AIR SPACE
ASPC's crowd-sourced blog
https://airpower.airforce.gov.au

Ogden, T, Air/Space Vol 2 BP27207741
Published: 29 August 2022

Satellite Security in New Space

Theodora Ogden[1,2,3]
[1]RAND Corporation, USA; [2]Center for Space Governance, USA; and [3]Arizona State University, USA

There is a growing threat to societies, and their critical infrastructure as more actors take to the skies. Satellites are essential to everyday lives, providing crucial data for navigation, communication, environmental monitoring and ensuring national security. Australian defence heavily relies on space-based systems for joint command, intelligence, communications, navigation, targeting and surveillance (Australian Department of Defence, 2016). However, the space domain is becoming increasingly 'congested, contested and competitive' (Eberhardt, 2019). A greater number of actors are entering space than initially thought possible. Private companies and countries that have not traditionally held space capabilities are striving for a presence in space. Satellites are important for economic development, for instance, in assessing the climate, monitoring natural disasters, locating resources, and enabling agricultural activities (Durrani, 2018). Commercialisation, lower technology costs and miniaturisation are key factors opening the domain to more players (Wrench, 2019). Though a more inclusive and equitable space is beneficial to all, certain risks remain.

The weaponisation of space and the development of anti-satellite systems pose a threat in terms of 'kinetic' attacks on satellites, e.g., from missiles and 'non-kinetic' attacks, which include jamming or cyber-attacks (Bellasio et al., 2021). In November 2021, Russia conducted weapons tests, eliminating one of its inactive satellites. As well as generating a ripple of concern around the international community, this show of strength blasted more than 1,500 pieces of debris into low orbit, adding to an increasingly dangerous space environment (Bugos, 2021). The United States (U.S.) Department of Defence, however, warns that the real threat comes from cyber, as one attack could target an entire network of hundreds of satellites, in contrast to the barrage of missiles required otherwise to disable such a constellation (Erwin, 2021). Cyber is relatively cheap, whereas it could cost more to physically destroy a satellite than to launch and operate the satellite itself (Erwin, 2021). As more commercial satellites enter the space domain, attackers may seek to target them, denying access to key services and jamming signals to disrupt critical infrastructures, such as electric grids, water networks, transport systems and supply chains (U.S. Senate Committee on Homeland Security and Governmental Affairs, 2022).

In 2014, the U.S. accused China of hacking its National Oceanic and Atmospheric Administration weather satellite (Flaherty et al., 2014). Although U.S. officials handled this particular attack relatively quickly and discretely, these satellites provide critical data for forecasts and warnings—their disruption could have a severe effect, especially during a climate event. The U.S. is not the only target, with several attacks on Australian systems in recent years. In 2016, foreign hackers attacked the systems of Newsat, a small Australian satellite company that had planned to launch two satellites and boost the Australian satellite industry. The attackers left the network utterly corrupted, leading to the company's liquidation. It was reported that the attackers had been inside the network for two years, likely spying on their activities ('Hackers corrupt satellite company IT', 2016). Increasingly, malicious actors seek to exploit the vulnerabilities in space-based systems to disrupt lives on earth. Attackers could include criminal groups, nations or even amateurs. Moreover, satellites are made from

thousands of combined parts manufactured around the world, and vulnerabilities could be built in by threat actors who seek access to the entire satellite system (Holmes, 2022).

Unlike the traditional space heavyweights of the U.S. and Russia, the Australian Space Agency only came into operation in 2018. Australia's space sector is relatively young but has shown sustained solid growth. Over the two years from 2016–2017 to 2018–2019, the space industry grew by 15.6 per cent, with an industry employment growth of 14 per cent (Australian Government & Australian Space Agency, 2020). This growth is likely to continue, with more than A$700 million invested in the civil space sector since 2018 as part of efforts to expand the sector to A$12 billion and generate 20,000 additional jobs by 2030 (Australian Trade & Investment Commission, 2021). Further, the first launch facility licence was granted to Australian company Southern Launch in April 2021, opening the Koonibba Test Range in regional South Australia to domestic and international clients (Australian Trade & Investment Commission, 2021). The formation of the Australian Space Command comes at a critical time, considering the reliance of industry and defence on Australia's space domain, including from international partners. Australia plays a critical role in generating space situational awareness, contributing significantly to ground-based optical and radar imaging.

Australia's space sector relies on government grants, which could challenge future growth. The nature of the market may change with emerging technologies. In relative terms, the government's investments are reducing, partly due to cheaper Commercial Off The Shelf (COTS) parts and open source software accessible to all (Holmes, 2022). Though these developments are promising, they may lead to constrained space budgets, which within a booming industry could cut corners elsewhere, including cyber security. The increasing risk of cyber-attacks requires a planned approach. These three priorities may prove particularly important in building up satellite cyber resilience:

1. Awareness of Emerging Threats and Investment in Cyber Security

In terms of technology, the main cyber threats affect ground station infrastructure, open source software, and COTS hardware installed onboard satellite systems (Holmes, 2022). Generally, the growing number of space-based systems increases the likelihood of cyber-attacks, as there are more opportunities for attackers and more access points that require sufficient security measures (Holmes, 2022). Additional risks come from irregular software patching, inadequate encryption and outdated IT equipment (U.S. Senate Committee on Homeland Security and Governmental Affairs, 2022). To mitigate some of these risks, there needs to be a greater focus on 'training and retaining' cyber talent and keeping equipment and knowledge up to date. The Cyber Security National Workforce Growth Program is a good step in the right direction, with the Cyber Security Skills Partnership Innovation Fund playing a key role in diversifying the cyber security workforce. Initiatives such as these will require sustained funding to keep up with emerging cyber threats in the space domain. In addition to cyber security investment, these threats require greater awareness across the entire space sector. The Australian Cyber Security Centre within the Australian Signals Directorate is well-placed to continue advising civilian companies and organisations. However, it is recommended that there is an additional tailored focus on space actors. Space Command's coordination, expertise and high-level input are important to ensure that this advice is adequately designed.

2. Further Knowledge Sharing Across the Civilian Space Sector

Space Command remains at the centre of space security for defence, but there is a growing need to ensure that the civilian space sector is equipped to manage evolving threats. Newly proposed bipartisan legislation in the U.S. aims to enhance the cybersecurity of commercial satellites. The Satellite Cybersecurity Act, introduced in January 2022, encourages voluntary satellite cybersecurity recommendations to help operators address emerging threats (Ropek, 2022). The proposed Act sees the creation of a list of 'best practices' for the private sector by the Cybersecurity and Infrastructure

Security Agency (CISA). The Act also requires the U.S. Government Accountability Office to assess the federal government's support in terms of cybersecurity for the commercial satellite industry (Ropek, 2022). Although it is too soon to tell, such efforts could prove highly effective in strengthening resilience across the civilian space sector. In Australia, the Australian Cyber Security Centre could create cyber 'best practices' specific to satellite operators or private companies utilising space-based systems, with input and direction from Space Command. Moreover, the Australian National Audit Office could be best placed to assess federal cybersecurity support for the civilian space sector, generating recommendations for additional support structures or funding streams. Creating new avenues for sharing data, knowledge and lessons could deliver significant advantages in national cyber resilience.

3. Cooperation with Like-Minded Countries to Enhance Cyber Security

Australia makes a good partner, and its joint efforts with other countries have been considerable. For example, Australia and the U.S. jointly operate the space surveillance C-band radar. Plans are also underway to relocate a U.S. optical space surveillance telescope to Western Australia, from where it will track objects in space to help avoid collisions and monitor space debris (Australian Department of Defence, 2016). Australia and the United Kingdom strengthened their longstanding ties by signing the Space Bridge Framework Arrangement on 23 February 2021, which enhances cooperation and aims to boost both space industries. Australia's geopolitical position makes it a favourable partner for Asian space actors. In December 2021, South Korea and Australia signed a memorandum of understanding to enhance collaboration on satellite development, launch services, space exploration and satellite navigation (Park, 2021). The next step is to put security at the forefront of collaboration agreements to ensure that contemporary threats are understood and mitigated.

New Space is evolving rapidly, with emerging players entering an increasingly congested domain. The proliferation of private actors and spacefaring countries holds opportunities for business, scientific exploration and space governance. However, the weaponisation of space poses a significant threat in terms of kinetic and non-kinetic attacks. Cyber security is now more important than ever to safeguard national critical infrastructure and societies dependent on them. Australia could only benefit from increasing satellite cyber resilience in the civilian space sector as a key emerging space player.

To this end, this article suggests three key priority areas. First, there is a need to raise awareness of emerging threats and promote investment in cyber security. Initiatives such as the Cyber Security National Workforce Growth Program will likely require sustained funding, while the Australian Cyber Security Centre could raise awareness among civilian space actors. Second, further knowledge sharing across the space sector is key to ensuring resilience. The Australian Cyber Security Centre could create cyber 'best practices' specific to the civilian space sector. The Australian National Audit Office could be best placed to assess federal satellite cybersecurity support, with coordination and input from Space Command. As threats in space evolve, there is a growing need for a whole-of-government approach to securing Australian space assets. Finally, international cooperation could enhance Australian satellite cyber security. Australia is becoming a key global partner in space. It is, therefore, more important than ever to focus on protecting the security of satellites and, in turn, lives on earth.

References

Australian Department of Defence. (2016). *2016 Defence White Paper*. Retrieved from https://www.defence.gov.au/about/publications/2016-defence-white-paper

Australian Government and Australian Space Agency. (2020). *State of Space Report.* Retrieved from https://www.spaceindustry.com.au/wp-content/uploads/2020/05/state-of-space-report-2018-19.pdf

Australian Trade and Investment Commission. (2021). *Australian space industry set to rocket to new heights.* Retrieved from https://www.austrade.gov.au/international/invest/investor-updates/2021/australian-space-industry-set-to-rocket-to-new-heights

Bellasio, J., Slapakova, L., Huxtable, L., Black, J., Ogden, T. & Dawaele, L. (2021). *Innovative Technologies and the 2040 Battlefield*. RAND Europe. Retrieved from https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2021)690038

Bugos, S. (2021). *Russian ASAT Test Creates Massive Debris. Arms Control Association.* Retrieved from https://www.armscontrol.org/act/2021-12/news/russian-asat-test-creates-massive-debris

Durrani, H. (2018). The Bogotá Declaration: A Case Study on Sovereignty, Empire, and the Commons in Outer Space. *Columbia Journal of Transnational Law.* Retrieved from https://www.academia.edu/35362196/The_Bogot%C3%A1_Declaration_A_Case_Study_on_Sovereignty_Empire_and_the_Commons_in_Outer_Space

Eberhardt, J. (2019). *Outer Space Increasingly 'Congested, Contested, and Competitive'.* Retrieved from https://www.un.org/press/en/2013/gadis3487.doc.htm

Erwin, S. (2021). DoD space agency: Cyber attacks, not missiles, are the most worrisome threat to satellites. *Space News*. Retrieved from https://spacenews.com/dod-space-agency-cyber-attacks-not-missiles-are-the-most-worrisome-threat-to-satellites/

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

Hackers corrupt Satellite Company IT. (2016). *SBS News*. Retrieved from https://www.sbs.com.au/news/hackers-corrupt-satellite-company-it

Holmes, M. (2022). *The Growing Risk of a Major Satellite Cyber Attack. Via Satellite.* Retrieved from http://interactive.satellitetoday.com/the-growing-risk-of-a-major-satellite-cyber-attack/

Park, S.S. (2021). South Korea, Australia sign MOU on space cooperation. *Space News*. Retrieved from https://spacenews.com/south-korea-australia-sign-mou-on-space-cooperation/

Ropek, L. (2022). Senators Introduce Bill to Protect Satellites From Getting Hacked. *Gizmodo*. Retrieved from https://gizmodo.com/senate-weighs-bill-to-protect-satellites-from-getting-h-1848384237

U.S. Senate Committee on Homeland Security and Governmental Affairs. (2022). *Peters, Cornyn Introduce Bipartisan Legislation to Protect Commercial Satellites from Cybersecurity Threats*. Retrieved from https://www.hsgac.senate.gov/media/majority-media/peters-cornyn-introduce-bipartisan-legislation-to-protect-commercial-satellites-from-cybersecurity-threats

Wrench, J. (2019). Non-Appropriation, No Problem: The Outer Space Treaty Is Ready for Asteroid Mining. *Case Western Reserve Journal of International Law*, *51*(1), 437–-462. Retrieved from https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=2546&context=jil