, the more satellites there are, the greater the possibility of collision with debris, leading to a cascade effect known as the Kessler Effect, mentioned above, as the spatial density of debris increases.⁴⁸

For military satellites, the security of ground stations and their operations has been and continues to be addressed. The communications links are well secured, and physical infrastructure is well protected. Although commercial satellite operators are becoming more sensitive to the potential physical vulnerabilities of ground stations, in reality few people are required to actually manage these systems on a day-to-day basis. Ground stations – or satellite control centres – are highly automated systems, with very few operatives physically present at a control centre. However, the ability of commercial satellite operators to secure their datalink communications through automation is limited. Because of the way satellites orbit, a global network of ground stations is needed for fleets of satellites, and both uplinks and downlinks can be sent from a multiplicity of stations in many countries. This creates major confidentiality issues and difficulties in sharing system information with local partners. Nevertheless, despite these risks, the need to know and the need to share are fundamental to effective space security operations.

⁴⁶ US-China Economic and Security Review Commission (2011), *2011 Report to Congress of the U.S.-China Economic and Security Review Commission*, Washington, DC: US Government Printing Office, http://www.uscc.gov/sites/default/files/annual_reports/annual_report_full_11.pdf.

⁴⁷ Russia Today (2014), ‘Attempt to jam Russian satellites carried out from Western Ukraine’, 14 March 2014, <https://www.rt.com/news/ukraine-attacks-television-satellites-990/>.

⁴⁸ European Space Agency (2012), ‘The Kessler Effect and how to stop it’, 13 November 2012, http://m.esa.int/Our_Activities/Space_Engineering_Technology/The_Kessler_Effect_and_how_to_stop_it.

5. Promoting International Cooperation and Other Policy Measures

Principles of a space cybersecurity response

The response to a complex and specifically internationalized cybersecurity problem needs to be based on an international coherent approach, which can be defined as a regime – that is, a set of:

... implicit or explicit principles, norms, rules and decision-making procedures around which actors' expectations converge in a given area of international relations. Principles are beliefs of fact, causation and rectitude. Norms are standards of behaviour defined in terms of rights and obligations. Rules are specific prescriptions or proscriptions for action, decision-making procedures are prevailing practices for making and implementing collective choice.⁴⁹

There is an urgent requirement to develop a space cybersecurity regime that will inform and organize policy efforts and subordinate strategies, while remaining federally networked rather than controlled from a centre or hierarchically driven.

Too centralized an approach would give the illicit actors, who are generally unencumbered by process or legislative frameworks, an unassailable advantage simply because their response and decision-making time is more flexible and faster than that of their legitimate opponents. To be successful and durable, the space cybersecurity regime should be one that functions intelligently and responsively, and possesses enough flexibility to be able to react in a coordinated way as the environment and circumstances alter.

As noted above, over-zealous central direction by regulators in a market-driven sector tends to lead to the supply chain finding 'workarounds', leading to the risk of developing a general culture of cyber insecurity in which the default condition is simply to identify the best way to dodge the rules. This hands another advantage to the adversaries of legitimate users of the space domain.

However, the international space community has not yet acted as a coherent system in the area of cybersecurity. This problem is compounded by the fact that the nature of space and its relationship to society are entering a period of fundamental change. The stakeholders required for the space cybersecurity discourse remain essentially segregated (apart from occasional meetings at events such as conferences), and are only concerned with managing risks within their narrow fields of interest. Left unaddressed, this dynamic will in all likelihood continue unless there is an external stimulus. As a result, there will be little recognition that each stakeholder can be affected by another's security, or lack of it, unless there is a change in perceptions. A significant element of self-help is required to make up for the shortcomings of the regulatory cadre.

A space cyber regime, based on a lightly regulated initiative from the supply chain, seems to offer the most suitable and sustainable basis for channelling multinational contributions to an internationalized space cybersecurity capability which has to include an ever greater number of different stakeholders.

⁴⁹ Cornish, P., Hughes, R. and Livingstone, D. (2009), *Cyberspace and the National Security of the United Kingdom: Threats and Responses*, Chatham House Report, London: Royal Institute of International Affairs, <https://www.chathamhouse.org/publications/papers/view/109020#sthash.DZAeWwRY.dpuf>.

Such a regime must be agile enough to meet the rapidly evolving security challenge facing the space domain, and to continue to develop as the market is transformed over the next decades.

Policy requirements

Ideally, the policy needed to establish a space cybersecurity regime would align the needs of all the various concerns: on an already complex international stage this would include the millions of end users, individual scientists, the corporate sector and the military; address technical, political, economic and social interests; and combine the tactical with the strategic and the bottom-up with the top-down approach.

To align across and within all sectors, one approach is to adopt a single focus – such as the provision of assured broadband via space – and make that the driving force, organizing all other initiatives around it. But the space domain is now becoming so intrinsic to every human activity, whether government, private-sector or individual, that the foundation of a more robust and coherent space cybersecurity regime requires a common understanding of what is essential to determine both the nature of the problem and threat mitigation responses. The approach must be non-hierarchical, where each stakeholder is empowered by knowledge provided by the regime and feels valued as a contributor.

Ensuring security in space must correspondingly be a common ambition for all concerned players. Thus a common approach to cybersecurity can be developed and encouraged by applying the principles of governance, management and inclusiveness as outlined below.

Governance

There are three paramount dimensions in the governance of a space cybersecurity regime. First, whatever is done to combat space cyber *in*security, policy should be adopted and applied in order to *enable* legitimate users of space-related capability, while increasing the costs (of entry, for example, or discovery and being subject to law enforcement action) for illegitimate users.

A culture of space cybersecurity must lead to the development of an innate instinct for what is safe and what is risky throughout the supply chain.

Second, the governance of space cybersecurity needs a collective approach, involving as many legitimate stakeholders as possible and practical. This will also create a progressive and dynamic environment where knowledge is a key ingredient; if participants can share experiences and lessons learned, cybersecurity will become increasingly instinctive, from the boardroom down to the shop floor, and its sum will increase.

Third, the regime needs to be based on a self-governing and lightly regulated effort by a wide range of legitimate users of space capability. This is because space infrastructure, with its multiple uses, is a complex and constantly adapting area that defies control, centralized management and oversight by any single stakeholder (except for some very specific processes such as orbit or communications frequency allocation). Experience suggests that there is no other option but to deliver this effort within a business environment of transparency and accountability involving collaboration designed to share knowledge. Effective and durable governance of cyberspace requires a shared

awareness that implies a dynamic, common approach to raising cyber capability. A culture of space cybersecurity must lead to the development of an innate instinct for what is safe and what is risky throughout the supply chain.

Management

To achieve absolute, perfect cybersecurity in space and its associated infrastructure and uncountable plethora of applications would require all threats and vulnerable components in an ever-expanding and unmappable ecosystem to be identified and isolated, and certain actions performed to counteract attacks before they develop into harmful events. But to do so – even if it were possible – would be to contradict the concept of ‘new space’ as a business-led, technology-supported global commons; and it would constrain the functioning and development of a worldwide ‘republic’ of communications and data gathering and exchange, and a platform for global economic development.

The requirement is rather to *manage* rather than try to *eliminate* threats and risks that reside in cyberspace, or those that use cyberspace as an attack pathway. Furthermore, rather than hoping to be able to prevent every imaginable cybersecurity threat and attack, a more practical approach must be to create a cybersecurity regime that is centred on security-by-design and *pre-emptive* risk mitigation controls with the flexibility and resilience to handle emergencies as they develop.

Much as in any other environment, risk management in this context of space-related infrastructure is a process of identifying critical vulnerabilities and potential threats or harms, and working out what the likely outcomes would be if an attack were to occur, couched in terms of likelihood relative to impact. The art of risk management is to reduce risk intelligently to an acceptable level by mitigating, excluding, transferring or accepting it, and by doing so to improve the prospects for continued functioning of the capability concerned. Risk management is necessarily an iterative process, and not a ‘tick-box’ exercise.

Risks and countermeasures need to be continually re-evaluated as new factors emerge, priorities and vulnerabilities change and threats proliferate. Additionally, a balance between the cost-effectiveness of a given countermeasure and the value of the capability being protected must be taken into consideration. Furthermore, in complex networks and complex adaptive systems, the risk-versus-reward evaluations by one actor could be very different to those imagined by others – particularly in conflicts of interest between government regulators and commercial organizations which focus on more immediate financial targets.

Bringing these strands together, cybersecurity in the space sector is a matter of risk management on a very large scale, in which monitoring all stakeholders for their approach to cyber risk would be impossible, but there would be confidence that at the very least the whole community was well informed on the implementation of good practices.

Inclusiveness

It may be tempting to shy away from addressing cybersecurity in the current space infrastructure as too complex, too technically sophisticated and too rapidly changing a problem for the diverse set of analysts, users and policymakers. The complexity of corresponding countermeasures could also promote a narrow technical approach, thereby excluding the many system users who could otherwise have made useful intellectual contributions to the cybersecurity discourse.

This tendency to default to a simply technical standpoint has not served cybersecurity well in the past, and should be avoided in any future regime in which technical safeguards and countermeasures will only be part of the overall response. The Chatham House expert roundtables observed that as the space sector evolves, so the threats and challenges that emanate from it will evolve correspondingly.

It is vital to include technical experts in the development and implementation of any regime so that the shifts in space and cyberspace, new technologies and the nature of threats and challenges to society are fully understood and anticipated. The technical community is most likely to envisage potential developments in space-based capabilities. If it can be integrated into space cybersecurity policy development, then everyone involved should achieve a deeper comprehension of the range of likely future technologies and uses of space and of the likely threats and challenges. Furthermore, if for their part technical specialists can develop a better feeling for the requirements and constraints of cybersecurity, space technology might be steered in more benign directions, starting with the component design stage. Simply put, technical experts are best placed to undertake horizon-scanning, to be able to provide the longest possible warnings of new threats, along with the relevant technical solutions. But the organizational aspects of how new controls are to be applied will remain a matter for the non-technical stakeholders in the regime.

Types of regime behaviour

The first step towards a common conception of cybersecurity in space requires agreement on a set of principles – discussed above – by which strategy can be guided and risk assessed. Policy coherence at the strategic level may nevertheless be undermined by inconsistencies in implementation. Furthermore, there must be acknowledgment that a regime will be both driven and accessed by a large and diverse range of stakeholders including individual users, ad hoc communities, the private sector, the public sector, the insurance industry, the national security community and technical experts. And illicit actors will also make their presence felt.

Three key additional principles and types of behaviour for operations and implementation can be identified: agility and initiative, actor neutrality and risk management.

Agility and initiative

Cyberthreats are broad and mutate quickly, so a static, defensive stance by a space cybersecurity regime will result in two things. First, agile, intelligent and well-resourced cyber adversaries are likely to win. They will have the initiative in the contest, and will not have had to invest significantly to gain that initiative – an unaware and ill-prepared user will have surrendered that initiative by default. Second, the defences to cyberthreats are generally more reactive than anticipatory and they are rarely pre-emptive, so the majority of legitimate non-aggressive users of the space domain will only begin to address cyberthreats at the point at which they are fully formed and causing real impacts. Cybersecurity policy must therefore build in agility and focus on gaining and maintaining the initiative. This can only be done by matching or bettering the ‘battle rhythm’ of the adversary.

Actor neutrality

An ‘actor-neutral’ approach to cybersecurity in the space sector can help to ensure that energy and resources are applied promptly and efficiently, and where they can be of most benefit in responses to the threats. That is to say, with a diverse and evolving set of adversaries, not only are there difficulties in attribution, but knowing the identities and ambitions of adversaries is less important than knowing their capabilities and the potential for damage. It follows that it is necessary to have the policies, procedures and equipment in place to meet or anticipate the challenges and attacks, whatever their source and whenever they proceed. Definitions of cybersecurity that correspond to the roles and interests of individual departments of government or private-sector concerns are not as useful as developing a coherent and collective approach to the management of the problem – that is, through the regime approach that seems so far to provide the most appropriate response. A more inclusive response to cybersecurity challenges could be developed by focusing more on those elements of the risk equation – vulnerability and impact within a culture of risk management – that society can do most to mitigate within its own means, and less on the identity of the adversary.

Risk management

As noted above, it is unrealistic to expect to be able to eliminate all cyberthreats in the space sector in the foreseeable future. They are wide-ranging and rapidly changing, and it is impractical to imagine that all criminal or hostile use of the global information and communications technology (ICT) infrastructure, of which space is a major part, can be filtered out, given the widespread and absolute dependence on ICT in the modern world and the increasing role that space plays in delivering ICT-type services. Space technology has created a global common good: the barriers to entry are low, and inexpensive access to space capability has begun to take hold on global markets. Dependence cannot be eliminated in the near term; and neither, consequently, can exposure and vulnerability to cyberthreats. If threats, dependency and vulnerability cannot be excluded, they have to be managed. A risk-management approach to cybersecurity in space would:

- Ensure that participants understand that legitimate uses of space-based systems cannot be assumed to be free of threats and adverse consequences;
- Assess cybersecurity on the basis of cost-effectiveness and proportionality: potential benefits can be weighed against appropriate costs and penalties, including insurance premiums, and benefits can be prioritized and procurement systems put in place;
- Build in adaptability and agility so that as cybersecurity threats change, priorities can be recast;
- Frame space cybersecurity policies at a system level, offsetting the dangers and risks in one sector by advantages and benefits in another.

Emerging policy approaches

Clearly, numerous issues need to be addressed as the space supply chain sets out for the first time to reduce vulnerabilities in the domain. As it does so, some compelling themes emerge.

The first point that must be accepted is that space cybersecurity policy can and should be extended beyond its traditional position, which focused on the protection of critical national infrastructure and a ‘bottom-up’, reactive sectoral concern with computer and network security, information

security and assurance. Those policies, which have been implemented in the past two decades as unitary solutions to cybersecurity more generally, have been shown to fail, one after another. But a bottom-up approach does retain value as it includes the activities that contribute to compliance with various ISO standards. It is also the best place to elicit a response when national or international law enforcement agencies are brought into action; there are generally robust links between the two that can be exploited, either from national levels upwards or conversely down into the national agencies from an international coordinating function.

But a space cyber regime has to reach beyond a tick-box mentality that provides comfort yet still allows well-informed adversaries to take up threatening positions against users who remain rooted in a static regulated environment, believing they have done the right thing and risks have been satisfactorily mitigated. In such a fast-evolving domain as space, and reflecting a regime approach that encourages actions to counteract developing threats, it is essential for people, processes and technological issues to be amplified through better *organization*, better management of *business change* (i.e. agility) and also (because space vehicles are not generally recoverable for upgrading), constant *obsolescence management*.

Thus the space cyber regime doctrine needs to incorporate:

- People and organization;
- Processes and business change;
- Technology and obsolescence management.

Second, cybersecurity policy should be based on an agreed set of operational and strategic principles, with the following objectives: to turn the intersection of space and cyberspace from a permissive, ungoverned environment into a self-governing network; to raise the costs of use by illicit actors; to encourage a comprehensive and inclusive understanding of cybersecurity across the user community; and to facilitate and assure legitimate use of the ICT infrastructure supported by space technologies.

Moving from theory to practice, an active strategy for space cybersecurity should incorporate agile organization, coherent planning and deconfliction, creativity and responsiveness.

Reduction of supply chain risk: the task ahead

In a 2006 paper setting out proposals for best practices for the protection of commercial satellite communications infrastructure,⁵⁰ Richard Buenneke et al. suggested a series of principles aimed at guiding commercial satellite service providers that wished to develop increased resilience and that had also had responsibilities in the US strategy of network-centric warfare. The authors recognized that commercial satellite systems were playing an ‘increasingly important role in supporting US and coalition concepts for network-centric warfare’ and similar military strategies. They noted that this dependency also ‘increases the possibility of a hostile attack on privately owned and operated SATCOM networks’ working within that military ecosystem to provide additional and spare capacity.

⁵⁰ Buenneke, R., Abramson, R., Shearer, T. and McArthur P. (2006), ‘Best Practices for Protection of Commercial Satellite Communications Infrastructure’, AIAA 2006-5386, paper presented at 24th AIAA International Communications Satellite Systems Conference, San Diego, California, 11–14 June 2006, <http://arc.aiaa.org/doi/10.2514/6.2006-5386>.

To address these potential threats, in 2006 the then US National Security, Space Management and Organization conducted a comprehensive survey of approaches used by commercial operators and integrators to protect SATCOM networks against electronic, physical and cyberattacks. The survey identified a set of seven ‘best practices’ for information sharing and analysis, as well as responses to intentional jamming, physical attacks, cyber/network threats and other hazards.⁵¹ These best practices, Buenneke et al. suggest, should ‘form the basis for new incentives in US Department of Defense contracts for commercial SATCOM services’. As a starting position, these practices can also serve as the ‘basis for improved public-private and coalition collaborations for preparing and responding to a full spectrum of hazards’, not necessarily just from cyber adversaries, but also from natural events such as coronal mass ejections and other phenomena found in ‘space weather’.

Further development by the UK Space Agency⁵² and others has increased the number of best-practice strands to 10. These functions could form the basis of the proposed space cyber regime, as follows:

1. Raising awareness;
2. Encouraging vigilance;
3. Identifying dependencies;
4. Recognizing vulnerabilities;
5. Building in resilience and measured responses;
6. Future-proofing hardware and software;
7. Drawing up procurement strategies;
8. Identifying regulatory requirements;
9. Sharing experience, including military and civilian knowledge exchange;
10. Establishing best and good practices.

⁵¹ Ibid.

⁵² UK Space Agency (2015), *National Space Policy*.

6. Implementation of a Space Cybersecurity Regime

An international response is required to the cybersecurity challenges of space, but there are no relevant international organizations or agreed mechanisms that could conceivably constitute the basis for that response. A framework needs to be developed quickly to harmonize the space supply chain and its offerings, which are now being market-led. However, government-to-government dialogue in international security matters works slowly, particularly through UN and ITU structures, as does the academic discourse. In the international structures, there are a number of frameworks and international agreements for addressing international peace and security in space, including the Committee on the Peaceful Uses of Outer Space (COPUOS); the UN Office for Outer Space Affairs; the Disarmament Commission; the Conference on Disarmament and the UN Office of Disarmament Affairs; the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (the Outer Space Treaty); the Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space; the Convention on International Liability for Damage Caused by Space Objects; the Convention on Registration of Objects Launched into Outer Space; the Constitution and the Convention of the International Telecommunication Union and its Radio Regulations (amended).

An international response is required to the cybersecurity challenges of space, but there are no relevant international organizations or agreed mechanisms that could conceivably constitute the basis for that response. A framework needs to be developed quickly to harmonize the space supply chain and its offerings, which are now being market-led.

Recent progress has been made in the Wassenaar Arrangement⁵³ and two UN processes: the Group of Governmental Experts on Transparency and Confidence-building Measures in Outer Space Activities (GGE-Space);⁵⁴ and the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE-Cyber). In addition, space and cyber guidelines are currently being discussed within COPUOS,⁵⁵ including, for example, Guideline 9 (formerly guideline 43) to ‘implement policy aimed at precluding interference with the operation of foreign space objects through unauthorized access to their on-board hardware and software’ and Guideline 18 (formerly guideline 35) to ‘ensure the safety and security of terrestrial infrastructure that supports the operation of orbital systems and respect the security of foreign space-related terrestrial and information infrastructures’.

⁵³ The Wassenaar Arrangement (2015), *Summary of Changes: List of Dual-Use Goods & Technologies and Munitions List as of 3 December 2015*, <http://www.wassenaar.org/wp-content/uploads/2015/06/Summary-of-Changes-to-2015-Lists.pdf>.

⁵⁴ United Nations Office for Disarmament Affairs (2016), ‘Outer Space’, <https://www.un.org/disarmament/topics/outerspace/>.

⁵⁵ Committee on the Peaceful Uses of Outer Space (2016), *Updated set of draft guidelines for the long-term sustainability of outer space activities*, A/AC.105/L.301, United Nations General Assembly, http://www.unoosa.org/res/oosadoc/data/documents/2016/aac_105l/aac_105l_301_0.html/AC105_L301E.pdf.

Box 1: UN Group of Governmental Experts on Transparency and Confidence-building Measures in Outer Space Activities (GGE-Space)

The 2013 report from GGE-Space⁵⁶ agreed on a set of substantive transparency and confidence-building measures (TCBMs) for outer space, conclusions and recommendations. The main points were as follows:

1. Categories of transparency and confidence-building measures for outer space activities:

- (a) General transparency and confidence-building measures aimed at enhancing the availability of information on the space policy of States involved in outer space activities;
- (b) Information exchange about development programmes for new space systems, as well as information about operational space-based systems providing widely used services such as meteorological observations or global positioning, navigation and timing;
- (c) The articulation of a State's principles and goals relating to their exploration and use of outer space for peaceful purposes;
- (d) Specific information-exchange measures aimed at expanding the availability of information on objects in outer space and their general function, particularly those objects in Earth orbits;
- (e) Measures related to establishing norms of behaviour for promoting spaceflight safety such as launch notifications and consultations that aim at avoiding potentially harmful interference, limiting orbital debris and minimizing the risk of collisions with other space objects;
- (f) International cooperation measures in outer space activities, including measures aimed at promoting capacity-building and disseminating data for sustainable economic and social development, that are consistent with existing international commitments and obligations.

2. Specific TCBMs that include the following that could be used in enhancing the cybersecurity of space:

- Exchanges of information on the principles and goals of a State's outer space policy;
- Exchanges of information on major military outer space expenditure and other national security space activities;
- Exchanges of information on orbital parameters of outer space objects and potential orbital conjunctions;
- Notifications in the case of emergency situations;
- Demonstrations of rocket and space technologies;
- International cooperation and coordination;
- Consultative mechanisms, including for preventing or minimizing potential risks of physical damage or harmful interference.

3. Conclusions and recommendations:

- Universal participation in, implementation of and full adherence to the existing legal framework relating to outer space activities including the:
 - Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies;
 - Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space;
 - Convention on International Liability for Damage Caused by Space Objects;
 - Convention on Registration of Objects Launched into Outer Space;
 - Constitution and the Convention of the International Telecommunication Union and its Radio Regulations, as amended;
 - Convention of the World Meteorological Organization, as amended;
 - Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space and Under Water;
 - Comprehensive Nuclear-Test-Ban Treaty.

⁵⁶ United Nations Office for Disarmament Affairs (UNODA) (2016), 'Outer Space', <https://www.un.org/disarmament/topics/outerspace/>.

- Endorsing efforts to pursue political commitments such as unilateral declarations, bilateral commitments or a multilateral code of conduct, to encourage responsible actions in, and the peaceful use of, outer space.
- Proposing that voluntary political measures be a basis for concepts and proposals for legally binding obligations.
- Implementing transparency and confidence-building measures to the greatest extent practicable and in a manner that is consistent with states' national interests. As specific unilateral, bilateral, regional and multilateral transparency and confidence-building measures are agreed to, states should regularly review the implementation of the measures and discuss potential additional ones that may be necessary, including those necessitated owing to advances in the development of space technologies and in their application.
- Adhering fully to the existing legal framework relating to outer space activities and the principles and guidelines endorsed on the basis of consensus by the Committee on the Peaceful Uses of Outer Space and the General Assembly and other internationally recognized space-related principles.

Box 2: UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE-Cyber)

The 2014–15 GGE-Cyber⁵⁷ noted that common understandings on how international law applies to state use of ICTs are important for promoting an open, secure, stable, accessible and peaceful ICT environment, and put forward a set of views on how international law applies to the use of ICTs that include:

- State jurisdiction over the ICT infrastructure located within territory;
- Existing obligations and principles of international law to respect and protect human rights and fundamental freedoms, the principles of humanity, necessity, proportionality and distinction, state sovereignty, sovereign equality, the settlement of disputes by peaceful means and non-intervention in the internal affairs of other states and the inherent right of states to take measures consistent with international law and as recognized in the UN Charter;
- The requirement that states must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-state actors to commit such acts, noting that the accusations should be substantiated.

The GGE-Cyber addressed the critical infrastructure, of which the satellite networks form a vital part. This included taking appropriate measures to protect to critical infrastructure from ICT threats; the creation of a global culture of cybersecurity and the protection of critical information infrastructures; responses by states to requests for assistance when critical infrastructure is subject to malicious ICT acts; responses by states to requests to mitigate malicious ICT activity aimed at the critical infrastructure of another state if emanating from their territory; the integrity of the supply chain so that end users can have confidence in the security of ICT products; and the prevention of the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions. The GGE-Cyber also agreed a set of conclusions and recommendations for future work that included recognizing that ICTs are a driving force in development and calling for:

- Concept development and research on ICTs in international peace and security;
- Increased cooperation at regional and multilateral levels to foster common understandings on risks posed by the malicious use of ICTs and on the security of ICT-enabled critical infrastructure;
- Identification of mechanisms for the participation of the private sector, academia and civil society organizations;
- Dialogue on security and common understandings on the application of international law and norms, rules and principles for responsible behaviour.

⁵⁷ Group of Governmental Experts (2015), Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN General Assembly, A/70/174, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

The new dialogue on cybersecurity at senior official levels between the United States and China could be the start of a process that will operationalize the GGE-Cyber's call to establish 'dialogue on security and common understandings on the application of international law and norms, rules and principles for responsible behaviour'. The 2015 US–China cyber agreement was part of a wider group of measures to strengthen bilateral relations and build trust and confidence between the two countries. The agreement includes: i) timely responses to requests for information and assistance concerning malicious cyber activities; ii) cooperation in the investigation of cybercrimes, including the collection of electronic evidence, and mitigation of malicious cyber activity emanating from the territories of either party; iii) agreement not to conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information; iv) identifying and promoting appropriate norms of state behaviour in cyberspace within the international community; v) a high-level joint dialogue mechanism on cybercrime and related issues; and vi) a hotline for the escalation of issues that may arise in the course of responding to such requests.⁵⁸

Any proposed organization to address cybersecurity in space needs to reflect the multi-stakeholder character of the cyber and space communities.⁵⁹ Its structure would need to be fundamentally non-regulatory and sensitive to national perspectives in cybersecurity policies, accepting the need for regulation where necessary, and yet being nimble and responsive – in other words, everything that most governmental organizations are not. To begin with, and to ensure sensibilities are protected, the regime should set out simply to instil a culture of 'getting the basics right' – which, according to experts in the field, constitutes 80 per cent of the strategic response.⁶⁰

All participants and stakeholders in this regime need to understand this objective. The essence of the regime is that it works from all perspectives – organizational, business change and obsolescence management – to give it competitive advantage over its adversaries. The regime must be agile and act with initiative; actor-neutral; risk-based; and able to understand that a system level of response (i.e. based on technology alone) is not the answer. Not only that, but its core deliverable is to increase *collaboration* and *cooperation* in this highly dynamic environment in order to enhance *knowledge*. The outputs it generates will be hard to measure, as its success depends on a reduction in the number of attacks, in a domain where these have not been reported widely, making it hard to ascertain their absence.

The response to space cyber insecurity should be based on soft power, rather than controls underpinned by an international diplomatic community moving at glacial pace with a series of 'sticks' wielded by national regulators. The approach required must be from an international community of the willing responding to 'carrots', who have a shared awareness of the problem and a shared goal. Such an approach offers the most appropriate basis for an international space cybersecurity strategy that includes – rather than mandates – a wide variety of stakeholders with the necessary agility and flexibility. The regime would develop the essential 'top-down' approach needed to complement the 'bottom-up' security measures being developed by technological experts and state organizations assisting with intelligence and threat information and with highly complex forensics work.

⁵⁸ A summary of the agreement on cybersecurity, among other measures, is available at: The White House, Office of the Press Secretary (2015), 'Factsheet: President Xi Jinping's State Visit to the United States', 25 September 2015, <https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states>.

⁵⁹ See for example proposals in The President's National Security Telecommunications Advisory Committee (NSTAC) (2009), *Report to the President on Commercial Satellite Communications Mission Assurance*, http://www.dhs.gov/sites/default/files/publications/NSTAC%20STF%20Report%20FINAL%2011302009_0.pdf.

⁶⁰ As noted by GCHQ Director Sir Iain Lobban, 'Perhaps 80% of what we need to do is stuff we already know how to do – getting the basics of Information Assurance right will of itself raise the bar for malicious activity.' See transcript at: GCHQ (2012), 'Director GCHQ makes cyber speech at the International Institute of Strategic Studies', 12 October 2012, <https://www.gchq.gov.uk/speech/director-gchq-makes-cyber-speech-international-institute-strategic-studies>.

The regime needs to be a platform for communication and collaboration rather than taking any operational steps, or even overseeing tactical procedures, to increase security. From the outset, those functions would be left to national regulation and law enforcement authorities that may already be able to work with other states via existing bilateral and multilateral instruments designed to tackle other risks to society. However, research in other cybersecurity domains suggests that there is little history of successful institutional sharing, and this is perhaps the most critical failure of all. The regime's philosophy should therefore be based on a sharing economy. This may not suit some national authorities, however, given their traditional concern with security, which is principally directed at threats to the state and terrorist attacks.

Nevertheless, some states that already work in multilateral risk-reduction and multi-stakeholder enterprises may be more relaxed about participating in an international community of the willing. Such a regime would focus on cooperation and information-sharing in its early phases, if only to explore and set up systems for joint working and collaboration that can be expanded incrementally over time, and include more stakeholders as confidence increases. The regime would, however, have to recognize that any analysis it undertakes of cyberspace and related security threats is a problem that concerns all of society; not the exclusive concern of governments, commercial enterprises or international organizations. As noted above, in cyberspace security, different interests and constituencies are challenged by a variety of interconnected actors and actions. And if society – for all its diversity – cannot respond in a similarly interconnected way, then the sum of security diminishes overall and becomes dangerous.

This prospective multi-stakeholder alliance should initially be made up of those states and non-state entities that already have a relatively high national-level awareness of cyber risks and commensurately mature countervailing strategies, and that also accept the need for a decentralized approach. Such a group will be able to swiftly and collectively identify sets of core capabilities, particularly in best practices within each of their national strategies, and to produce those as industry-led standards for the benefit of an expectant community of interest. This will constitute the beginnings of a space cybersecurity regime.

7. Conclusions and Recommendations

Although cybersecurity is a technical issue, technology alone cannot provide the basis for driving policy. Entirely or largely technological approaches will not have the necessary breadth or depth to allow comprehensive participation in addressing the full range of cybersecurity challenges. They would exclude many stakeholders who could otherwise contribute usefully to responses to the variety of threats propagated through the internet. An over-reliance on technical fixes is why cybersecurity controls failed to make an effective impact on cyberthreats in the late 1990s and early 2000s. It is only in recent years that cybersecurity is being recognized as central to an organization's operations.

Yet if cybersecurity policies had inadvertently marginalized those with technological expertise, the pendulum would have swung too far the other way. Thus an effective regime requires a comprehensive technological response that is integrated into a wider circle of knowledge, understanding and collaboration.

The research for this project has led to a number of clear conclusions:

- Satellites and the commensurate space infrastructure, which also includes space vehicles and ground stations, are potentially vulnerable to a wide range of cyberattacks. They can be susceptible to the more common and well-understood cyberattacks such as data theft and data corruption, as well as to more sector-specific attacks including cyber-jamming, cyber-spoofing and hostile cyber-hijacking.
- Because so much of human activity is now dependent on space-based assets and infrastructure, most countries' critical infrastructure is potentially vulnerable to cyberattacks in that domain. An insecure environment in space will hinder economic development and increase risks to societies, particularly in crucial sectors such as communications, transport (air, maritime and land), energy (conventional, renewable and nuclear), financial transactions, agriculture, food and other resources management, environmental and weather monitoring, and defence. Space-related cybersecurity gaps and weaknesses therefore need to be addressed as a matter of urgency.
- Highly regulated institutional responses such as government-led approaches are likely to lack the agility and flexibility required for these cybersecurity capabilities.
- Lightly regulated multi-stakeholder approaches to cybersecurity in space that develop industry-led standards, particularly with regard to collaboration, knowledge exchange and innovation are more likely to ensure the required agility, creativity and speed of response.
- An international multi-stakeholder space cybersecurity regime – based on an international community of the willing, and shared risk assessments and threat responses – is likely to provide the best opportunity for developing a sectoral response to match the range of threats.

Producing a set of options to mitigate the risks would bring foreseeable, tangible benefits for the space infrastructure by increasing the resilience of the global economic infrastructure to cyberthreats, and enhancing confidence in space-related goods and services, including those associated with new global markets in space cybersecurity.

By developing an international multi-stakeholder cybersecurity regime, the space industry would enhance its existing reputation as a forward-thinking, market-leading community. It could also play an increasingly influential role in developing international standards and establishing a strong sustainable knowledge base in the cybersecurity domain.

An international community of the willing should be formed to act as a focal point for good practice in the space–cyber intersection. This like-minded, multi-stakeholder group would be tasked with concentrating on risk management approaches to space cybersecurity, and the formulation of industry-led standards in order to develop pace and agility in response.

The group, which could grow over time to include any state concerned with space cyber risks, would identify actions that can develop the skills, knowledge and collaborative mechanisms needed to catalyse greater resilience in the international space infrastructure. This would include the development, manufacture, deployment and operational management of space vehicles along with associated data systems and communications links.

In parallel, other work, commissioned by national authorities, should seek to identify and mitigate risks in infrastructures, concentrating not only on ground stations but also on working with manufacturers and insurance providers to protect satellites more effectively from the potential for unauthorized interference.

Recommendations

To develop the required end-to-end competence in a space cybersecurity regime, a number of capability development needs can be identified under each of the following functions. The research project from which this paper has been developed did not set out to capture a full set of requirements, but many were identified during the roundtables. Examples are noted here as recommended attributes of the individual functions of the envisaged space cyber regime.

Raising awareness

- Ascertain the minimum levels of knowledge required to develop an *instinct* for cybersecurity throughout the supply chain.
- Identify communications platforms that can be used to develop a common collaborative environment.
- Decide on communications platforms and paths, languages, lexicon and right of access.
- Agree on whether the authority should be regional or international, and how the authority should function.
- Develop an educational infrastructure that can spread throughout the internationalized supply chain into the user communities and adjacent sectors.
- Delineate what governments can do to help, such as providing threat briefings on a trust basis.
- Establish ways to maintain concepts of trust and operational security in a very broad and potentially large community.

- Agree on the qualifications needed to join a community of interest, and how to ensure that all members of the community add value.
- Establish a virtual knowledge platform with agreed security levels and operational redundancy.

Encouraging vigilance

- Ascertain specific needs in terms of identifying symptoms of an attack, or preceding reconnaissance.
- Provide threat briefings to explain what vigilance is needed.
- Train experts in how to notice unusual activity, and how to verify suspicions and then alert the community.

Identifying and mapping dependencies

- Establish procedures for identifying dependencies within relevant timescales.
- Assess dependencies for criticality and for lack of redundancy.
- Identify ecosystem connections that are driven by commercial considerations and configured for agility.
- Develop a sustainable, near-real-time, cloud-based system for mapping space ICT configurations.

Recognizing vulnerabilities

- Develop and maintain a risk matrix by matching vulnerabilities to threats, paying attention to the alignment of commercial and national infrastructure vulnerabilities and regularly updating the matrix.
- Identify the vulnerabilities that will not be commercially compelling to resolve, and ensure that regulators are aware.

Building in resilience and measured responses

- Agree what levels of resilience are required and how to ensure these are regularly revisited and updated.
- Find the right mix of market and governmental risk and reward judgments.
- Develop a funding stream for increased resilience and new technologies to achieve critical infrastructure levels of protection at both national and international levels.
- Build in incentives for investment in cyber resilience in satellite vehicles for cases where the value of the satellite and payload is comparatively low.
- Develop regulatory controls and standards (including templates as needed) for critical national and international systems, including minimum acceptable availability levels.
- Ensure a reporting mechanism is established to report changes in critical network configurations with monitoring and regulatory facilities.

- Delegate cyber controls into the supply chain at agreed standards so as to facilitate investment.
- Develop well-understood penalties for non-compliance under established legal frameworks.
- Work with the insurance sector to increase incentives.

Hardware and software future-proofing

- Develop approaches to future-proofing of existing hardware and software, given the often long life cycle of satellites and the problems of obsolescence in some ground systems as well.
- Invest in new ‘hack-proof’ or ‘hack-resistant’ technologies, including ‘blue-sky’ approaches such as quantum technologies for communication.

Procurement strategies

- Develop cooperative mechanisms whereby cybersecurity in space is made equivalent to physical safety in space and is not part of the commercially competitive agenda.
- Identify the procurement processes and legislative frameworks that should be used for public procurement in an international supply chain.
- Draw up security-conscious procurement strategies that match the speed of the market.
- Develop industry standards so that cybersecurity rigour can be ensured and insured through the entire supply stack, from the highest boardroom level all the way down to microchip level, with penalties for default.
- Establish clarity with regard to implementing national and international controls such as on international trafficking in arms regulations *vis-à-vis* the development and sharing of cybersecurity technology.⁶¹

Regulatory requirements

- Develop an international discussion on how the regime might function as an international community of the willing, and its relationship with international bodies such as COPUOS.
- Develop the regime in the form of a ‘general obligation to cooperate’ mechanism, deciding whether it should be a regulated or non-regulated information management environment, or both; and whether industry, academia or government should lead, or whether a multi-stakeholder approach could be more effective.
- Balance regulated and non-regulated instruments within the regime.
- Incorporate mechanisms beyond the regulated environments so that organizations are not inhibited from sharing knowledge, and ensure that this is understood by the regulatory bodies.
- Install mechanisms that enable legislative and regulatory requirements to be passed back to national and international authorities as needed.

⁶¹ See US Congress Subcommittee on Information Technology (2016), ‘Wassenaar: Cybersecurity and Export Control’, Oversight & Government Reform, 12 January 2016, <https://oversight.house.gov/hearing/wassenaar-cybersecurity-and-export-control>.

Sharing experience, including civilian–military knowledge exchange

- Establish mechanisms for communications processes to share experience and knowledge, including agreeing a common lexicon.
- Demonstrate that participation in the regime leads to significant advantage whereas non-participation is detrimental.
- Build confidence in the process so that traditional military reluctance to share technical data and threat information is overcome; this is particularly important given the considerable number of overlaps in civil and military capabilities.
- Develop understanding within the military authorities on the need for light-touch regulation in the commercial domain and increase the comfort level for the military authorities to work in, and contribute to, a low-regulation environment.
- Establish mechanisms for analysis and sharing of sensitive information.
- Implement established practices for international quality control.
- Develop collaborative mechanisms required for raising awareness and operational responses.
- Determine which communities should have access to the shared experience data.
- Identify an impartial player who can monitor inputs and outputs and share information safely and securely.
- Develop incentives for sharing information across the divides.

Establishment of good practice

- Determine what is good practice and good-enough practice.
- Aggregate good practice into a single system of guidance.
- Adapt working models for good practice and bring in mechanisms specific to the cyberspace community of interest.
- Agree on models for risk management.
- Set up mechanisms to determine the appropriate current and future requirements for cybersecurity in the various satellite missions.

Glossary of Terms

autonomous vehicles	self-driving, robotic vehicles
BeiDou	China's Navigation Satellite System
C-RAN	Cloud-Radio-Access-Network
CD	Conference on Disarmament
CERT	Computer Emergency Response Teams
CI	critical infrastructure
COPUOS	Committee on the Peaceful Uses of Outer Space
COTS	commercial orbital transportation services
cyber	associated with computers and digital technologies
cybersecurity	the security of digital technologies and networks
deconfliction	adjusting the orbits of satellites to guard against collision
denial of service [attack]	an interruption, typically with malicious intent, in an authorized user's access to a computer network; sometimes abbreviated to DoS; a distributed denial of service (DDoS) attack is when a DoS attack emanates from multiple sources
downlink	satellite-to-ground communication
EEAS SAB	European External Action Service Space Advisory Board
EGNOS	European Geostationary Navigation Overlay Service
encryption	encoding messages accessible only to authorized parties
Galileo	Europe's Global Satellite Navigation System
GEO	geostationary equatorial orbit
geostationary orbit	A geosynchronous orbit in which the satellite remains stationary over the same point on the earth's surface at a height of 35,786 km above the equator
geosynchronous orbit	Orbit with a period equal to the earth's rotational period
GGE	Group of Governmental Experts [United Nations]
GLONASS	Russia's Global Navigation Satellite System
GNSS	Global navigation satellite system
GPS	Global positioning system
ground station	a ground-based facility that communicates with satellites
hacking	exploiting weaknesses in cyber systems
HAPS	high-altitude pseudo-satellite
ICS	industrial control systems
ICT	information and communications technology
InSAR	Interferometric Synthetic Aperture Radar
internet	global system of interconnected computer networks
internet of things	internet connected devices that can communicate independently of the people using them
IRNSS	India's Regional Navigation Satellite System (now NAVIC)
ISS	International Space Station
ITAR	International Trafficking in Arms Regulations

ITU	International Telecommunication Union
jamming	deliberately interfering with wireless communications
Kessler Effect	a cascade of LEO satellite collisions in which each collision generates space debris that further increases the probabilities of subsequent collisions
LEO	low Earth orbit (180–2,000 km)
man-in-the-middle attack	an attack in which communications between two parties are covertly intercepted and hacked
MEMS	micro electro-mechanical systems
MIL-SPEC	military specification
M2M	machine-to-machine
NAVIC	Navigation Indian Constellation (formerly called IRNSS)
NOAA	United States National Oceanic and Atmospheric Administration
payload	the carrying capacity of a launch vehicle
PNT	positional, navigation and timing [information]
polar orbit	a highly inclined orbit in which the satellite moves around the Earth from pole to pole
QZSS	Quazi-Zenith Satellite System of Japan
RAD-hard	radiation-hardened
remote sensing	gathering information from a distance including from satellites
SAR	Synthetic Aperture Radar
SATCOM	satellite communications
satellite	an object in orbit
satellite constellations	group of satellites working in coordination
SBAS	satellite-based augmentation system
SCADA	supervisory control and data acquisition
SIM	subscriber identity module
SIM toolkits	standard of the GSM system that enables SIM-initiated actions (also called STK)
space	also called outer space; the universe beyond the earth's atmosphere
spoofing	masquerade through the falsification of data
supply chain	system of activities and resources required to supply a product or service from producer to customer
TCBM	transparency and confidence-building measures
UAS	unmanned aircraft system
uplink	ground-to-satellite communication
UN DC	UN Disarmament Commission
UNODA	UN Office of Disarmament Affairs
UN OOSA	UN Office for Outer Space Affairs

About the Authors

David Livingstone is an associate fellow at Chatham House, where he has participated in a broad range of projects on national-level risk management, cybersecurity, counterterrorism, serious organized crime, nuclear security and space security. He has given evidence to the UK parliament, has provided expert witness services to the Central Criminal Court, and is a regular media commentator. In his previous military career, he was policy lead on Military Aid to the Civil Powers at the UK Ministry of Defence between 1994 and 1999. He was a staff officer in the 'COBR' national crisis management centre, and worked on a number of cabinet official committees dealing with counterterrorism and security. He was a founder member of the cabinet official committee on cybersecurity in 1996. He currently advises government and commercial clients on security capability development in various capacities, including as cybersecurity strategy adviser to the Scottish government; doctrine development for the UK Financial Services Virtual Task Force; contributing to National Audit Office studies on the UK's cybersecurity strategy; and as author of the ACPO (Association of Chief Police Officers) 2011 Cyber Crime Strategy.

Dr Patricia M. Lewis is the research director of the International Security Department at Chatham House. Her former posts include deputy director and scientist-in-residence at the Center for Nonproliferation Studies at the Monterey Institute of International Studies; director of the United Nations Institute for Disarmament Research; and director of VERTIC. She served on the 2004–06 Weapons of Mass Destruction Commission and the 2010–11 Advisory Panel on Future Priorities of the Organisation for the Prohibition of Chemical Weapons, and was an adviser to the 2008–10 International Commission on Nuclear Non-proliferation and Disarmament. She is currently a commissioner on the 2014–16 Global Commission on Internet Governance, and is a member of the European External Action Service Space Advisory Board as a senior adviser to the EU Special Envoy for Space. She publishes widely on all aspects of international security, including chemical, biological, radiological and nuclear weapons; conventional forces; cybersecurity; space security; internet governance; terrorism; and conflict prevention. She holds a BSc in physics from the University of Manchester, a PhD in nuclear physics from the University of Birmingham, and an Honorary LLD from the University of Warwick. She is the recipient of the American Physical Society's 2009 Joseph A. Burton Forum Award recognizing 'outstanding contributions to the public understanding or resolution of issues involving the interface of physics and society'.

Acknowledgments

This research paper has been produced with support from the Sasakawa Peace Foundation (SPF). We are grateful to the SPF for the generous financial, practical and intellectual support in 2015–16 that enabled the research for and writing of this paper. Special thanks are due to Risa Arai and Tetsuya Hiroshima of the SPF for all their assistance. We thank the participants in the Chatham House roundtables who gave generously of their time and expertise and the peer reviewers of the paper.

Thanks also go to Toby Simon and his team at the Synergia Foundation in Bangalore, India, who generously hosted a high-level roundtable at which the experts provided further high-quality information. The meeting was co-chaired by Dr Raji Rajagopalan of the Observer Research Foundation (ORF) in Delhi. And we also thank Finmeccanica (now Leonardo) for its continued participation in this research stream at Chatham House.

We are immensely grateful to Paul Febvre, Chief Technology Officer at Satellite Applications Catapult for his assistance with technical aspects of the paper, and to Margaret May for her work in editing the text. Henry Dodd deserves a special mention for his note-taking and support throughout the project. Thanks are also to Hannah Bryce and Nilza Amal of the International Security Department at Chatham House, and to Jo Maher of the publications team, for all their support.

Independent thinking since 1920



Chatham House, the Royal Institute of International Affairs, is an independent policy institute based in London. Our mission is to help build a sustainably secure, prosperous and just world.

All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical including photocopying, recording or any information storage or retrieval system, without the prior written permission of the copyright holder. Please direct all enquiries to the publishers.

Chatham House does not express opinions of its own. The opinions expressed in this publication are the responsibility of the author.

Copyright © The Royal Institute of International Affairs, 2016

Cover image: The Soyuz TMA-19M spacecraft attached to the International Space Station on 16 June 2016.

Copyright © Photo by Tim Peake/ESA/NASA via Getty Images

ISBN 978 1 78413 120 3

This publication is printed on recycled paper.

The Royal Institute of International Affairs
Chatham House
10 St James's Square, London SW1Y 4LE
T +44 (0)20 7957 5700 F +44 (0)20 7957 5710
contact@chathamhouse.org www.chathamhouse.org

Charity Registration Number: 208223