Safeguarding Australia's Assets in Space

Cybersecurity for Satellites

Australia's 2020 Cyber Security Strategy - A call for views

1 NOVEMBER 2019

WiseLaw

Authored by: Jonathan Lim

WISE LAW

Contents

1. **Introduction**……..Page 2
2. **Context**……..Page 3
   - *A Rapidly Expanding Space Industry* Page 4
   - *Cybersecurity Risks in Space* Page 6
3. **Critical Analysis**……...Page 8
   - *Current Policies and Regulations* Page 8
   - *Case Examples* Page 9
4. **Recommendations**……Page 12
   - i) *Creation of a Cyber Security Task Force to Address Space-Related Assets* Page 12
   - *ii) Adopting Transparency and Confidence Building Principles* Page 12
   - *iii) Devise a Cyber Best Practice Toolkit for Space-Related Assets* Page 13
   - *iv) Recognize Both Space and Cyber as Critical Infrastructure Sectors* Page 14
   - *v) Intra and Extra Governmental Coordination* Page 15
   - *vi) Expand Cyber-Specific Insurance to Cover Space-Related Assets* Page 15
   - *vii) Adherence with International Laws and Principles* Page 16
5. **Summary**……..…Page 17

1. Introduction

The continued absence of federal legislative provisions, policies, or guidelines addressing the issue of cybersecurity surrounding space-based assets within Australia's Cyber Security Strategy represents a significant oversight by the government in safeguarding our national critical infrastructure, ensuing a stable and secure marketplace for commercial space enterprises, and defending Australia's collective national security in the 21st century.

The continuing importance for policy makers to consider the manifold impacts of increased connectivity and larger attack-surfaces, via the Internet of Things (IoT), necessitates cyber security risk analysis over the impacts of increased interconnectivity upon space-based systems. The progression of traditional market incentives to reduce costs and enhance innovation has resulted in the access to space becoming increasingly democratized. Consequently, the offering of low-cost launch options, the relaxation of restrictive laws, and the ever-lowering manufacturing costs for electronics facilitates an increasingly crowded and hazardous cyber ecosystem in outer space.

Despite the existing significant amount of funds invested into satellite security, readily-available advanced technologies make these satellites prone to non-kinetic attacks (i.e. cyberattacks) – including jamming, data theft, hacking and spoofing. All levels of government and any private organisation working in the domain of space must therefore possess a solid cybersecurity foundation – where an efficient, mature and well-developed cyber strategy is necessary to underpin a robust cybersecurity posture for Australia in outer space.

2. Context

Presently, Australia's regulatory framework does not adequately provide for a cybersecurity strategy encompassing space-based assets – whether it includes satellites, rockets, satellite ground stations, or human habitats in outer space. The current absence of any regulatory direction in the sector is given the recent establishment of the Australian Space Agency in the aftermath of Australia's 2016 Cyber Security Strategy.

Since the establishment of Australia's Space Agency (ASA) on 1 July 2018,[1] the new agency has been enthusiastically pursuing collaborative efforts with domestic satellite companies (i.e. Myriota, Gilmour Space Technologies) and foreign space agencies in a bid to enhance the capabilities of Australia's space industry. This was most recently demonstrated in federal government's signing of a $150 million investment in the Australian space sector over 2019 to 2024 - intending to support local businesses and create new technologies which will bolster NASA's interplanetary travel initiatives.[2]

It is the stated intent of the ASA to triple the size of the Australian space sector from $3.9 billion to $12 billion and create 20,000 new jobs by 2030. [3] However, the government has not yet taken the opportunity to consider the centrality of cyber security in safeguarding and facilitating the prosperity of the nascent space sector.

The democratisation of space activities (i.e. launches) requires organisations to be prepared for the advanced technical multi-order problems incited by advanced cyber actors, whom have turned their attention to space as the next strategic high ground open to competition and domination. Both the ASA and commercial space sector collectively require a fundamental change in how they manage cybersecurity. This is increasingly important within the context of the Fourth Industrial Revolution (4IR) – where simultaneous revolutions across the cyberspace and outer space provide a multitude of risks and opportunities within the fusion of these two domains. [4]

Within cybersecurity this includes the advent of 5G and the growth in adoption of sophisticated mobile devices, the Global IoT and small device network access, globally accessible broadband internet infrastructure, and more affordable and faster processes – contributing to advances in machine learning, artificial intelligence and blockchain technology.

Within space, this includes the democratising of payload launches - where almost anyone can launch a small satellite, employ cheaper and higher-quality space qualified designs, explore satellite connectivity as a mainstream service, and pursue satellite constellations as a service with time-based access to dynamically reprogrammable payloads.

---

[1] Megan Clark, 'Australian Space Agency launches operations: A message from Head, Dr Megan Clark AC' on Department of Industry (29 June 2019) <https://www.industry.gov.au/news-media/australian-space-agency-news/australian-space-agency-launches-operations-a-message-from-head-dr-megan-clark-ac>.
[2] Nadine Craneburgh, 'Australia's space industry gets $150 million boost to help NASA hit its 2024 moonshot' on Ceate Digital (27 September 2019) <https://www.createdigital.org.au/australias-space-industry-150-million-boost-help-nasa-hit-next-moonshot/>.
[3] Jacqui Tyack, 'Building satellite IoT capability' on Department of Industry (15 July 2019) <https://www.industry.gov.au/news-media/australian-space-agency-news/building-satellite-iot-capability>.
[4] Frank Pound, 'Space Cybersecurity – Why we mustn't forget the basics'(2019) 3(21) *Room – Space Journal of Asgardia* 9.

The continued absence of regulatory foresight into cybersecurity safeguards for Australia's space assets leaves our space-based infrastructure open to the potential for untold harm to end-point users – encompassing damage to physical systems, destruction of physical systems, reputational damage to one's government/organization, operational disruption (reduction in safety, productivity, revenue, functionality), the outright theft of remote space-based assets, and the compromise of business-critical data, and IP theft and industrial espionage.

A Rapidly Expanding Space Industry

Across the international commercial space sector there has been an increased emphasis surrounding the area of miniaturized satellites (includes small satellites, microsatellites, and nanosatellites). This is given the specific democratising impacts of 4IR upon the commercial space sector – resulting in ever-lowering barriers of entry through decreasing costs of electronics and constant miniaturisation of technology.

Over the past several years, reliance upon satellite technologies has increased due to technological advancement. Satellites comprise one of the most critical infrastructure assets a nation can own in outer space, attributed to the immense amount of expenses required to manufacture, launch, and operate it. [5] Satellites are considered as essential assets in navigation, communication, defence systems, metrology, multiple applications, and remote sensing. Some everyday applications which rely upon satellite functionality include television, telephones, GPS navigation, and business and finance. [6]

Miniaturized satellites (minsats) stand as the next iterative step within the NewSpace/Space 2.0 ecosystem, given their rapid innovation and deployment cycles, and lower cost structures – with construction and launch ranging from below USD$100,000 for microsats, to $1,000 for nanosatellites depending on the payload mass. This is as opposed to the traditional cost of satellites, which cost within the tens of millions to construct, authorize, launch and operate. [7]

The number of active satellites in orbit has continued to increase exponentially over the past decade, with the number having increased from 1,500 to 2,062 between 2017 [8] to 2019. Presently, the country operating the largest number of satellites in the US (901), followed by China (299), Russia (153) and others (709). [9]

[5] Alex Roney Matthew, 'Cyber Security – How Vulnerable are Satellites to Cyber Attacks' (2019) 7(3) *International Journal for Research in Applied Science & Engineering Technology* 2427.
[6] Union of Concerned Scientists, 'What Are Satellites Used For?' on Union of Concerned Scientists (15 January 2015) <https://www.ucsusa.org/resources/what-are-satellites-used>.
[7] Peter Dockrill, 'This Tiny Satellite Could Be Your Own Personal Spacecraft From Just $1,000' on Science Alert (8 April 2016) <https://www.sciencealert.com/this-tiny-satellite-could-be-your-own-personal-spacecraft-from-just-1-000>.
[8] Nick Routley, 'A High Level Look at Satellites' on Stratfor (25 May 2017) <https://worldview.stratfor.com/article/high-level-look-satellites>.
[9] Union of Concerned Scientists, 'UCS Satellite Database' on Union of Concerned Scientists (31 March 2019) <https://www.ucsusa.org/resources/satellite-database##targetText=Assembled%20by%20experts%20at%20the,currently%20in%20orbit%20around%20Earth >.

Additionally, earlier 2016 industry projections of 3,000 nano/microsatellites being launched between 2016 to 2022 [10] have been outstripped by a rapidly expanding space industry – with current predictions expecting the launch of 6,000 nano/microsatellites between 2019 to 2025. [11] It has been advanced that by 2025 upwards of 1,100 satellites could be launching each year, as opposed to 365 in 2018. [12]

A host of commercial space companies are striving to develop low-cost access to space and spaceflight technologies. This includes several privately funded transnational companies including SpaceX, Boeing, Virgin Galactic and Blue Origin – all of whom are engaged in the research, production and sale of space-based technologies which will enable the launch of commercial passengers into space over the next decade. [13] SpaceX's ambitious are highlighted within the Starlink project, which aims to construct an orbital satellite network of 12,000 minisats by 2027 – providing high-speed, low-latency and affordable internet access worldwide. [14]

Accordingly, congestion in signalling networks has become a significant concern for satellite operators. Large satellite manufacturers and operators increasingly oppose the allocation of designated frequencies to small satellites via the International Telecommunications Union (ITU) and the Australian Communication and Media Authority (ACMA). This is driven by the fact that small satellites often do not use less bandwidth in proportion to their smaller size – with their mass proliferation representing a significant risk of congestion and interference in the electromagnetic spectrum. [15] Accordingly, it is this increasingly interconnected, congested, and fragile network of space-based infrastructure which represents an acute vulnerability within Australia's cyber security strategy.

[10] Bill Doncaster and Jordan Shulman, '2016 – Nano/Microsateellite Market Forecast' on SpaceWorks Enterprises (30 March 2016) <https://digitalcommons.usu.edu/cgi/viewcontent.cgi?filename=0&article=3336&context=smallsat&type=additional> 17.
[11] Nanosats Database, 'World's largest database of nanosatellites, over 2500 nanosats and CubeSats' on Nanosats Database (30 October 2019) <https://www.nanosats.eu/>.
[12] Tate Ryan-Mosley et al., 'The number of satellites orbiting Earth could quintuple in the next decade' on MIT Technology Review (26 June 2019) <https://webcache.googleusercontent.com/search?q=cache:bAkmW90jj98J:https://www.technologyreview.com/s/613746/satellite-constellations-orbiting-earth-quintuple/+&cd=1&hl=en&ct=clnk&gl=au>.
[13] Jim Bozin, 'Why Big Business Is Making a Giant Leap into Space' on Knowledge@Wharton (4 June 2019) <https://knowledge.wharton.upenn.edu/article/commercial-space-economy/>.
[14] Dave Mosher, ' Elon Musk just revealed new details about Starlink, a plan to surround Earth with 12,000 high-speed internet satellites. Here's how it might work' on Business Insider (15 May 2019) <https://www.businessinsider.com.au/spacex-starlink-satellite-internet-how-it-works-2019-5?r=US&IR=T>.
[15] Duncan Blake, 'The problems with small satellites – and what Australia's Space Agency can do to help' on The Conversation (7 December 2019) <http://theconversation.com/the-problems-with-small-satellites-and-what-australias-space-agency-can-do-to-help-108156>.

Cybersecurity Risks in Space

The cyber warfare capabilities of state actors could become a larger challenge in the coming years to Australia's space infrastructure – especially where satellites present a visible target for attackers to rapidly disable our national critical infrastructure. Indeed, a crude cyber capability is more easily accessible than other kinetic counter-space capabilities – where it is developed and deployed much faster than an ASAT, it is comparatively inexpensive. [16]

Satellites possess a series of vulnerable points, rather than a single point that is easier to defend. This is given the remote operational functions of a satellite - where it requires a constant stream of communication and data with either ground stations or other satellites to monitor its status, track its position, and perform its functions. [17] Cyber-attacks will thus quickly evolve to exploit the new satellite-driven data economy which is heavily bolstered by Space 2.0 resources.

Where a communication satellite is compared to a radio repeater that has about 24 transponders and uses a specific frequency block. – the uplink sends signals at the range of 6 GHz, while the satellite receives and converts it to 4 GHz and transmits it back. The only form of security herein is through encryption and encoding the signals which are not efficient to keep the attackers away. Regardless, satellite users and operators face persisting cyber security issues, include the following: [18]

- Double illumination interference – Where an attacker to interferes with a satellite's service during a double illumination, where one frequency carries two or more carriers. While the carriers may be from uplinks of different location, the effects of illumination jams the satellite with signals from overlapping frequencies. If the interference is strong enough, it can effectively cut satellite transmissions. [19]

- Supply chain attack – Where attackers implant foreign devices on ground satellites and exploit it later after gaining access. This device may decrypt and decodes the system, granting access to the attackers, whom may wreak havoc through misinformation, disinformation and mal-information. The attack may decide to alter the traffic system, manipulate weather data, gain access to financial information, or alter television broadcasts to their preference.

- Targeting Very Small Aperture Terminals (VSATs) – These are small telecommunication earth stations which receive and transmit real-time data via satellite. Potential attackers may penetrate the passwords of factories and industries which were never changed. They may then jam, hack and exploit the signals, gaining access to the satellite's system

[16] Rajeswari Pillai Rajagopalan, 'Electronic and Cyber Warfare in Outer Space' on UNIDIR (May 2019) <https://www.unidir.org/files/publications/pdfs/electronic-and-cyber-warfare-in-outer-space-en-784.pdf> 9.
[17] Meghan Bartels, 'Why Satellites Need Cybersecurity Just Like You' on Space.com (10 December 2018) <https://www.space.com/42658-cybersecurity-for-satellites.html>.
[18] Matthew, above n5, 2428.
[19] Morgen E. Peck, 'Bitcoins in Space' on IEEE (9 December 2013) <https://spectrum.ieee.org/computing/networks/bitcoins-in-space##targetText=Satellites+do+have+their+own,with+signals+from+overlapping+frequencies>.

- False earth station attacks – Where satellites are controlled from the earth through ground stations, if the authentication between the ground station and the satellite is poor or non-existent, an attacker can gain control of the satellite or its transmitted payload. [20]

- Evil satellite twin – Where an attacker whom sets up a device at an altitude (i.e. drone) can broadcast information as though it came from a legitimate source. The expected action based on satellite information would then be easily manipulated, resulting in GPS scrambling, overridden television broadcasts, or blocking of satellite communications.

- Inter-satellite trust – Where satellites often form parts of mesh networks, this allows other satellites in the network to sit with their security perimeter. Since satellites are usually unhardened to radio, posing as a member of the network grants easy access to it.

This expanding space ecosystem is also prone to the traditional cyber security risks afflicting IoT devices – including insecure web interfaces, insufficient authentication and authorisation, insecure network services, lack of transport encryption, privacy concerns, insecure cloud interface, insufficient security configurability, insecure software/firmware, and poor physical security of terrestrial based assets. [21]

National space agencies have often been singled out as a prime target for nation-states and criminal elements – given their retention of a nation's research and development assets, control of national critical infrastructure, and their symbolic representation of a nation's technological and economic prowess. This has been illustrated by the scale of cybersecurity incidents encountered by NASA, which encounters at least one cybersecurity threat per day from state actors involved in technology acquisition. [22]

In 2018, NASA's Jet Propulsion Laboratory (JPL) was hacked via an unauthorized Rasberry Pi computer connected to JPL servers, which prompted concerns that the attackers could move laterally into JPLs communications systems and disrupt signals used on human space flight missions. [23] Cyber security experts have also expressed concerns over the vulnerability to space suits, especially where suits are created with network access and are interfaced with any onboard systems. [24]

[20] Craig Gibson, 'Attack Vectors in Orbit: The Need for IoT and Satellite Security in the Age of 5G' on Trend Micro (11 June 2018) <https://blog.trendmicro.com/trendlabs-security-intelligence/attack-vectors-in-orbit-need-for-satellite-security-in-5g-iot/>.
[21] Ashwin Pal, 'The Internet of Things (IoT) – Threats and Countermeasures' on CSO (20 May 2015) <https://www.cso.com.au/article/575407/internet-things-iot-threats-countermeasures/>.
[22] Hanneke Weitering, 'NASA Battled Cybersecurity Threats During Government Shutdown' on Space.com (4 February 2019) <https://www.space.com/43215-nasa-cybersecurity-government-shutdown.html>.
[23] Office of Inspector General, 'CYBERSECURITY MANAGEMENT AND OVERSIGHT AT THE JET PROPULSION LABORATORY' on NASA (18 June 2019) <https://oig.nasa.gov/docs/IG-19-022.pdf>.
[24] Wes O'Donnell, 'We Asked NASA: Is It Possible to Hack into a Spacesuit?' on In Space News (7 October 2019) <https://inspacenews.com/we-asked-nasa-is-it-possible-to-hack-into-a-spacesuit/>.

3. Critical Analysis

Current Policies and Regulations

Not once within the Australia's 2016 Cyber Security Strategy was the issue of space-based technology mentioned – highlighting a worrying lack of notice concerning cybersecurity or encryption standards for Australia's space-based assets. [25]

The most current regulatory framework for Australia's activities in space is dictated by the *Space (Launches and Returns) Act 2018* (Cth), which commenced on 31 August 2019. The Act manages the launching and returning of a space objects both to and from Australia and overseas, and specifies the requirements for organisations operating a launch facility in Australia.

While the 2018 Act does not provide for neither cybersecurity nor specific "technology security plans," it is reinforced by several rules. Rules are not formal acts of parliament, but are subordinate pieces of legislation created by the executive branch of government with the authorisation of parliament. [26] These rules explain the application requirements for space and high-power rocket activity approvals, and contain provisions covering "technology security": [27] [28]

1) Space (Launches and Returns) (General) Rules 2019 [29]
2) Space (Launches and Returns) (High Power Rocket) Rules 2019[30]
3) Space (Launches and Returns) (Insurance) Rules 2019 [31]

The General Rules[32] includes provisions which require that the holder of a launch facility license to provide a technology security plan(TSP) for the launch facility – R.8(1)I, requires information on individuals involved in the preparing/implementing/monitoring of the TSP – R18(2), that an application must contain a TSP for the launch facility – R.22(1), and that an application must include a TSP relating to the launch and any connected return – R.56(1).

---

[25] Department of Home Affairs, 'Australia's Cyber Security Strategy' on Department of Home Affairs (2016) <https://cybersecuritystrategy.homeaffairs.gov.au/AssetLibrary/dist/assets/images/PMC-Cyber-Strategy.pdf>.
[26] Attorney-Generals Departmebt, 'Understanding Legislation' on Government of South Australia (2019) <https://www.legislation.sa.gov.au/Web/Information/Understanding%20legislation/UnderstandingLegislation.aspx#rules>.
[27] Department of Industry, 'Regulating Australian Space Activities' on Department of Industry (2019) <https://www.industry.gov.au/regulations-and-standards/space-regulation>.
[28] Ian McGill and Connie Ye, 'The Launches and Returns Act: one of the most significant updates to the Space Activities Act since its implementation' on Allens Linklaters (26 September 2019) <https://www.allens.com.au/insights-news/insights/2019/09/the-launches-and-returns-act-one-of-the-most-significant-updates-to-the-space-activities-act-since-its-implementation/#anchor4>.
[29] Federal Register of Legislation, 'Space (Launches and Returns) (General) Rules 2019' on Federal Register of Legislation (2019) <https://www.legislation.gov.au/Details/F2019L01118>.
[30] Federal Register of Legislation. 'Space (Launches and Returns) (High Power Rocket) Rules 2019' on Federal Register of Legislation (2019) <https://www.legislation.gov.au/Details/F2019L01119>.
[31] Federal Register of Legislation, 'Space (Launches and Returns) (Insurance) Rules 2019' on Federal Register of Legislation (2019) <https://www.legislation.gov.au/Details/F2019L01120>.
[32] Federal Register of Legislation, above n27.

The High Power Rocket Rules[33] includes provisions which require the holder of a high power rocket (HPR) permit to provide a TSP of their launch to the Minister on request – R.9I, an application for a HPR permit to include information on the individual involved in preparing/implementing/monitoring the TSP – R.17(2), and an application for HPR permit to include a TSP relating to the launch – R.29(1).

Beyond these provisions there does not exist more detailed requirements regarding the quality of such TSPs – for requirements concerning the type of operating systems to be used, for requirements on updating operating systems and software, requirements concerning how the data is to be stored on space-based assets, requirements for SIEM software, requirements for logs/data retention, nor requirements for reporting damage or losses sustained from cyber-attacks.

Accordingly, in the event of a cyberattack upon an Australian entity's satellite the victim may not be obligated to disclose to the government that such an incident has occurred, nor detail what aspects of national critical infrastructure were affected. Any response and recovery efforts taken in its aftermath may also be taken without the involvement of the ACSC.

Additional to this is the Australian Civil Space Strategy, a document which works on strengthening Australia's competencies and growing capabilities across position, navigation and timing (PNT), earth observation (EO), communications technologies and services, space situational awareness and debris monitoring, leapfrog R&D, robotics and automation on Earth and in space, and access to space. [34]

The contents of the strategy acknowledges that cyber security provides risks for the growing space industry and regulations, outlines the responsibility of the government to advise on the intersection between space matters and the broader security environment (incl. cyber security), and advances that it is the government's responsibility to develop a world-class regulatory system that enables entrepreneurship while ensuring security (incl. cyber security). [35] Accordingly, it is incumbent upon the federal government to analyse, consider and regulate for cyber security standards across Australia's space-based assets.

Case Eexamples

During a military crisis, the potential for cyberattacks could cast doubt on intelligence and increase the risk of misperception. An attack could also threaten missile systems, both strategic and tactical, which rely on satellites and the space infrastructure for navigation and targeting, command and control, operational monitoring, and other functions.

Indeed, existing vulnerabilities across numerous space systems have given rise to a number of suspected and confirmed non-kinetic (cyber) attacks from both state and non-state actors - the consequences of which have

[33] Federal Register of Legislation, above n28.
[34] Department of Industry, 'Australian Space Agency' on Department of Industry (2019) <https://www.industry.gov.au/strategies-for-the-future/australian-space-agency>.
[35] Australian Space Agency, 'Advancing Space – Australian Civil Space Strategy 2019-2028' on Department of Industry (2019) <https://publications.industry.gov.au/publications/advancing-space-australian-civil-space-strategy-2019-2028.pdf>.

enabled the development of transnational organized crime, impeded access to national critical infrastructure, and allowed states actors to restrict human rights efforts abroad. The following list represents noted instances of non-kinetic interference with space-based assets: [36]

- In 2005, the Libyan government jammed 2 telecommunications satellites - disrupting entertainment services across European and US diplomatic, military, and intelligence communications. The jamming started on 19 September following the launch of the radio station 'Sout Libya' broadcasting on human rights and freedom of speech issues to Libya from London, and resulted in significant financial losses for the radio station. [37]

- In 2009, Brazilian authorities arrested 39 people using homemade equipment to hijack UHF frequencies dedicated to the US Navy's Fleet Satellite Communication system (FLTSATCOM) for their personal use.

  The open and unencrypted nature of the FLTSATCOM communication channel enabled a number of rogue loggers and drug dealers operating in the region to communicate, coordinate, and escape law enforcement through the use of an ordinary ham radio transmitter operation in the 144- to 148-MHZ range. [38]

- In 2010, the head of the Islamic Republic of Iran Broadcasting acknowledged the jamming of Persian-language satellite broadcasts originating from other countries. This followed a statement from the ITU condemning satellite interference signals coming from Iran, which was harming signals from satellite networks run by EutelSat – a French satellite operator. [39]Accordingly, the incident compelled Eutelsat's operators to drop BBC and VOA programming from the satellite. [40]

- In 2011, a report to Congress by the US-China Economic and Security Review commission determined at least two US government satellites (Landsat-7 and Terra AM-1) had experienced at least two separate instances of interference consistent with cyber activities against their command and control systems.

  It was alleged that the Chinese military had gained access to the satellites by hijacking the internet connection at the Svalbard Satellite Station in Norway, potentially allowing them to destroy or exploit the system for intelligence purposes. [41]

---

[36] Robert Lemos, 'Cybersecurity Experts Worry About Satellite & Space Systems' on DarkReading (2 July 2019) <https://www.darkreading.com/attacks-breaches/cybersecurity-experts-worry-about-satellite-and-space-systems/d/d-id/1335131>.
[37] David Hencke and Owen Gibson, 'Protest to Libya after satellites jammed' on The Guardian (3 December 2005) <https://www.theguardian.com/uk/2005/dec/03/politics.libya>.
[38] Wired Staff, 'The Great Brazilian Sat-Hack Crackdown' on Wired (20 April 2009) <https://www.wired.com/2009/04/fleetcom/>.
[39] Stephanie Nebehay, 'U.N. tells Iran to end Eutelsat satellite jamming' on Reuters (26 March 2010) <https://www.reuters.com/article/us-iran-jamming-itu/u-n-tells-iran-to-end-eutelsat-satellite-jamming-idUSTRE62P21G20100326>.
[40] Human Rights Watch, 'Letter to Eutelsat Regarding Iranian Government's Jamming of Satellite Broadcasts' on Human Rights Watch (25 June 2010) <https://www.hrw.org/news/2010/06/25/letter-eutelsat-regarding-iranian-governments-jamming-satellite-broadcasts>.
[41] Matthew Humphries, 'Chinese hackers took control of NASA satellite for 11 minutes' on Geek.com (19 November 2011) <https://www.geek.com/geek-pick/chinese-hackers-took-control-of-nasa-satellite-for-11-minutes-1442605/>.

- In 2019, Symantec reported of a sophisticated hacking campaign, launched from several computers in China which infiltrated satellite operators, defense contractors and telecommunications companies in the US and Southeast Asia.

  The attackers had employed "living off the land" tactics to comprise victim networks, using operating system features and legitimate network administration tools to remotely install malware on computers. [42] Where the attackers infiltrated computers involved in the operational control of satellites, the hackers were touted as possessing the potential to alter the positions of the orbiting devices and disrupting data traffic. [43]

- In 2019, the Centre for Advanced Defence (C4AD) alleged that Russia was hacking the global navigation satellite system (GNSS) on a mass scale. [44] These incidences of GNSS spoofing were tied closely to sensitive Russian government locations and the supposed location of President Vladimir Putin, with the aim of obfuscating his movements.

  These GNSS spoofing activities conducted by the Russian government were described as "more indiscriminate and persistent, larger in scope, and more geographically diverse than previous public reporting suggested" – with 9,883 suspected instances of spoofing between Feb 2016 to Mar 2019 affecting 10 locations and 1,311 civilian vessel navigation systems.[45]

  This incident shed light on the increasing affordability and accessibility of GPS spoofing technologies, which researchers highlighting that such technologies could be purchased for as little as $300, [46] and Pokemon Go players having used GPS spoofing apps and technologies (i.e. software-defined radio) to gain unfair advantages in the game. [47]

---

[42] Security Response Attack Investigation Team, 'Thrip: Espionage Group Hits Satellite, Telecoms, and Defense Companies' on Symantec (20 June 2019) <https://www.symantec.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets>.
[43] Joseph Menn, 'China-based campaign breached satellite, defense companies: Symantec' on Reuters (20 June 2018) < https://www.reuters.com/article/us-china-usa-cyber/china-based-campaign-breached-satellite-defense-companies-symantec-idUSKBN1JF2X0>.
[44] Jim Edwards, 'The Russians are screwing with the GPS system to send bogus navigation data to thousands of ships' on Business Insider (14 April 2019) <https://www.businessinsider.com.au/gnss-hacking-spoofing-jamming-russians-screwing-with-gps-2019-4?r=US&IR=T>.
[45] C4ADS, *Above Us Only Stars – Exposing GPS Spoofing in Russia and Syria* (C4ADS, 2019) <https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5c99488beb39314c45e782da/1553549492554/Above+Us+Only+Stars.pdf> 3.
[46] Matt Burgess, 'To protect Putin, Russia is spoofing GPS signals on a massive scale' on Wired (27 March 2019) <https://www.wired.co.uk/article/russia-gps-spoofing>.
[47] Maria Simsky, 'How do we ensure GNSS security against spoofing?' on GPS World (9 October 2019) <https://www.gpsworld.com/how-do-we-ensure-gnss-security-against-spoofing/>.

4. Recommendations

i) Creation of a Cyber Security Task Force to Address Space-Related Assets

Specifying for the creation of a such a task force by the Department of Home Affairs within Australia's 2020 Cyber Security Strategy to address specific cyber security concerns in outer space would help bolster Australia's economic, military and political posture in space.

This entity would ideally be involved in generating attack scenarios and incident response playbooks, acting as a cooperative liaison with foreign space agencies, acting as a centralized node for victim organisations to refer to, designing mitigation measures for the ASA, and raising awareness of cybersecurity matters in space through industry collaboration, engagement, and education.

In improving cyber resilience in the space sector, the entity may consider the following in designing space mitigation measures for both the ASA and private satellite operators: [48]

- Technological aspects – Such as incorporating terrestrial back-ups for national critical infrastructure, or investing in quantum systems for secure communication;
- The value of insuring in assurance or redundancy systems;
- Recovery capacity – Including how quickly a system can be fixed, what type of forensic applications may aid attribution process;
- Organisational culture and human resources aspects – Including training and education and human-in-the-loop considerations while incorporating emerging technologies (i.e. artificial intelligence); and
- Counteracting foreign interference – Where there exists a history of satellite operators having their space-based assets targeted by foreign actors, in response for the hosting and broadcasting of human rights and freedom of speech content, the task force may consider how Australia may support such victims and respond diplomatically to such incursions. [49]

ii) Adopting Transparency and Confidence Building Principles

Within the 2020 Cyber Security Strategy, the federal government must keep in mind the following principles when engaging with private entities. This is necessary in crafting the formation of an inclusive national policy and advancing global cybersecurity. [50]

Firstly, the advancement of voluntary, industry-led efforts, and public-private partnerships represent the optimal way to address cybersecurity at the national or international levels. This will involve encouraging dialogue between start-up satellite operators, established satellite and telecommunication companies, and the government over how best to coordinate in addressing potential cyber threats to Australia's space assets.

---

[48] Beyza Unal, 'Space-based cybersecurity challenges for NATO'(2019) 3(21) *Room – Space Journal of Asgardia* 18
[49] Human Rights Watch, above n38.
[50] Global Satellite Coalition, 'Cybersecurity' on Global Satellite Coalition (2019) <https://gscoalition.org/policy/cybersecurity>.

Secondly, satellite industry organizations should actively address cybersecurity using industry best practices for risk management. This would involve reference to international standards under the ITU, and each company in the satellite ecosystem developing individual risk management approaches until such time that the government can adequately legislate and regulate on the matter. This includes organisations assessing whether to implement or customize one or more of many available tools/technologies such as blockchain and artificial intelligence within their space assets.

Finally, robust cybersecurity is aided by voluntary information sharing, free from the fear of adverse consequences by the government. Where space sector participants may face several common cyber threats, so they must be free to collaborate with industry partners and the government to identify and respond to attacks, share mitigations, and learn from past experiences. This may precipitate the formation of a bespoke notifiable data breaches scheme, tailored to the specific cyber security challenges facing the space industry.

iii) Devise a Cyber Best Practice Toolkit for Space-Related Assets

The 2020 Cybers Security Strategy would benefit from the inclusion of an essential toolkit – outlining several basic cybersecurity measures which Australian space companies can implement. This may include a host of technical and non-technical guidelines, including:

- Mandating for standardised encryption standards for space-based assets – This is important in ensuring a minimum compliance standard and improving clarity, thus competently ensuring the integrity of data and safeguarding the privacy and reputation of stakeholders.

- Questioning how satellite operators are securing their satellite and ground-based networks - [51] Today's challenge is to ensure that an entity's entire ecosystem is safeguarded by the highest security posture, and able to withstand constant attacks from determined state actors.

- Requirements for an information assurance plan – All satellite operators need to take a systematic defence-in-depth approach to detect, prevent and mitigate attacks. Satellite operators and their ecosystem partners must therefore have separate plans to deal with cyber security – ensuring that the security and monitoring of the framework remains centrally managed and controlled by the satellite operator.

- Incorporating fall-back measures to ensure that the satellite portion of a network remains available during an attack – A satellite provider should incorporate in its service's high availability and resiliency, which may include standby satellite operation centres.

- Intelligence and threat awareness[52] – Satellite operators must stay abreast of increasingly sophisticated and power cyberattacks. This would be enhanced via an operator's information assurance program; which would be preventative in possessing countermeasures to block threats, detective in identifying threats with

[51] Safety4Sea, '4 cyber security questions to ask your satellite services provider' on Safety4Sea (18 October 2019) <https://safety4sea.com/4-cyber-security-questions-to-ask-your-satellite-services-provider/>.
[52] Marlink, 'CYBER SECURITY QUESTIONS YOU SHOULD ASK YOUR SATELLITE SERVICE PROVIDER' on Marlink (18 October 2019) <https://marlink.com/cyber-security-questions-for-satellite-service-provider/>.

intelligence sources, manage access and authentication to information, and manage the integration of countermeasures.

- Urging caution in the integration of new technologies – Including blockchain, machine learning, 5G and artificial intelligence. While the hardware to support such advanced computations is readily available, the rush to adopt may cause organisations to ignore basic cybersecurity tenants and the benefits of robust software implementation.

A best practice toolkit may also address specific security for Australian satellite ground systems. A choke point exists for both cyber and space technologies within ground systems, where the transfer and translation of data occurs. These systems carry vulnerabilities where they receive waivers from security updates due to perceived "performance issues" with the satellite, or operate on slower updates schedules due to contracts or operational constraints. [53]

iv) Recognize Both Space and Cyber as Critical Infrastructure Sectors

All satellites depend on cyber technology – including software, hardware, firmware and other digital components. Any non-kinetic threat to a satellite's control systems or available bandwidth poses a direct challenge to Australia's national critical infrastructure. [54] The Australian government's definition of critical infrastructure as:[55]

> *"those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of the nation or affect Australia's ability to conduct national defence and ensure national security"*

Examples of critical infrastructure as defined by the TISN encompass the 8 interlinked essential service sectors on which communities rely during their daily lives – including banking and finance, government, communications systems, energy, good and grocery, health, transport and water. [56]

It has been noted that the federal government is in the process of drafting laws which would permit cyber-intelligence agencies such as the Australian Signals Directorate to intervene on behalf of critical infrastructure providers should they come under cyberattack from overseas. Such laws are imagined enabling the Australian government to step in and mount cyber counterattacks on behalf of Australian entities. [57]

---

[53] David Hanson, 'Mitigating Cyber Security Risk in Satellite Ground Systems' on Defense Technical Information Center (April 2015) <https://apps.dtic.mil/dtic/tr/fulltext/u2/1012754.pdf>.
[54] Beyza Unal, 'Cybersecurity of NATO's Space-based Strategic Assets' on Chatham House (July 2019) <https://www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf>.
[55] TISN, 'Critical Infrastructure' on TISN (2019) <https://www.tisn.gov.au/Pages/Critical_infrastructure.aspx>.
[56] TISN, 'Critical Infrastructure' on TISN (2019) <https://www.tisn.gov.au/Pages/Critical_infrastructure.aspx>.
[57] John Davidson, 'Cyber 'Pearl Harbour' laws desperately needed, experts say' on Financial Review (29 October 2019) <https://www.afr.com/technology/cyber-pearl-harbour-laws-desperately-needed-experts-say-20191027-p534r4?fbclid=IwAR2uPRKqsmkYXkqs8WeD61LcfdQIcNcoQ0csK-ziLB51mB0dWp57lbvi5Ck>.

In legitimising the intervention of the ASD in mounting counter cyber-operations following a cyberattack upon Australia's space-based assets, the 2020 Cyber Security Strategy must thus advocate for the recognition of both space and cyberspace as elements of Australia's national critical infrastructure.

v) Intra and Extra-Governmental Cooperation

Australia can leverage its reputation as a developed middle power in providing leadership on cybersecurity in outer space, through adopting a comprehensive regulatory framework for the commercial space sector. Where Australia has revealed its capacity to conduct offensive cyber operations since 2016 and is an active member of the five eyes intelligence community, we are uniquely positioned to addressing non-kinetic threats to space operations. [58]

Addressing cybersecurity concerns in space represents a complex multi-agency effort given its wide-reaching implications. This necessitates joint cooperation between the Department of Home Affairs, the Australian Signals Directorate, the ACSC, the TISN, the ACMA, and the ASA. The Prime Minister must also instruct these agencies to make cybersecurity a priority in their space collaborations with the private sector.

Accordingly, the 2020 Cyber Security Strategy must invite closer inter-agency cooperation, promote the free exchange of information, and invite comments from both the cyber security and commercial space sector in crafting a comprehensive response to cyber security threats in space. [59]

vi) Expand Cyber-Specific Insurance to Cover Space-Related Assets

Where the Launches and Returns Act provides for the holder of a launch permit to possess insurance for a maximum amount of $100 million,[60] the creation and regulation of an insurance framework for cyber security matters in outer space must be considered indispensable in creating a stable and risk-managed commercial environment conducive to widespread access and economic prosperity.

Accordingly, the Lloyd's Market Association (LMA) has recognized that there is an urgent need for insurers to address the potential of a cyber-attack on satellites, launch vehicles or ground-based control systems. LMA has recently proposed model policy clauses in response to the publication of expectations relating to cyber insurance from the U.K. government, and these clauses serve as a guideline for insurers, brokers and satellite operators and can be modified as needed. [61]

The provision of tailored insurance services across this niche area is pivotal in keeping commerce moving, imbuing confidence within lenders, introducing a peace of mind through the shifting of risk, ensuring family and business stability, and in protecting start-ups and small business owners. The federal government must thus

---

[58] Tom Uren, 'Australia's offensive cyber capability' on ASPI (10 April 2018) <https://www.aspistrategist.org.au/australias-offensive-cyber-capability>.
[59] David Fidler, 'Cybersecurity and the New Era of Space Activities' on Council on Foreign Relations (3 April 2018) <https://www.cfr.org/report/cybersecurity-and-new-era-space-activities>.
[60] McGill and Ye, above n26.
[61] Richard Parker, 'Op-ed | If hackers cripple your satellite, are you covered? Don't count on it.' on Spce News (18 September 2019) <https://spacenews.com/op-ed-an-insurers-perspective-on-defining-cyber-risk-in-space/>.

advocate for the consideration of an insurance framework or requirement specifically addressing the specific issue of cyber security in space for Australian entities within the contents of its 2020 Cyber Security Strategy.

vii) Adherence with International Laws and Principles

Australia's status as an intermittent member of the ITU Council since 1959 emphasizes our nation's unique position to address the unique cyber security challenges faced by space-based assets. [62] The ITU represents the international regulator and specialized agency of the UN responsible for matters concerning information and communications technologies – comprised of 196 member states. Australia is required to uphold its duties and obligations under the ITU Constitution, ITU Convention, the ITU Radio Regulations, and International Telecommunications Regulations. [63]

Consequently, our cyber security posture in space would be heightened where the 2020 Cyber Security Strategy specified the need for TSPs to adhere to the volume of recommendations issued by the ITU-R – among which include recommendations on security issues in network management of digital satellite systems (Recommendation ITU-R S.1250) and performance enhancements of transmission control protocol over satellite networks (Recommendations ITU-R S.1711). [64]

International customary principles contained within the Tallinn Manual 2.0, covering the occurrence of cyber operations directed against space-related cyber infrastructure for malicious purposes, must also be heeded. The Tallinn Manual represents a non-binding set of principles covering cyber conflicts and cyber warfare, which will prove indispensable in tailoring an offensive cyber response by the Australian government to an attack on our national critical infrastructure.

Of particular note would be Rule 58(b) and Rule 59(b) of the manual - specifying how cyber operations in space are subject to limitations on the use of force in international law, and how cyber operations in space must be conducted with due regard for the need to avoid interference with peaceful space activities of other states. [65] The importance of adhering to the rule of law in responding to cyber threats in outer space must therefore be highlighted within the contents of the Australia's 2020 Cyber Security Strategy.

[62] Department of Communications and the Arts, 'ITU Plenipotentiary Conference 2018 Outcomes' on Australian Government (2018) <https://www.communications.gov.au/what-we-do/internet/itu-plenipotentiary-conference-2018-outcomes>.
[63] Michael N. Schmitt and Liis Vihul, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017) 285.
[64] ITU, 'Securing Radiocommunications' on ITU (2019) <https://www.itu.int/en/action/cybersecurity/Pages/radiocommunications.aspx>.
[65] Schmitt and Vihul, above n57, 273-277.

5. Summary

Recognizing the immense potential and risks associated with cyber security upon Australia's space-based assets and infrastructure, the federal government must take lead in instilling the importance of cybersecurity across Australia's space sector as part of the 2020 Cyber Security Strategy - in safeguarding our collective national security and economic prosperity within the 21st century.

Accordingly, it is imperative for the federal government to facilitate joint industry and government communication and collaboration, advance responsible cyber security guidelines across the space sector, and promote Australia's cyber security posture and resilience amongst the stars.

The following questions and responses follow upon the series of 26 questions included within the "call for views" pamphlet in relation to Australia's 2020 Cyber Security Strategy. The questions selected below represent the most pertinent points of information in relation to cyber-specific risks to Australia's space-related assets.

Question No.1 - What is your view of the cyber threat environment? What threats should government be focusing on?
The cyber threat environment is one which is wrought by risks enabled by the mass proliferation of IoT devices. With the number of IoT connected devices projected to increase from 14.2 billion to 25 billion between 2019 to 2025, [66] the government must maintain active awareness of its increasing attack surface in space based assets and infrastructure, and encourage increased discussion and industry collaboration in plugging this cyber vulnerability before it becomes unmanageable.

Where it may already be too late to legislate and enforce a prohibition on the potential use of such affordable and widely available disruptive technologies to target Australia's space-related assets, organisations must organise to identify which commercially available tools pose the most risk, revise countermeasures to such risks and boost overall cyber resilience, and clarify a clear remediation plan for victims.

Question No.4 - What role should Government play in addressing most serious threats to Australian institutions and businesses?
The government must take policy action in introducing standards and regulations concerning the need for cybersecurity precautions across the Australian space sector. This is imperative in protecting our national critical infrastructure, safeguarding our collective national security, and precluding an ultimate calamity.

The government must thus assume the role of a regulator and consultative body in fostering the creation of a best practice tool kit for cyber security amongst Australia's space-related assets, in devising an enforcement framework to facilitate resilience across our cyber security posture in space, in maintain an awareness of the dynamic cyber risk environment, and in assisting critical infrastructure sectors which have been targeted.

[66] Casey Crane, '20 Surprising IoT Statistics You Don't Already Know' on Hashedout (4 September 2019) <https://www.thesslstore.com/blog/20-surprising-iot-statistics-you-dont-already-know/>.

Question No.7 – What role can government/industry play in supporting the cyber security of consumers?
The government must play the role of both regulator and educator. This involves regulating how private industry approaches the issue of cyber security in the context of space, enforcing a set compliance standard, and levelling penalties where entities are non-compliant. Where the regulatory environment surrounding cyber in space is in its infancy, the formation of a voluntary industry best practice guideline must form the foundational basis for future government legislation within the area.

The government may also act as an educator in engaging with Australian companies and start-ups throughout the space sector, alerting them to their cybersecurity risks within their activities, and organising public forums and consultations between government and industry.

Question No.12 - What needs to be done so cyber security is 'built in' to digital goods and services?
The federal government advocate for the creation of specific standards for encryption within the transmission of data covering space-based assets within the contents of the 2020 Cyber Security Strategy. This must be conducted in tandem with the emergence of an insurance framework covering cyber related risks in space. The formation of such standards for entities throughout the space industry would form the basis for consumer expectations concerning the standard of services expected from start-up satellite operators.

Achieving this will require coordination with the ACCC and relevant enforcement bodies to tailor the contents of the *Competition and Consumer Act 2010* (Cth) to protect the interests and safety of consumers, support fair trading in the commercial space sector, promote the economically efficient operation of infrastructure, undertake market studies, and specify for specific cyber security standards in the provision of space related services.

Question No.19 – How could we approach instilling better trust in ICT supply chains?
Within an increasingly globalizing world, supply chain networks are comprised of multiple businesses and organisations - each comprising a key node within an interconnected system. Herein the element of trust is paramount in insuring the integrity of the ICT supply chain, particularly given the often vast geographical distances and often obfuscated nature of supply chains.

Trust is particularly important given the use of electronic components in systems across government departments and critical infrastructure sectors - including water, transportation, energy, and healthcare. This highlighted in October 2018 following a Bloomberg report, revealing how China was able to infiltrate 30 US multinational companies by compromising their ICT supply chain. It was advanced that Chinese manufacturing subcontractors were able to introduce an innocuous microchip across server motherboards, allowing attackers to create a stealth doorway into any network that included the altered machines. [67]

[67] Bloomberg, 'The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies' on Bloomberg (4 October 2018) <https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies>.

Consequently, instilling better trust across Australia's ICT supply chians for both the government and private businesses requires that the following measures be adopted:[68]

1) Training and fostering talent within the supply chain security area - An organisation's CISO/security manager develop trust and credibility with management, and collaborate with them on supply chain security;
2) Engaging in asset management, vulnerability assessment, and configuration control - This is premised on portfolio management, involving the discovery of all supply chain partners, and a regular assessment of vulnerabilities and detection of changes in exposure.
3) Scaling multiple supply chain risk assessment approaches - Engaging a mix of techniques may be necessary to support business responsiveness demands, and to enable continuous monitoring of risk levels.
4) Extend dashboards and reporting to business units and IT managers – Involving the use of supply chain processes and tools to provide visibility into current risk views to non-security personnel, and enabling them to incorporate risk info in their decision-making.
5) Communication with vendors – Involving providing feedback to encourage all suppliers to adopt higher quality processes, and weeding out low-quality suppliers.

[68] John P. Mello, '5 keys to protect your supply chain from cyberattacks' on CSO (5 November 2019) <https://www.csoonline.com/article/3449238/5-keys-to-protect-your-supply-chain-from-cyberattacks.html>.