SATELLITES ARE CYBER INSECURE: WE NEED REGULATION TO AVOID A DISASTER

EDWARD VERCO*

The cybersecurity of satellites requires significant improvement. Smallsats and CubeSats present particular vulnerabilities to cyberattacks, predominantly due to their minimal construction costs for commercial entities. The deployment of thousands of satellites in constellations overcrowds low Earth orbit, which, coalesced with the presence of military satellites, provides attractive opportunities for malicious actors. Compromising a satellite could result in substantial economic disaster, as well as loss of life. Private corporations have failed to engage with cybersecurity, potentially due to a lack of awareness. This is compounded by the cost of adequately securing their satellites against cyberattacks and the absence of regulation. This is an immediate practical problem that requires urgent action.

Employment of further encryption, such as quantum encryption, will significantly harden the cybersecurity of satellites against these risks. Alternative solutions include the development of laser-based communication and concerted focus on strengthening both intrusion detection systems (IDS) and intrusion prevention systems (IPS). Enforcement of such measures is required, and hence, improvement to the regulatory regime regarding the cybersecurity of satellites must urgently be enacted. Current international space law does not adequately address issues of cybersecurity and does not protect satellites from cyberthreats. An international multilateral space cybersecurity regime should be developed, which could be implemented by initially engaging existing intergovernmental organisations. Australia can demonstrate its value as a global leader in space cybersecurity regulation by developing its own comprehensive domestic system, requiring a minimal level of cybersecurity for all satellites. Australia's capabilities in high-technology cybersecurity position the nation favourably to develop a sophisticated regime of cybersecurity regulation for satellites.

* (LLB, BIS, GDLP) is a law graduate of the University of Adelaide and a lawyer admitted to practice in the Supreme Court of South Australia. He is currently employed as a Contracts Management Associate at Lockheed Martin Australia, and his research areas of interest include regulation in the space and cybersecurity sectors, as well as the defence industry in general.

I BACKGROUND

A *Introduction*

Dependence on satellites has never been greater. The global impact of satellites on societies is evidenced by their range of capabilities, including communication, internet access and observation of Earth for weather and military purposes. In fact, a 'critical portion of cyberspace can only be provided by space operations'.[1]

However, satellites are becoming increasingly vulnerable to cyberattacks, which intensifies the risk of large-scale disasters. Cybersecurity competencies for satellites are advancing but currently require significant installation costs.[2] Further, due to the competitive nature of the private sector and pressures to maximise profit, companies willingly or otherwise manufacture and deploy thousands of satellites that are fundamentally exposed to cyberthreats.[3] Regulation of private corporations, both at the international and domestic levels, fails to ensure these satellites are adequately protected from cyberattacks.[4] It is only a matter of time before this results in a disaster of dramatic proportions.

It pays to be prepared for the unexpected. While critics may argue that a major cyberattack of a satellite is yet to occur, it is imperative that the prospect is anticipated and acted upon. It had been previously hypothesised that a global pandemic could affect the world in a significant way.[5] However, the theory did not receive the necessary attention and funding for preparation.[6] As a result, COVID-19 has devastated the world since early 2020, resulting in crippling economic consequences and substantial loss of life.[7] The cyber vulnerability of satellites

[1] Cherian Samuel and Munish Sharma, *Securing Cyberspace: International and Asian Perspectives* (Pentagon Press, 2016) 158.
[2] David E Cunningham, Geancarlo Palavicini Jr and Jose Romeo-Mariona, 'Towards Effective Cybersecurity for Modular, Open Architecture Satellite Systems' (Conference Paper, AIAA/USU Conference on Small Satellites, 6 August 2016) 5.
[3] David P Fidler, 'Cybersecurity and the New Era of Space Activities', *Council on Foreign Relations* (online, 3 April 2018) <https://www.cfr.org/report/cybersecurity-and-new-era-space-activities>.
[4] Deborah Housen-Couriel, 'Cybersecurity Threats to Satellite Communications: Towards a Typology of State Actor Responses' (2016) 128 *Acta Astronautica* 409, 414.
[5] Robin Marantz Henig, 'Experts Warned of a Pandemic Decades Ago. Why Weren't We Ready?' *National Geographic* (online, 8 April 2020) <https://www.nationalgeographic.com/science/article/experts-warned-pandemic-decades-ago-why-not-ready-for-coronavirus>.
[6] Ibid.
[7] Ibid.

presents the potential for a similar crisis, which must be avoided by the urgent implementation of regulatory mechanisms.

B *Outline*

Firstly, this article will identify the key characteristics of satellites, including their differing capabilities and classifications due to size, types of orbital locations and which states are responsible for their production and launch. This section will also discuss the satellites currently orbiting the Earth and likely future development trends. Emphasis will be placed on constellations currently being launched, such as SpaceX's Starlink,[8] and their properties, as well as the increasing development of 'smart' satellites.

Following this will be a comprehensive examination of how satellites are inherently vulnerable to cyberattacks. This will explore how the individual segments of a satellite system and perilous commercial practices contribute to satellites' vulnerability. The presence of military satellites and the difficulty of detection for those who compromise satellites serve as incentives for potential malicious actors. These incentives will also be discussed.

Improvements regarding adequate methods of hardening the cybersecurity of satellites will then be explored, focusing on developing encryption, such as quantum encryption. Laser-based communication will be examined as an alternative, as will other suggested practices, including an emphasis on constructing strong IDS and IPS.

Lastly, the importance of regulation will be examined concerning the enforcement of adequate cybersecurity practices for satellites. This section will first explain the current international legal regime and its obsolete applicability to the capabilities of satellites in 2021. It will then focus on two proposals for improved regulation. The first will explore a comprehensive international mechanism that could be applied to existing intergovernmental bodies,[9] or the establishment of an international multidisciplinary space cybersecurity regime. Alternatively, the

[8] The Starlink satellite constellation is discussed in section II.B, including an examination of its purpose and the number of proposed satellites. Further information can be found at: Adam Mann, 'Starlink: SpaceX's Satellite Internet Project', *Space.com* (online, 29 May 2021) <https://www.space.com/spacex-starlink-satellites.html>.

[9] The existing intergovernmental bodies are discussed in section V.B, but of particular relevance are the United Nations Committee on the Peaceful Uses of Outer Space (COPUOS) and the North Atlantic Treaty Organisation (NATO).

potential for states to develop their domestic regulatory mechanisms presents the opportunity for Australia to propel itself as a global leader—if it employs such a regime effectively.

The article then draws conclusions regarding the required improvement of cybersecurity for satellites. A number of recommendations are made to reduce the risk of disaster occurring.

II SATELLITE CAPABILITIES

To comprehend the cyber vulnerabilities of satellites, it is integral to understand their classifications and capabilities. This section will explain the differing sizes, orbital locations and functions used to classify satellites. It then examines constellations and 'smart' satellites.

A *Classification*

NASA establishes that the term 'satellite' refers to a moon, planet or machine that orbits a planet or star.[10] This means that Earth itself is actually a satellite in constant orbit of the sun.[11] However, this article will focus on the function of human-constructed satellites, as 'artificial space-based objects' that collect and transmit information while in orbit of Earth.[12] Each satellite, generally, possesses an antenna to send and receive information and a power source.[13] Satellites operate as part of a system including at least one ground station, used to transmit and receive data, and generally use radiofrequency waves as communications links through which the data is transmitted.[14]

1 *Size*

As evidenced in Table 1, the size of satellites is an aspect of their classification. Large satellites weigh more than 1,000 kg, medium satellites between 500 and 1,000 kg, and the term 'small satellite' or 'smallsat' refers to any satellite weighing less than 500 kg.[15] Smallsats are classified further in Table 1 and comprised 43 per cent of satellites launched in 2018.[16] A CubeSat is

[10] Dan Stillman, 'What is a Satellite?' *NASA* (Web Page, 13 February 2014) <https://www.nasa.gov/audience/forstudents/5-8/features/nasa-knows/what-is-a-satellite-58.html>.
[11] Ibid.
[12] SSI Governance Group, *2019 Space Security Index* (Library and Archives Canada, 16th ed, 2019) 161.
[13] Ibid.
[14] Ibid.
[15] Ibid.
[16] Tara Halt and Anna Wieger, 'Smallsats by the Numbers 2019', *Bryce Space and Technology* (Presentation, 2019) <https://brycetech.com/reports/report-documents/Bryce_Smallsats_2019.pdf> 5.

constructed by using up to 12 modular cubes, each measuring 10 cm.[17] Between 2012 and 2018, more than 70 per cent of the 1,300 smallsats launched were CubeSats.[18] Over half of these were to provide commercial services.[19] This is predicted to continue into the future as it is expected that commercial CubeSats, with artificial intelligence applied to them, are the future of worldwide satellite use.[20]

Table 1.

Classification of satellites due to their mass

Category		Weight
Large satellite		>1,000 kg
Medium satellite		500-1,000 kg
SmallSats	Minisatellite	100-500 kg
	Microsatellite	10-100 kg
	Nanosatellite	1-10 kg
	CubeSat	Composed of 1-12 modular 10 cm cubes
	Picosatellite	100 g-1 kg
	Femtosatellite	10-100 g
	Attosatellite	1-10 g
	Zeptosatellite	0.1-1 g

Note: This table was generated by the author using information from SSI Governance Group, *2019 Space Security Index* (Library and Archives Canada, 16th ed, 2019) 161.

[17] Ibid 6.
[18] Ibid 4.
[19] Ibid.
[20] Massimiliano Pastena, *SmartSat CRC Distinguished Speaker Series* (Webinar, SmartSat CRC, 4 June 2020).

2 *Orbital Locations*

The height at which a satellite orbits impacts how often it completes one whole revolution of Earth and, therefore, how it can be used to transmit information.[21] The terms 'apogee' and 'perigee' are important when discussing satellite orbit. Apogee refers to the furthest distance from Earth during orbit, and perigee is the closest point to Earth that the satellite reaches.[22] Table 2 presents information regarding orbits and their corresponding characteristics.

Table 2.

Types of Earth orbits

Orbit	Altitude Above Earth	Time Per Revolution	Common Uses
Low Earth Orbit (LEO)	<2,000 km	approx. 90 mins	Remote sensing, Earth observation, constellations for broadband communication
Medium Earth Orbit (MEO)	2,000-36,000 km	2-12 hours	Global navigation
Geostationary Orbit (GEO)	approx. 36,000 km	24 hours (equal to Earth)	Communication, large-scale weather observation
Highly Elliptical Orbit (HEO)	Low-altitude perigee and extremely high-altitude apogee	Varied, but visibility exceeding 12 hours at apogee	Polar communication, missile early warning

Note: This table was generated by the author using information from SSI Governance Group, *2019 Space Security Index* (Library and Archives Canada, 16th ed, 2019) 162.

Table 3 explores the locations of the 3,372 currently operational satellites as of 1 January 2021. The majority of satellites (77.5%) are located in Low Earth Orbit (LEO), which is followed by an

[21] SSI Governance Group (n 12) 161.
[22] Ibid 163.

additional 16.7 per cent in Geostationary Orbit (GEO), and few remaining in Medium Earth Orbit (MEO) and Highly Elliptical Orbit (HEO).[23] There is demand for orbit space in LEO due to the locational advantages of these satellites and their consequent ability to transmit information efficiently.[24]

Table 3.

Orbital location of currently operational satellites

Orbit	Altitude Above Earth	Percentage of Total Satellites in Orbit
Low Earth Orbit (LEO)	2,612	77.5%
Medium Earth Orbit (MEO)	139	4.1%
Geostationary Orbit (GEO)	562	16.7%
Highly Elliptical Orbit (HEO)	59	1.7%

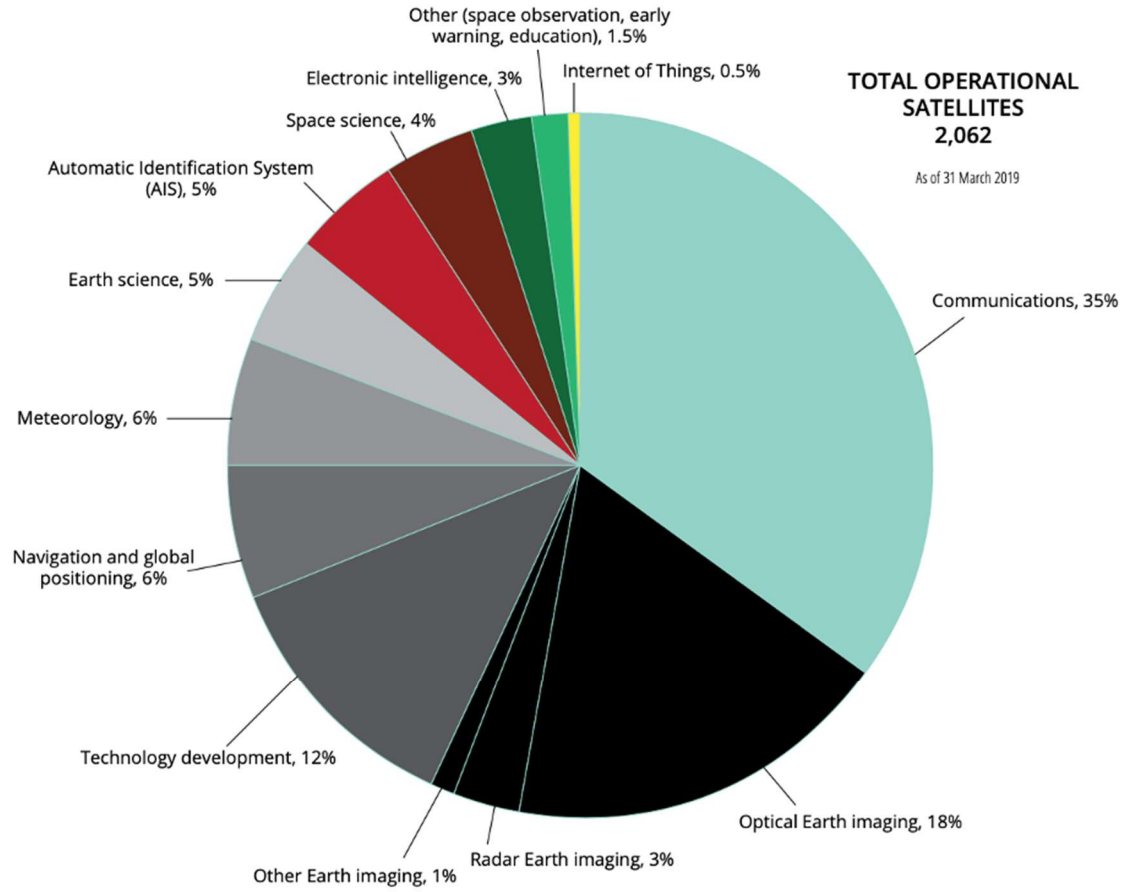
Note: This table was generated by the author using information from Union of Concerned Scientists, 'UCS Satellite Database', *UCSUSA* (Article, 1 January 2021) <https://www.ucsusa.org/resources/satellite-database>.

3 *Functions*

Satellites are further classified in relation to their variety of functions. Figure 1 illustrates that as of 31 March 2019, 35 per cent of functional satellites were used for communications, comprising the largest proportion.[25] This is followed by optical Earth imaging (18%) and technology development (12%).[26] These trends have been reflected by the satellites launched since the graphic was produced.[27]

[23] Union of Concerned Scientists, 'UCS Satellite Database', *UCSUSA* (Web Page, 1 January 2021) <https://www.ucsusa.org/resources/satellite-database>.
[24] Ibid.
[25] SSI Governance Group (n 12) 164.
[26] Ibid.
[27] Union of Concerned Scientists (n 23).

Figure 1. Functions of operational satellites



Note: Reproduced from SSI Governance Group, *2019 Space Security Index* (Library and Archives Canada, 16th ed, 2019) 164.

4 *Attribution*

Satellites can be further classified by their launching state. As of January 2021, a staggering 1,897 (56%) currently operational satellites had been launched from the United States of America (US).[28] This is more than four times the next-prominent state, being China with 412 (12%).[29] Over half (54%) of the operational satellites are for commercial use, which is projected to increase even further.[30] State-operated satellites form the second and third largest attributions for government (16.4%) and military (12.7%) uses, respectively.[31]

[28] Ibid.
[29] Ibid.
[30] Ibid.
[31] Ibid.

5 *Australia's Role*

Australia has a significant, albeit small, role in the history of space technology and regulation. Australia became only the seventh state in the world to build and launch its own satellite when it launched the Weapons Research Establishment Satellite from Woomera onboard a modified US Sparta LV rocket in 1967.[32] In 2017, three Australian CubeSats developed by researchers at Australian universities, including the University of Adelaide, became part of the European Union's QB50 program launch of 50 satellites.[33] On 19 April 2017, they were deployed to the International Space Station (ISS).[34] Importantly, on 19 September 2020, Australia launched its first commercial space-capable rocket from the Koonibba Test Range in South Australia.[35] Australia has a long history of providing ground station services to operators such as the US military,[36] as well as being a member of the United Nations (UN) Committee on the Peaceful Uses of Outer Space (COPUOS) since 1958.[37] However, as a nation, it remains uncertain about its place in the space supply chain.[38]

There remains an opportunity for Australia as a growing leader in cybersecurity, and a trusted technologically advanced state, to become a prominent spacefaring nation.[39] This is typified by the Government of South Australia's announcement of a proposed satellite launch from South Australia in mid-2022.[40] A role of the Australian Space Agency is to anticipate the

---

[32] Allan Forbes, 'A Historical Perspective on WRESAT' (2018) 6(1) *Australian Journal of Telecommunications and the Digital Economy* 118, 120.
[33] ANU College of Science, 'Australian-Built Satellites Launched into Space', *The Australian National University* (Web Page, 2017) <https://science.anu.edu.au/news-events/news/australian-built-satellites-launched-space>.
[34] Ministers for the Department of Industry, Science, Energy and Resources, 'Aussie CubeSats Launched Towards International Space Station' (Media Release, 19 April 2017).
[35] Stephen Kuper, 'Lift-Off for Australia's First Commercial Space Capable Rocket', *Space Connect* (online, 21 September 2020) <https://www.spaceconnectonline.com.au/launch/4536-lift-off-for-australia-s-first-commercial-space-capable-rocket>.
[36] Matthew James, *Australia in Orbit: Space Policy and Programs* (Current Issues Briefs 1997–98 No 12, 6 April 1998).
[37] United Nations Office for Outer Space Affairs, 'Committee on the Peaceful Uses of Outer Space: Membership Evolution', *UNOOSA* (Web Page, 15 February 2021) <https://www.unoosa.org/oosa/en/ourwork/copuos/members/evolution.html>.
[38] Melissa de Zwart, 'No Launch from Australia: Something is Missing from Our Plans for the New Space Race', *The Conversation* (online, 12 June 2018) <https://theconversation.com/no-launch-from-australia-something-missing-from-our-plans-for-the-new-space-race-97924>.
[39] David Soldani, 'On Australia's Cyber and Critical Technology International Engagement Strategy Towards 6G: How Australia May Become a Leader in Cyberspace' (2020) 8(4) *Journal of Telecommunications and the Digital Economy* 127.
[40] Isabel Dayman, 'South Australia to Launch its Own Satellite to "Cement Place" in Space Sector, Premier says', *ABC News* (online, 20 January 2021) <https://www.abc.net.au/news/2021-01-20/south-australia-to-launch-satellite-in-space-sector-milestone/13072378>.

issues that will likely face the space sector in the future.[41] Hence, it must not neglect the cyber vulnerability of these proposed satellites.[42] Further, Australia's International Cyber Engagement Strategy 2019 Progress Report states that its goal is for a strong and resilient cybersecurity posture for Australia, the Indo-Pacific and the global community.[43] Setting a global example regarding the cybersecurity of satellites would be an effective means of achieving this goal.

B *Development of Constellations*

A growing trend is the launching of thousands of smallsats in LEO to create a constellation of satellites. In a constellation, each smallsat is able to communicate with the other satellites and the ground station on Earth.[44] Data indicates a recent increase in the deployment of CubeSats in large constellations for high-volume data collection and observation.[45] It is predicted that these constellations will inevitably present new challenges to the long-term sustainability of the space environment.[46] For example, the Science Applications International Corporation estimates that a constellation in excess of 4,000 satellites would generate 64 million collision warnings per year for spacecraft within that constellation alone.[47] Later in the article, it will be explored how satellite constellations possess qualities that make them exceptionally vulnerable to the risk of cyberattacks.

Of particular relevance is the Starlink constellation, launched by the US-based commercial entity, SpaceX. On 16 February 2021, SpaceX launched its nineteenth bulk Starlink launch, meaning the constellation currently has 1,081 satellites in LEO.[48] SpaceX proposes to launch a total of

---

[41] Rebecca Cowan-Hirsch, 'KPMG's 30 Voices on 2030, Part Four: Space Data Comes Back to Earth' (Webinar, American Chamber of Commerce in Australia, 25 June 2020).
[42] Ibid.
[43] Department of Foreign Affairs and Trade, *Australia's International Cyber Engagement Strategy* (Progress Report, March 2019) 22.
[44] Zulfikar Abbany, 'SpaceX's Starlink Satellite Internet: It's Time for the Tough Talk on Cyber Security in Space', *Deutsche Welle* (online, 21 February 2018) <https://www.dw.com/en/spacexs-starlink-satellite-internet-its-time-for-tough-talk-on-cyber-security-in-space/a-42678704>.
[45] Joel Lisk and Melissa de Zwart, 'Watch This Space: The Development of Commercial Space Law in Australia and New Zealand' (2019) 47(3) *Federal Law Review* 444, 449.
[46] Ibid 455.
[47] Owen Brown et al, Science Applications International Corporation, *Orbital Traffic Management Study*: *Report on Space Traffic Management Assessments, Frameworks and Recommendations* (Final Report, 21 November 2016) E1.
[48] Stephen Clark, 'SpaceX Successfully Deploys 60 Starlink Satellites, but Loses Booster on Descent', *SpaceFlight Now* (online, 16 February 2021) <https://spaceflightnow.com/2021/02/16/spacex-successfully-deploys-60-more-starlink-satellites-but-loses-booster-on-descent/>.

11,943 minisatellites, each weighing approximately 260 kg, over the next decade.[49] The purpose of Starlink is to deliver high-speed, low-latency broadband internet to 'near global coverage of the populated world in 2021'.[50] As evidenced in Table 4, Starlink is the largest planned constellation, possessing nearly four times as many satellites as a similar proposal by Amazon.

Table 4.

Top 10 largest proposed satellite constellations

Company name	Country	Number launched	Planned size	First launch	Purpose	Status
SpaceX	United States	62	4,425 7,518	2018	Internet	Prototype(s) launched
Amazon	United States	0	3,236	N/A	Internet	Prototype development
SatRevolution	Poland	1	1,024	2019	Earth Observation	Prototype(s) launched
Galaxy Space	China	0	1,000	2019	Internet	Unknown
OneWeb	United States	6	648	2019	Internet	Prototype(s) launched
EarthNow	United States	0	500	N/A	Earth Observation	Unknown
Hongyan (CASC)	China	1	320	2018	Internet	Prototype(s) launched
KLEO (Kaskilo, eightyLEO)	Germany	0	300	N/A	IoT/M2M*	Unknown
Efir/Sfera	Russia	0	288	N/A	Internet & Earth Observation	Unknown
Telesat	Canada	2	117 117	2017	Internet	Prototype development
Sky and Space Global	United Kingdom & Israel	3	200	2017	IoT/M2M*	Prototype(s) launched

* *IoT/M2M means Internet of Things/Machine to Machine communication*
Note: Whilst this table was based on 2018 statistics, the 'Planned Size' information is still relevant. Reproduced from SSI Governance Group, *2019 Space Security Index* (Library and Archives Canada, 16th ed, 2019) 19.

[49] Mann (n 8).
[50] Starlink, 'High Speed Internet Across the Globe', *Starlink* (Web Page, 2020) <https://www.starlink.com/>.

C *Emergence of 'Smart' Satellites*

Another development of satellites is the proposal of 'smart' satellites, where satellites contain onboard learning machines on miniaturised satellite systems.[51] Australia possesses the capabilities to become a global leader in this underdeveloped area. This comes after the Australian Office of National Intelligence issued a request for tender seeking a provider of research and engineering services for the development, test, launch and operation of a prototype smart satellite.[52] Australia has an opportunity to develop a significant aspect of worldwide satellite capabilities. However, it must first establish adequate cybersecurity regulation. This is because if smart satellites reflect current artificial intelligence technology on Earth, they will be further vulnerable to cyberattacks. Adequate mechanisms would therefore be required to stabilise such vulnerabilities.

III CYBER VULNERABILITIES OF SATELLITES

American multinational technology conglomerate Cisco defines cybersecurity as the 'practice of protecting systems, networks, and programs from digital attacks'.[53] Such cyberattacks are typically intended to access, change or destroy sensitive information, extort money from users or interrupt normal business processes.[54] Cybersecurity is becoming increasingly challenging as there are more 'hackable' devices than people on Earth, a trend that will only continue as the population grows alongside malicious actors' technological advancements.[55] It will now be explored why satellites are particularly vulnerable to cyberattacks and how the consequences could be detrimental.

[51] Sandy Milne, 'Office of National Intelligence Seeks "Smart" Satellites', *Space Connect* (online, 7 May 2020) <https://www.spaceconnectonline.com.au/operations/4328-office-of-national-intelligence-seeks-smart-satellites>.
[52] Office of National Intelligence, 'Prototype National Intelligence Community Smart Satellite System (NICSAT)', *Aus Tender* (Request for Tender, ONI 024/2020, 4 May 2020) <https://www.tenders.gov.au/Atm/ShowClosed/1f724e25-68a1-41fe-be2f-20bcd3bcd89e?PreviewMode=False>.
[53] Cisco, 'What is Cybersecurity', *Cisco* (Web Page, 13 February 2020) <https://www.cisco.com/c/en_au/products/security/what-is-cybersecurity.html>.
[54] Ibid.
[55] Ibid.

A *Contributing Characteristics of the Satellite System*

The multiple segments that form a satellite system contribute significantly to its cyber vulnerability. A space system comprises four segments: space, ground, link and user.[56] The different components to the satellite systems simply provide more targets for cyber intrusion.[57] A satellite system's predominant function is to transmit information, while a primary objective of hacking is to intercept information.[58] The specific threats associated with the four segments are displayed in Table 5.

[56] Brandon Bailey et al, 'Defending Spacecraft in the Cyber Domain' (Research Paper, Center for Space Policy and Strategy, November 2019) 1, 2.
[57] SSI Governance Group (n 12) 112.
[58] Swapnil Sayan Saha, Shafizur Rahman and Mosabber Uddin Ahmed, 'Ensuring Cyberspace Telemetry and Telecommand in Small Satellites: Recent Trends and Empirical Propositions' (2019) 10 *IEEE A&E Systems Magazine* 34.

Table 5.

Individual cyber threats to segments of a space system

Segment	Cyber Threats
Space Segment	Command intrusion Payload control Denial of service Malware
Ground Segment	Spoofing Denial of service Malware
Link Segment	Command intrusion Spoofing Replay
User Segment	Hacking Hijacking Malware

Note: This table was generated by the author using information from Brandon Bailey et al, 'Defending Spacecraft in the Cyber Domain', [2019] (November) *Center for Space Policy and Strategy* 1, 2.

Table 6 explains many of the aforementioned threats and other types of electronic interference with space systems. Each of these presents a critical risk to satellites, ultimately demonstrating their inherent cyber vulnerability.

Table 6.

Types of interference with space systems

Common name	Description
Malware	A portmanteau of 'malicious' and 'software', typically used as a catch-all term to refer to any software designed to cause damage to a single computer, server, or computer network, whether it is a virus, spyware et al.
Orbital jamming	A beam of contradictory signals directed toward a satellite, which then mixes, overriding legitimate signals and blocking their transmission.
Terrestrial jamming	Rather than target a satellite itself, terrestrial jamming directs rogue frequencies to ground-based targets, such as consumer-level satellite dishes, and distorts their transmission accordingly.
Hijacking	The unauthorised use of a satellite for transmission, or seizing control of a signal, such as a broadcast, and replacing it with another.
Spoofing	Spoofing devices create false GPS signals to fool receivers into thinking that they are a different location and/or time.
Scanning	A process for identifying, attacking, and stealing information from a targeted host.

Note: This table was generated by the author, using information from Robert Moir, 'Defining Malware FAQ', *Microsoft* (online, 1 April 2009) <https://docs.microsoft.com/en-us/previous-versions/tn-archive/dd632948(v=technet.10)?redirectedfrom=MSDN> and SSI Governance Group, *2019 Space Security Index* (Library and Archives Canada, 16th ed, 2019) 112.

B *Denial of Vulnerability*

Private and public entities repeatedly believe that satellite systems are sufficiently cybersecure, predominantly because a disaster has yet to occur.[59] This belief is fundamentally incorrect and insidiously dangerous, as it creates an environment in which commercial bodies continue to ignore the importance of hardening their satellites against cyberattacks.[60] Any component of an integrated system, such as space, can be manipulated, particularly if connected to a network.[61] Less than a decade ago, it appeared implausible that malicious actors could employ refrigerators, digital video recorders and other devices to compromise Twitter, Netflix and Spotify, as they did

[59] Fidler (n 3).
[60] Ibid.
[61] Samuel and Sharma (n 1) 159.

in 2016.[62] History, therefore, suggests a major cyberattack on a satellite will occur.[63] Consequently, it would be prudent to pre-emptively implement the necessary precautions rather than merely await such an attack.[64]

C *Perilous Commercial Practices*

The perilous actions of many commercial entities compound the cyber vulnerabilities of satellites. Malicious actors target satellites as commercial entities favour lower operational costs over increased cybersecurity spending.[65] This vulnerability is particularly evident in smallsats as the low-cost, 'off-the-shelf' technology required for production correlates directly to the absence of onboard cybersecurity services.[66] It is also suggested that as the cost of developing smallsats decreases, their complexity and cost to harden for cybersecurity increases.[67] Therefore, adequate cybersecurity often out-costs the satellites themselves.[68] Even for companies with intentions to implement adequate cybersecurity, it often becomes uncommercial and hence not sufficiently achieved.[69] Therefore in practice, many private commercial entities, knowingly or otherwise, develop their satellites as vulnerable to cyberattacks.[70]

Many cybersecurity non-specialists and satellite enthusiasts in the commercial sector simply do not appreciate the cyber-related risks associated with launching smallsats.[71] This is partially because smallsat operators traditionally favour innovation over management solutions.[72] This reflects the argument that commercial entities recognise a dramatic cyberbreach of a satellite is yet to occur and therefore falsely believe against the essentiality of protecting against hypothetical attacks.[73] The increasing volume of satellites in orbit increases the risk associated

---

[62] Nicky Woolf, 'DDoS Attack that Disrupted Internet was Largest of its Kind in History, Experts say', *The Guardian* (online, 27 October 2016) <https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet>.
[63] Debra Werner, 'Small Satellite Sector Grapples with Cybersecurity Requirements, Costs', *SpaceNews* (online, 8 August 2018) <https://spacenews.com/small-satellite-sector-grapples-with-cybersecurity-requirements-cost/>.
[64] Woolf (n 62).
[65] Bailey et al (n 56) 1.
[66] Ibid.
[67] Cunningham, Palavicini and Romeo-Mariona (n 2) 2.
[68] William Akoto, 'Hackers Could Shut Down Satellites – Or Turn Them into Weapons', *The Conversation* (online, 13 February 2020) <https://theconversation.com/hackers-could-shut-down-satellites-or-turn-them-into-weapons-130932>.
[69] Ibid.
[70] Bailey et al (n 56) 4.
[71] Saha, Rahman and Ahmed (n 58) 36.
[72] Ibid 34.
[73] Bailey et al (n 56) 1.

with the collision of any two satellites, which is also a risk for corporations.[74] This information is presented in Table 7 and emphasises the increasing requirement for hardened cybersecurity.

Table 7.

Increasing risk of satellite collision

Year	Risk of Collision Occurring
2018	3%
2021	10%
2033	50%

Note: This table was generated by the author, using information from Swapnil Sayan Saha, Shafizur Rahman and Mosabber Uddin Ahmed, 'Ensuring Cyberspace Telemetry and Telecommand in Small Satellites: Recent Trends and Empirical Propositions' (2019) 10 *IEEE A&E Systems Magazine* 34, 34.

D *Military Uses of Space*

The presence of military satellites in space dramatically increases the range of potential consequences if a cyber intrusion were to occur. Minor intrusions would include malicious actors simply shutting down satellites and denying access to their services.[75] However, the ability to jam or spoof signals from military satellites could create significant disruption for critical infrastructure, including electric grids, water networks and transportation systems.[76] The presence of thrusters onboard military satellites presents further catastrophic possibilities for malicious actors, allowing them to control direction and collide with other satellites, the ISS or objects on Earth.[77] Such detrimental consequences evidently make the possibility of compromising a military satellite attractive for potential malicious actors.

Article IV of the *Outer Space Treaty* ('*OST*'), which will be discussed in depth later in the article, prohibits the presence of any nuclear weapons or weapons of mass destruction

[74] Saha, Rahman and Ahmed (n 58) 34.
[75] Akoto (n 68).
[76] Ibid.
[77] Ibid.

(WMD) in orbit or on a celestial body.[78] However, the provision has not been interpreted to prevent the transit of WMD through space or the placement or use of non-WMD weapons in outer space.[79] The presence of these WMDs provides further incentive for malicious actors to compromise satellites, as it compounds the level of destruction that could eventuate.[80] Increased access to these satellites facilitates an amplified opportunity for aggression.

Commercial satellites are increasingly used for military purposes; this meshing of satellite uses contributes to their targeting for cyberattacks.[81] Most satellite technology is capable of dual military and commercial use, demonstrating the entrenched attraction for potential malicious actors.[82] Current uses of space were developed initially for military purposes, denoting that military interests are historically linked to satellite use.[83]

Electronic warfare is also developing as an international military issue because of a state's ability to compromise other states' satellites.[84] For example, the integration of electronic warfare capabilities into the Russian ground and aerospace forces, and navy, have resulted in widespread allegations of jamming in its conflicts with Ukraine and Syria.[85] Moreover, Chinese defence academics have articulated the requirement to possess capabilities for attacks to 'blind and deafen the enemy,' according to the US Department of Defense 2020 China Military Report to Congress.[86] These propositions, coalesced with subsequent US accusations of China attacking their satellites, demonstrate how capabilities to cause detrimental outcomes result from the cyber vulnerability of satellites.[87] Further, in August 2020, a US Department of Defense satellite was hacked during DEFCON, a convention hosted by the US Air Force and Defense Digital Service,

[78] *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies*, opened for signature 27 January 1967, 610 UNTS 205 (entered into force 10 October 1967) ('*Outer Space Treaty*') art IV.
[79] Melissa de Zwart, 'Outer Space' in William H Boothby (ed), *New Technologies and the Law in War and Peace* (Cambridge University Press, 2018) 337, 345.
[80] Fidler (n 3).
[81] David Livingstone and Patricia Lewis, 'Space, the Final Frontier for Cybersecurity?' (Research Paper, Chatham House International Security Department, September 2016) 21.
[82] Fabio Tronchetti, 'Legal Aspects of the Military Uses of Outer Space' in Frans von der Dunk and Fabio Tronchetti (eds), *Handbook of Space Law* (Edward Elgar, 2015) 331, 332.
[83] de Zwart (n 79) 349.
[84] SSI Governance Group (n 12) 113.
[85] Ibid.
[86] United States of America Department of Defense, 'Military and Security Developments Involving the People's Republic of China' (Annual Report to Congress, 21 August 2020) 65.
[87] Fidler (n 3).

in an attempt to discover vulnerabilities before their adversaries.[88] This would imply that malicious actors possess the capabilities to compromise even the most robust of military satellites.

On 19 December 2019, the US founded its sixth branch of the US Armed Forces, the Space Force.[89] This exemplifies the evolving theme regarding the militarisation of space, which intensifies risks for all stakeholders in the sector.[90] General David Thompson proposes that military satellites, of utmost importance to the Space Force, will require the greatest possible cybersecurity measures to avoid being compromised.[91] Military uses of space demand attention as a nuclear detonation in space remains the most significant threat to Earth linked to the space sector.[92] This could be caused by cyberattacks, implying that the cybersecurity of military satellites remains of significant importance.[93]

E *Difficulty of Detection*

The insidious nature of compromising a satellite makes it appealing to potential malicious actors. Cyberattacks are difficult to detect and attribute due to the proprietary nature of the software onboard both the satellite itself and the ground station.[94] Cyberattacks are also difficult to distinguish from unintentional interference and, hence, are regularly conducted without detection.[95] Plausible deniability can also be used as a defence and contributes to the favourability of cybercrime.[96] Even the most significant compromises of satellites, including a breach on NASA in 2008, require years of investigation to locate the source, albeit imprecisely.[97] Further, NASA reported 1,500 cyber incidents in 2016, with thousands more likely unreported.[98] Without the implementation of adequate measures, detection is almost impossible.[99] In practice, what might become the most potentially detrimental crimes facing the world are likely to be untraceable. It

[88] B David Harley, 'DEF CON Hackers Compete to Hijack a Satellite in Orbit', *Freethink* (online, 10 August 2020) <https://www.freethink.com/technology/hacking-satellites>.
[89] SpaceNewsInc, 'Space Force Gets Down to Business presented by Lockheed Martin' (YouTube, 24 April 2020) 00:02:00–00:27:00 <https://www.youtube.com/watch?v=fjA3RE_Hvno&t=133s>.
[90] Fidler (n 3).
[91] SpaceNewsInc (n 89).
[92] Bailey et al (n 56) 5.
[93] Ibid.
[94] Cunningham, Palavicini and Romero-Mariona (n 2) 2.
[95] SSI Governance Group (n 12) 112.
[96] Samuel and Sharma (n 1) 159.
[97] Akoto (n 68).
[98] SSI Governance Group (n 12) 113.
[99] Bailey et al (n 56) 9.

is obvious, therefore, why such a crime is attractive for potential malicious actors, with minimal probability of detection and consequent punishment.

IV HARDENING SATELLITES AGAINST CYBERATTACKS

It is evidently important to harden the cybersecurity of satellites. Differing methods of how this could be achieved will now be explored.

A *Improved Encryption*

Seemingly, the most commonly proposed mechanism for improving the cybersecurity of satellites is to upgrade encryption techniques. This could be effectively achieved through employing quantum encryption, asserted to be 'theoretically unbreakable and unconditionally secure'.[100] Therefore, the continued development of quantum encryption applicable for smallsats presents the greatest security chance against cyberattacks.[101] Quantum encryption allows for 'more secure protocols for the authentication, integrity, and confidentiality of exchanged signals'.[102] This is most efficiently achieved through photon subtraction, a process that ensures the communication sent via the satellites is incredibly difficult to compromise.[103]

These schemes, including quantum key distribution (QKD), have been frequently proposed and tested.[104] An example is the SpooQySat program that attempts to develop a constellation of QKD-protected CubeSats.[105] The recent development of QKD capabilities to effectively secure CubeSats is relatively successful, and the first specialised CubeSat QKD mission is estimated to occur 'very soon'.[106] In addition, a dedicated quantum receiver, such as a Quantum Encryption and Science Satellite, has been extensively tested for almost a decade and is now considered viable.[107] Subsequently, the Canadian Space Agency has committed to launching a satellite in 2022 that will 'demonstrate the use of quantum technology for protecting

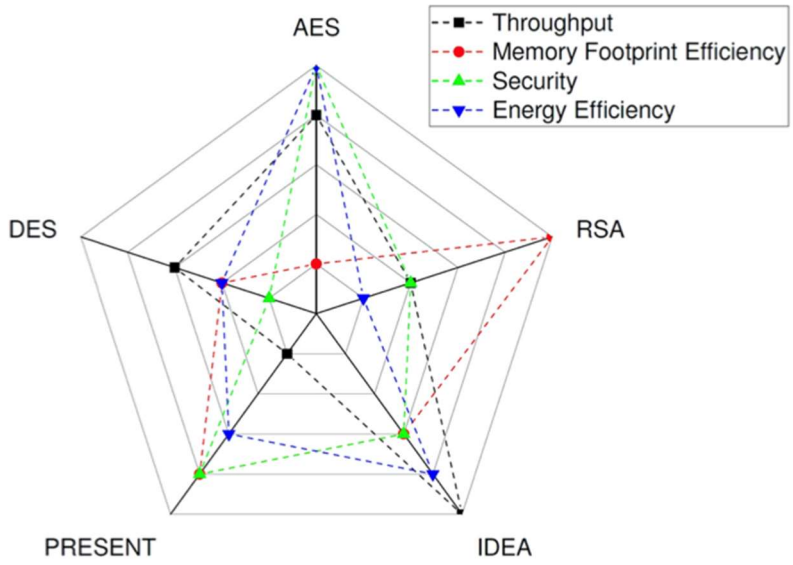
[100] Saha, Rahman and Ahmed (n 58) 37.
[101] Ibid.
[102] SSI Governance Group (n 12) 117.
[103] Mingjian He, Robert Malaney and Jonathon Green, 'Quantum Communications via Satellite with Photon Subtraction' (Research Paper No 978-1-5386-4920-6/18, Institute of Electrical and Electronic Engineers, 2018).
[104] Saha, Rahman and Ahmed (n 58) 37.
[105] James A Grieve et al, 'SpooQySats: CubeSats to Demonstrate Quantum Key Distribution Technologies' (2018) 151 *Acta Astronautica* 103, 103.
[106] Ibid 106.
[107] Thomas Jennewein, 'Towards Quantum Communications with Satellites' (Research Paper No 978-1-5386-5343-2/18, University of Waterloo Department of Physics and Astronomy & Institute for Quantum Computing, 2018).

commercial and national communication networks'.[108] For context, China launched the world's first quantum-enabled satellite in August 2016, named Micius.[109] It is believed that the US is developing capabilities of this nature at a similar rate, but its information on quantum encryption development remains predominantly classified.[110]

Alternatively to quantum encryption, there are currently many encryption techniques already suitable for smallsats, including the Advanced Encryption Standard (AES).[111] The five most effective encryption techniques are the AES, Data Encryption Standard, Rivest-Shamir-Adleman, International Data Encryption Algorithm and PRESENT cyphers.[112] Figure 2 compares the five cyphers, with AES being the most comparably favourable method in terms of balancing the four most desirable qualities: throughput, memory footprint efficiency, security and energy efficiency.[113] Therefore, it is suggested that AES encryption be employed while quantum encryption is further developed and tested.[114]

[108] David Pugliese, 'Honeywell to Build Canadian Quantum Encryption Satellite', *SpaceNews* (online 28 June 2019) <https://spacenews.com/honeywell-to-build-canadian-quantum-encryption-satellite/>.
[109] Saha, Rahman and Ahmed (n 58) 37.
[110] SSI Governance Group (n 12) 117.
[111] Saha, Rahman and Ahmed (n 58) 37.
[112] Ibid.
[113] Ibid 45.
[114] Ibid.

Figure 2. Rankings of proposed cyphers



Note: A graphic ranking from 1 to 5 of the proposed cyphers in four areas based on empirical results, where higher is more desirable. Reproduced from Swapnil Sayan Saha, Shafizur Rahman and Mosabber Uddin Ahmed, 'Ensuring Cyberspace Telemetry and Telecommand in Small Satellites: Recent Trends and Empirical Propositions' (2019) 10 *IEEE A&E Systems Magazine* 34, 45.

B *Laser-Based Communication*

An alternative to strengthening the cybersecurity of satellites themselves is the introduction of laser-based communication. It is suggested that laser-based capabilities 'could be a revolution in communication, both on Earth and across the solar system'.[115] If developed effectively, this would provide a viable alternative to satellite radio communication and, ultimately, greater protection from conventional jamming techniques, as well as faster communications.[116]

In August 2018, Aerospace Corporation's Optical Communication and Sensor Demonstration mission successfully tested a laser signal from a CubeSat in LEO.[117] This

[115] Donald Cornwell, 'Space-Based Laser Communications Break Threshold', *Optics & Photonics News* (online, May 2016) <https://www.osa-opn.org/home/articles/volume_27/may_2016/features/space-based_laser_communications_break_threshold/>.
[116] SSI Governance Group (n 12) 114.
[117] Dianna Ramirez, 'Laser Communications Demonstrated from CubeSats for the First Time', *The Aerospace Corporation* (Web Page, 2 August 2018) <https://aerospace.org/press-release/laser-communications-demonstrated-cubesats-first-time>.

spacecraft was able to transmit data 50 times faster than conventional communication techniques.[118] The demonstration establishes the viable possibility of using laser communications for large volumes of Earth observation data.[119] Before this, the European Data Relay System had attempted space-to-space communications instead of the more vulnerable space-to-Earth links.[120] However, there remain numerous challenges associated with laser-based communication, the most prominent of which is the degradation of signals through atmospheric turbulence and cloud cover.[121]

C *Other Improvements*

There are several additional proposed alternatives for hardening satellites against cyberattacks.

1 *IDS and IPS*

Smallsats, due to their increased vulnerability, must examine the employment of encryption. However, differing practices may be more effective for traditional spacecraft.[122] Arguably, the most integral aspect of ensuring a cybersecure satellite is the combination of a robust IDS and IPS.[123] The IDS implements both 'signatures- and machine-learning based anomaly detection techniques' to identify when a cyberattack is imminent or in progress.[124] The existence of an effective IDS can be essential to the avoidance of zero-day attacks, which occur when a cyberattack transpires on the same day a weakness is discovered in the software.[125] Zero-day attacks are a critical issue in cybersecurity and are generally considered the highest priority of malware detection.[126] The IPS, integrated into the existing onboard spacecraft fault management system, then employs automated actions to return the spacecraft to its known cyber safe mode, thus blocking any possible known cyberattack.[127]

---

[118] Ibid.
[119] SSI Governance Group (n 12) 116.
[120] Ibid 114.
[121] Cornwell (n 115).
[122] Bailey et al (n 56) 11.
[123] Ibid 12.
[124] Ibid.
[125] Kaspersky Lab, 'What is a Zero-Day Attack? Definition and Explanation', *Kaspersky Lab* (Web Page, 2021) <https://usa.kaspersky.com/resource-center/definitions/zero-day-exploit>.
[126] Jin-Young Kim, Seok-Jun Bu and Sung-Bae Cho, 'Zero-Day Malware Detection Using Transferred Generative Adversarial Networks Based on Deep Autoencoders' (2018) 460 *Information Sciences* 83, 84.
[127] Bailey et al (n 56) 9.

2 *Supply Chain Risk Management Program*

The implementation of a supply chain risk management program is also essential to a satellite's cybersecurity.[128] This would include how critical units and subsystems are identified and addressed independently from non-critical units and subsystems.[129] Further, all hardware and software acquisitions should be sourced from trusted vendors as part of an agreed-upon chain of custody.[130] The configuration management process should then thoroughly vet all the software, ensuring the mitigation of unintended weaknesses.[131]

3 *Development at Each Phase*

In 2016, the US Naval Information Warfare Center Pacific (formerly Space and Naval Warfare Systems Center Pacific) launched a five-year capability development effort to infuse cybersecurity technology into each phase of the smallsat lifecycle.[132] Table 8 demonstrates the individual measures that would be taken at each phase of the smallsat's development. While these suggested implementations are relatively expensive, it must be noted that the cost in response to any global disaster would be significantly more substantial.[133]

[128] Ibid 10.
[129] Ibid.
[130] Ibid.
[131] Ibid.
[132] Cunningham, Palavicini and Romero-Mariona (n 2) 2.
[133] Ibid 3.

Table 8.

The US Naval Information Warfare Center Pacific's ACTION laboratory cybersecurity objectives

Lifecycle Phase	Cybersecurity Overlay
Concept design	Survey hardware and software vulnerabilities Plan security controls
Payload and subsystem development	Incorporate security code and controls Graybox and blackbox testing of subsystem interfaces
Bus, payload, and ground subsystem acceptance	Static-dynamic analysis of payloads, buses Reverse engineering of subsystems and protocols
System-level integration and testing	Dynamic analysis and testing of communications interfaces, signals interference, interception, and injection
Launch, on-orbit operation, and maintenance	Monitor and defend network health

Note: This table was generated by the author, using information from David E Cunningham, Geancarlo Palavicini Jr and Jose Romeo-Mariona, 'Towards Effective Cybersecurity for Modular, Open Architecture Satellite Systems' (Conference Paper, No SSC16-IV-6, 30th Annual AIAA/USU Conference on Small Satellites, 2016) 3.

4 *Logging*

Lastly, logging all collection and storing of data over a period is essential to hardening satellites.[134] Logging enables the analysis of events and actions of the system during that period.[135] Both the spacecraft and ground station should independently perform their command logging and anomaly detection for cross-validation, which can identify an intrusion efficiently.[136]

[134] Bailey et al (n 56) 11.
[135] Ibid.
[136] Ibid.

V REGULATION

These proposed improvements should be employed to harden the inherent cyber vulnerabilities of satellites. However, of greater importance is the implementation of these measures through a significantly enhanced regulatory regime. Australia could play an effective role in developing this regulation at both the domestic and international levels.

A *Current International Legal Framework*

1 *Outer Space Treaty*

The *OST*, which entered into force in 1967, forms the basis for all international law in space.[137] Integrally for the operation of satellites, article VI provides that 'activities of non-governmental entities in outer space ... shall require authorisation and continuing supervision by the appropriate State Party to the Treaty'.[138] This attributes responsibility to the states for the regulation of the commercial entities who launch satellites into space.[139] Article VII provides: a state 'that launches or procures the launching of an object into outer space ... is internationally liable for damage to another [state]'.[140] Responsibility and liability remain two fundamental principles of international space law.[141]

2 *Liability Convention*

The *Liability Convention*, enacted in 1972, essentially expands upon article VII of the *OST* in attributing liability for the state responsible for launching a 'space object' in the event that it causes damage to any aspect of another state.[142] This is likely to be interpreted as applicable to satellites in the event that they collide with another object either in space or on Earth.[143]

---

[137] *Outer Space Treaty* (n 78).
[138] Ibid art VI.
[139] Frans von der Dunk, 'Liability versus Responsibility in Space Law: Misconception or Misconstruction?' (1991) 43 *Space, Cyber, and Telecommunications Law Program Faculty Publications* 363.
[140] *Outer Space Treaty* (n 76) art VII.
[141] von der Dunk (n 139) 363.
[142] *Convention on International Liability for Damage Caused by Space Objects*, opened for signature 29 March 1972, 961 UNTS 187 (entered into force 1 September 1972) ('*Liability Convention*') art II.
[143] Housen-Couriel (n 4) 412.

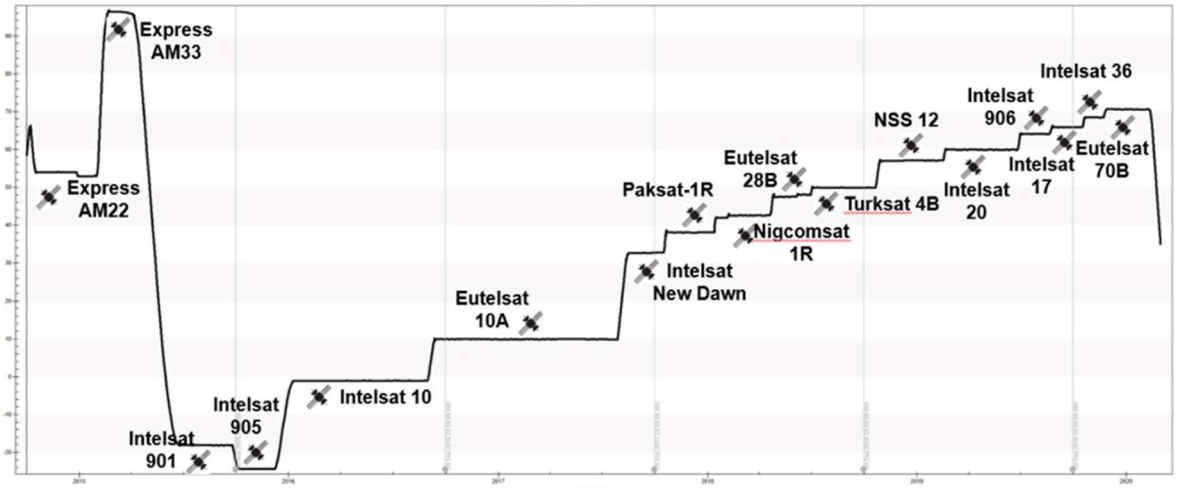
3 *UN Charter and Use of Force*

A critical issue for consideration will be whether a rendezvous and proximity operation (RPO), which may involve a cyber intrusion of satellites, constitutes a 'use of force' as defined by international law. If so, such action likely violates article 2(4) of the *UN Charter* and hence could be enforced with the existing mechanisms.[144] An example of an RPO is Russia's Luch/Olymp satellite, launched into GEO in 2014.[145] After its initial launch, it later drifted, meaning at certain times, it came within 10 kilometres of two US orbiting commercial satellites.[146] The Secure World Foundation establishes that the Luch/Olymp satellite has 'parked' near more than a dozen commercial communications satellites, typically close enough to be within standard ground terminal uplink windows (see Figure 3).[147] The term 'Luch' refers to a common type of civil communications satellite, whereas the Russian Government's decision to use the name 'Olymp' fuels suspicion that the satellite is used for military intelligence.[148] It is arguably emblematic of a growing uncertainty concerning states' intentions in space.[149] If the exercise of such RPOs, which likely facilitate cyber intrusions of other satellites, is to be defined as a use of force, RPOs could be prohibited and states consequently punished in accordance with article 2(4) of the *UN Charter*.[150] However, it is uncertain how interpretation of this provision will develop in the future.

---

[144] *Charter of the United Nations* art 2(4) ('*UN Charter*').
[145] Thomas G Roberts, 'Unusual Behaviour in GEO: Luch (Olymp-K)', *Aerospace Security* (online, 30 March 2020) <https://aerospace.csis.org/data/unusual-behavior-in-geo-olymp-k/>.
[146] Chris Zappone, 'Luch/Olymp Rogue Russian Satellite Symbolises New Worries about Space Peace', *The Sydney Morning Herald* (online, 24 November 2015) <https://www.smh.com.au/technology/lucholymp-rogue-russian-satellite-symbolises-new-worries-about-space-peace-20151123-gl59of.html>.
[147] Secure World Foundation, *Global Counterspace Capabilities: An Open Source Assessment* (April 2020) 2–9.
[148] Zappone (n 146).
[149] Ibid.
[150] *Charter of the United Nations* art 2(4).

Figure 3. Luch/Olymp's Orbital History



Note: A compilation of Luch/Olymp's orbital history and satellites visited since its launch in 2014. The *y*-axis demonstrates the satellite's latitude, and the *x*-axis the time since its launch. Reproduced from Secure World Foundation, *Global Counterspace Capabilities: An Open Source Assessment* (April 2020) 2-9.

4 *Criticisms of International Legal Framework*

The current international regime can be criticised in several ways.[151] First, there are genuine concerns regarding the 'lack of cybersecurity standards and regulations for commercial satellites' in the US and internationally.[152] The current legal regime is significantly outdated, predominantly because its drafting occurred when global space activities were dominated by two states, the US and the Soviet Union.[153] The space sector in 1967 was substantially different from its current form, with more than 80 states and hundreds of private companies now involved in the space industry.[154] Further, the international legal framework fails to address cybersecurity threats in any effective capacity. It must be modernised to achieve this and mitigate the aforementioned inherent risks.

Regulation generally reflects the 'antithesis of innovation and the exploitation of the commercial opportunity', resulting in a considerable gap in international recognition of cybersecurity threats.[155] The current regime leaves companies to safeguard themselves against

[151] Donna Lawler, 'Commercial Space Law: Launch and Operation of Spacecraft' (2020) 42(2) *Law Society Bulletin* 22, 23.
[152] Akoto (n 68).
[153] Steven Freeland, 'Challenges for the Future International Regulation of Space Activities: Space Law in a Changing Technological Paradigm' (2020) 42(3) *Law Society Bulletin* 16.
[154] Ibid.
[155] Livingstone and Lewis (n 81) 12.

potential cyberattacks, which is not achieved in practice.[156] International law's applicability to outer space and cyberspace requires urgent amending.[157] The change enacted must be appropriate for the current issues facing cybersecurity of satellites and envisage what is likely to be relevant in the future.[158]

B *Proposed International Regulation*

There are a number of proposals pertaining to how the regulation of hardened cybersecurity in space can be improved at an international level.

1 *Utilising Existing Organisations and Laws*

The utilisation of existing international organisations and laws could improve regulation worldwide. The *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* ('*Tallinn Manual 2.0*') should be considered as a guideline to clarify international law's current application in cyberspace.[159] Rule 60 of the *Tallinn Manual 2.0* could be applied, which provides '[a] State must authorise and supervise the cyber 'activities in outer space' of its non-governmental entities', and that '[c]yber operations involving space objects are subject to the responsibility and liability regime of space law'.[160] Through enacting these guidelines, improved regulation could be applied to the international function of cybersecurity laws within the states individually.[161] Any contravention of this would consequently result in that state breaching international law.[162]

The North Atlantic Treaty Organisation (NATO) has recognised the necessity to adopt a space policy and concluded that without such measures at a regulatory level, disaster is imminent.[163] However, there are difficulties associated with reaching a comprehensive multilateral agreement, meaning NATO could be used as an existing intergovernmental organisation to pursue collaboration on space cybersecurity.[164] By utilising NATO, as well as bilateral cooperation between spacefaring nations such as India, Japan and the European Space Agency,

---

[156] Akoto (n 68).
[157] Housen-Couriel (n 4) 414.
[158] Freeland (n 153) 17.
[159] Michael N Schmitt et al, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017) 279.
[160] Ibid.
[161] Fidler (n 3).
[162] Ibid.
[163] Bailey et al (n 56) 4.
[164] Fidler (n 3).

increased awareness of cybersecurity threats could be achieved.[165] Australia could play a critical role in raising awareness, potentially partnering with the US to develop solutions to this integral issue.

Additionally, urgency is required in undertaking a comprehensive review of the international law relating to hostile acts directed at satellites.[166] Such change should occur in four applicable international law regimes: the UN Charter, space law, international telecommunications law and transborder freedom of information.[167] Elements of the existing regime, such as the registration system required by the International Telecommunications Union, must be reflected in the amended regime. The UN COPUOS could also be used to discuss the requirement for more cooperation on space cybersecurity. The UN COPUOS incorporates 95 member states who meet annually, including the US, Canada, Japan, Russia and the European Space Agency.[168] This may provide an integral forum for discussion by engaging many of the largest spacefaring nations with this issue.

2 *Developing a New Regime*

The proposal of a new multistakeholder international regime on cybersecurity in space, in place of amending current international law, demands attention.[169] It will be challenging to negotiate adequate regulatory guidelines between states at an international level when most actors are private corporations.[170] Therefore, all stakeholders must exchange ideas, knowledge and expertise to establish an effective regime.[171] A multistakeholder approach involving public–private cooperation may be warranted to ensure adequate cybersecurity standards.[172] The Organisation for Economic Co-operation and Development (OECD) endorses the plausibility of public–private partnerships in the space sector, citing recent examples of such projects in the fields of satellite communications, Earth observation and global navigation satellite systems.[173] As evidenced by the case studies, the OECD argues that early and comprehensive preparation by

[165] Ibid.
[166] Housen-Couriel (n 4) 414.
[167] Ibid 411.
[168] United Nations Office for Outer Space Affairs (n 37).
[169] Freeland (n 153) 16.
[170] Ibid 18.
[171] Ibid.
[172] Akoto (n 68).
[173] Organisation for Economic Co-operation and Development, *Evolving Public-Private Relations in the Space Sector* (OECD Publishing, June 2021) 28.

both the public and private sectors is paramount to the success of these partnerships within the space sector.[174]

There is a necessity for the space industry to develop new binding international standards.[175] It is questionable how it could be legal to populate significant portions of low Earth orbit without consulting any international regulatory body.[176] Governance of such issues could come at an international level as space is a global commons, similar to the high seas.[177] Interestingly, it is predicted that by 2030 an international regulatory body for space data will be established in addition to space possessing its own legal jurisdiction.[178] As the US Federal Communications Commission has permitted the current perilous satellite activity enacted by US entities such as SpaceX, domestic regulation of satellites could be interpreted as ineffective, and the requirement for international regulation is supported.[179]

This multidisciplinary approach to vulnerability assessment would ideally advocate for secure encryption as the most effective response to cyberthreats and an increased focus on network security, risk management, mitigation and resilience techniques.[180] However, it will be important to avoid rigid centralisation or overzealousness in the regulatory response. History suggests restrictive regulation will cause those in a market-driven sector to develop workarounds and, ultimately, harbour a general culture of cyber insecurity.[181] A non-hierarchical approach, where stakeholders are valued and empowered by knowledge, could implement the United Kingdom (UK)'s Space Agency's 10-step process (see Figure 4).

[174] Ibid 32.
[175] Abbany (n 44).
[176] Ibid.
[177] Ibid.
[178] KPMG, *30 Voices on 2030: The Future of Space* (KPMG Australia, May 2020) 9.
[179] Abbany (n 44).
[180] Livingstone and Lewis (n 81) 22.
[181] Ibid 24.

Figure 4. The UK Space Agency's 1-step process of engaging commercial entities with improvement to their cybersecurity measures

Note: This figure was generated by the author, using information sourced from David Livingstone and Patricia Lewis, 'Space, the Final Frontier for Cybersecurity?' (Research Paper, Chatham House International Security Department, September 2016).

After generating awareness in existing organisations, the ultimate goal should be to establish a new intergovernmental coordination mechanism for developing guidance on space cybersecurity.[182] This could be modelled on the Inter-Agency Space Debris Coordination Committee, which, comprised of several space agencies of major spacefaring nations, has been credited with reducing space debris produced by new launches.[183] This international multistakeholder regime that concentrates on cybersecurity in space should include industry,

[182] Fidler (n 3).
[183] Dr Hae-Dong Kim, 'What's IADC', IADC (Web Page, 2019) <https://www.iadc-home.org/what_iadc>.

government and international and non-governmental organisations.[184] Initial engagement with the UN Office for Outer Space Affairs (UNOOSA), which orchestrates the UN COPUOS, is the most effective strategy for developing the regulation on cybersecurity in the sector.[185] Existing international bodies such as the UN COPUOS can be utilised initially before creating a comprehensive, multistakeholder regime, with facilitated access for private entities.

C *Proposed Domestic Regulation*

Regulation of the cybersecurity of satellites could also be developed at a domestic level, and Australia can demonstrate further leadership in regulating the cybersecurity of satellites in this capacity. In February 2020, the Australian Cyber Security Centre released its 'Australian Government Information Security Manual' outlining a cybersecurity framework that organisations can employ to protect their systems and information from cyberthreats.[186] However, this directive fails to acknowledge the cybersecurity risks of satellites, providing the opportunity to establish a corresponding framework.

1 *Domestic Legislation*

Australia should encourage the US Congress to adopt a comprehensive regulatory framework for the commercial space sector.[187] This would provide commercial space enterprises with regulatory certainty while concurrently complying with article VI of the *OST*.[188] This legislation should emphasise the existing law on cybersecurity information sharing, provide government assistance to industry-led efforts on strengthening space cybersecurity, and facilitate public–private collaborations.[189] Australia is positioned to achieve similar results by enacting equivalent legislation and, therefore, become a leader in domestic regulation on commercial space cybersecurity. There has been substantial development in promoting commercial space activity during Scott Morrison's tenure as Prime Minister of Australia, such as opening the Australian

[184] Pavan Duggal, 'Cyber Security Law, Its Regulation and Relevance for Outer Space' (Conference Presentation, International Commission on Cyber Security Law, 17 November 2017).
[185] Ibid.
[186] Australian Cyber Security Centre (Cth), *Australian Government Information Security Manual* (2020) 1.
[187] Fidler (n 3).
[188] Ibid.
[189] Ibid.

Space Agency in Adelaide.[190] This is projected to be sustained in the future.[191] This support for the industry should now pivot to effective regulation.

The US is favourably situated to generate a comprehensive strategy on cybersecurity in space due to the former Trump Administration's priorities aligning with 'improving critical infrastructure cybersecurity, addressing security threats to space operations, and promoting commercial space activities'.[192] An example of this was the White House's release of the Space Policy Directive 5 (SPD-5) on 4 September 2020, intended to improve the cybersecurity of space systems.[193] SPD-5 outlines a set of best practices, albeit not firm requirements, that agencies and companies should follow to protect space systems from hacking and other cyberthreats.[194]

Australia currently regulates the space industry through the *Space (Launches and Returns) Act 2018* (Cth) ('the Act').[195] The Act requires approval for:

- launching a space object from Australia;
- returning a space object to Australia;
- launching a space object overseas (for Australian nationals with an ownership interest);
- returning a space object overseas (for Australian nationals with an ownership interest); and
- operating a launch facility in Australia.[196]

The Act itself makes no mention of cybersecurity. However, the *Space (Launches and Returns) (General) Rules 2019* (Cth) ('the Rules') do require a 'cybersecurity strategy' to be approved for launches and returns of the nature listed in section 4 of the Act.[197] The Rules were introduced in August 2019, which exemplifies the infancy of what should develop into a comprehensively

[190] Department of Industry, Science, Energy and Resources, 'Australian Space Agency opens in Adelaide' (Media Release, 19 February 2020) <https://www.industry.gov.au/news/australian-space-agency-opens-in-adelaide>; Department of Defence, 'Morrison Government invests in a new sovereign controlled satellite capability' (Media Release, 13 July 2020) <https://www.minister.defence.gov.au/minister/lreynolds/media-releases/morrison-government-invests-new-sovereign-controlled-satellite>.
[191] Ibid.
[192] Fidler (n 3).
[193] Jeff Foust, 'White House Issues Cybersecurity Space Policy', *SpaceNews* (online, 4 September 2020) <https://spacenews.com/white-house-issues-cybersecurity-space-policy/>.
[194] Ibid.
[195] *Space (Launches and Returns) Act 2018* (Cth).
[196] Ibid s 4.
[197] *Space (Launches and Returns) (General) Rules 2019* (Cth) r 22(2)(ii).

legislated regime in the near future. The *Space (Launches and Returns (High Power Rocket) Rules 2019* (Cth), which came into force on 30 June 2020, require a similar cybersecurity strategy for launches and returns involving high power rockets.[198]

Due to the increasing threat of cyberattacks, it is imperative to act now.[199] Domestic regulation should be pursued initially, as international action is traditionally slow.[200] Specifically, a comprehensive domestic regulatory framework could require satellite manufacturers to develop a common cybersecurity architecture, which could be identified using the aforementioned proposed improvements to harden satellites.[201] By applying a domestic emphasis, projects such as the US Naval Information Warfare Center Pacific ACTION laboratory's proposal of hardening each development phase of a smallsat can be enacted.[202] Further, through domestic regulatory standards, a 'no encryption, no fly' policy could be implemented more effectively than an initial international requirement.[203] This is a necessary precaution, particularly for smallsats that are likely to possess onboard propulsion systems.[204] If compromised in LEO, the propulsion systems present a significant opportunity for intentional collisions through the ability to move the satellite in space.[205]

The Australian Government should develop federal legislation that requires a minimum security standard for satellites during their manufacturing process. This would ensure that upon deployment by commercial entities, satellites are sufficiently hardened against potential cyber intrusion. Consequently, Australia would become the world leader in a domestic regulatory mechanism of this nature and encourage other spacefaring states to employ similar regimes. Australia could then present their regulatory approach at existing intergovernmental organisations, such as the UN COPUOS, and inspire other states to enact similar legislation.

---

[198] *Space (Launches and Returns) (High Power Rocket) Rules 2019* (Cth) r 29(2)(ii).
[199] Ibid.
[200] Akoto (n 68).
[201] Ibid.
[202] Cunningham, Palavicini and Romero-Mariona (n 2) 5.
[203] Andrew Kurzrok, Manuel Diaz Ramos and Flora Mechentel, 'Evaluating the Risk Posed by Propulsive Small Satellites with Unencrypted Communications Channels to High-Value Orbital Regimes' (Conference Paper, No SSC18-XI-05, 32nd Annual AIAA/USU Conference on Small Satellites, 2018) 8.
[204] Ibid 1.
[205] Ibid.

2 *Existing Domestic Bodies*

Engagement of the Space Information Sharing and Analysis Centre (Space ISAC) could assist in developing an effective domestic regime in the US.[206] Established in April 2019 as a non-profit organisation, with founding members including Lockheed Martin, the Space ISAC intends to partner with as many as 200 companies from the commercial, civil and national security space sectors.[207] The organisation aims to act as a link between the US government and the private sector, as is specifically endorsed by SPD-5.[208] Similar actions could be implemented using existing organisations in Australia. Currently, the SmartSat Cooperative Research Centre (SmartSat CRC) serves a comparable purpose in Australia as a consortium of industry and research organisations that will develop technologies to 'bootstrap' Australia's space industry.[209] Engagement with the SmartSat CRC and the Cyber Security Cooperative Research Centre will be extremely beneficial for Australia in this area as the organisations act as informers for the Australian Federal Government, based on the collective knowledge acquired by organisations in the space sector. Ultimately, Australia's development of a comprehensive regulatory framework could be achieved by effectively engaging existing entities.

VI RECOMMENDATIONS

To effectively counteract the impending cyberthreats facing satellites, Australia must follow the below recommendations.

(1) The development of quantum encryption should be encouraged and applied to satellites whenever possible.
    a. AES encryption should be favoured while quantum encryption is developed; and
    b. other methods, such as laser-based communication, should continue to be explored as viable alternatives to radio frequency communication.

---

[206] Sandra Erwin, 'Space Industry Group Focussed on Cybersecurity to Begin Operations in Spring 2020', *SpaceNews* (online, 23 January 2020) <https://spacenews.com/space-industry-group-focused-on-cybersecurity-to-begin-operations-in-spring-2020/>.
[207] Ibid.
[208] Ibid.
[209] SmartSat Cooperative Research Centre, 'About Us', *SmartSat CRC* (Web Page) <https://smartsatcrc.com/about/about-us-2/>.

(2) The Australian Government should develop a comprehensive domestic system for regulating the cybersecurity of satellites with sufficient jurisdictional interest. This would require a minimal level of cybersecurity for satellites and could build on the foundations set by the *Space Activities (Launches and Returns) (General) Rules 2019.*
(3) Australia should collaborate with other states bilaterally and through existing intergovernmental organisations, such as the UN COPUOS, to introduce an international multidisciplinary organisation that will develop a regime for regulating space cybersecurity.
(4) Private companies within the space sector should be encouraged to educate themselves about the risks associated with inadequate cybersecurity and ensure their satellites are hardened against potential intrusions.

VII CONCLUSION

It is evident that the cybersecurity of satellites requires significant improvement. Commercial entities' manufacturing and the deployment of smallsats present substantial vulnerabilities to cyberattacks. This results from the minimal funds required to develop the satellites and, conversely, the expensive cybersecurity costs. Constellations, such as SpaceX's Starlink, are deploying thousands of satellites into low Earth orbit. Their overcrowding of this orbit, coalesced with the presence of military satellites, creates conditions for malicious actors to orchestrate disasters, both economic and to loss of life. The difficulty of detecting such intrusions and the evolving possibilities of destruction make compromising a satellite increasingly achievable and attractive to potential malicious actors. Private corporations have traditionally failed to engage with cybersecurity, potentially due to a lack of awareness, coalesced with the cost of adequately securing their satellites against cyberattacks and the absence of regulation.[210]

It is proposed that greater encryption, such as quantum encryption, will significantly harden satellites against cyberattacks. AES encryption should be implemented in satellites as the most effective alternative while quantum encryption is developed. Other solutions include the advancement of laser-based communication and the increased focus on strong IDS and IPS systems.

[210] Bailey et al (n 56) 1.

The regulatory regime governing the cybersecurity of satellites must urgently be upgraded to ensure the enforcement of such measures. The current framework, featuring the *OST* and *Liability Convention*, does not adequately protect satellites from current cybersecurity threats. An international multidisciplinary space cybersecurity regime should be developed, which could be implemented by initially engaging the current intergovernmental organisations such as NATO and UNOOSA, which orchestrates the UN COPUOS. Before then, Australia could demonstrate its capability as a global leader in space cybersecurity regulation by establishing its own comprehensive legislative regime.

Like COVID-19, compromising a satellite could further significantly strain the global economy and cause loss of life. The potentially detrimental consequences of inadequately securing satellites against cyberattacks should alarm every citizen on Earth. Following the COVID-19 pandemic, the world must acknowledge that it cannot afford another crisis of this scale and, therefore, develop anticipatory mechanisms. We must learn from history and ensure that satellites are adequately cybersecure against potential attacks. It pays to be prepared for the unexpected.