# SPACE

Sector Overview

Russian cyber-attacks against space technology as part of its war against Ukraine show that space technology is part of the front line of modern warfare. Australia needs to manage better the intersection of cyber security and physical security of space infrastructure.  So much more than just your air travel and your Garmin watch depends on space technology, with much of the earth's key critical infrastructure dependent on space-based infrastructure assets.

At the start of the Russia-Ukraine war, the commercial and defence satellite contractor Viasat underwent a targeted cyber-attack that halted the network, cut off internet connectivity, and disabled communications in Ukraine. Given its connections to the US military, Viasat was not a random victim but a purposeful target. Europe may feel far from Australia, but the threat to the Australian space sector is real.

The systems of Newsat, a small Australian satellite company, were hacked by foreign attackers in 2016, with the attackers completely compromising Newsat and causing the firm to be shut down. According to forensic analysis, the attackers had been inside Newsat's network for up to two years, highlighting the need for start-up space tech companies to prioritise cyber security from the outset rather than shifting it down the list of commercial priorities.

Space systems, including satellites, ground stations, and communication links at the national, regional, and international levels are essential to critical terrestrial infrastructure like communications, marine trade, financial services, weather monitoring, and defence. The vital services that are essential to our way of life on earth will be significantly impacted if cyber-attacks compromise space facilities through some of the following threats:

- Ground systems misused to communicate with a satellite maliciously
- Hacking communications on TT&C (Telemetry, Tracking and Command) systems using electronic means such as jamming and spoofing, replay assaults, or command link injection
- Malicious elements included in hardware development, such as hardware-based trojans that make use of design flaws to carry out malicious actions or send direct memory writes to satellites
- The compromise of software-defined radio
- Exploiting software flaws and vulnerabilities
- Insider threats

Prior to 2018, Australia had remained relatively absent as an international player in terms of Space missions or technology. Many Australians may not naturally consider cyber threats to vital space technology as a distinct national critical infrastructure risk to manage.

The establishment of the Australian Space Agency in July 2018 changed this and laid the foundations upon which Australia is currently expanding its space industry so that by 2030 the nation's space sector will be worth $12 billion and employing tens of thousands of Australians.

Whilst Australia currently contributes only 1% to the global space industry, over the next five years, Australia's position is predicted to grow at 7.1% annually, so that by 2030 Australia's space industry will triple in size from $4 billion to $12 billion. A big part of the Australian Government's Australian Civil Space Strategy 2019-2028 hinges upon two space investment programs: the Space Infrastructure Fund and the International Space Investment initiative. In addition to being a vital element of national critical infrastructure, the domestic space industry represents a growing source of value to the Australian economy. The value of the global space economy continues to surge ($420 billion in 2020) and is anticipated to surpass $1.1 trillion globally by 2040.

The main infrastructure elements that face cyber threats are:

**Space Systems:**

These assets are either in suborbital or outer space and can include certain ground control systems, including the facilities needed to launch assets and are referred to as space systems. The ground, space, and link segments are the three technological, and operational segments typically used to describe space systems. Groups of satellites in orbit make up the space segment. A satellite consists of a 'bus', which holds the payload and other satellite systems, and a payload, which is the apparatus intended to perform the functions of the satellite. The satellite-to-ground station and satellite-to-satellite transmission channels make up the link segment.

Given the age of many satellites, it is common for them to use antiquated technology, making them vulnerable to cyberattacks. For instance, they could have hard-coded security credentials or insecure communication protocols, which leaves them open to attack. Additionally, the attack surface is continually growing as more commercial players access space and start providing services.

**Ground Systems:**

The simplest technique to attack space systems is to compromise ground station infrastructures since they supply the technology and software needed to lawfully control and track space objects using already-existing terrestrial networks and systems. Space attack vectors involve the exploitation of misconfigurations and software vulnerabilities in systems, gaining unauthorised access to critical services, injection of Malware and phishing to obtain sensitive credentials.

Traditional Tactics, Techniques, and Procedures (TTPs) will be effective from the ground system down to the level of the modems and antennas since the ground segment is mostly made up of conventional information technology, such as Windows and Linux workstations and servers. An assault on Industrial Control Systems (ICS) is similar to an attack on modems and antennae.

**'Space Segment':**

The 'space segment' consists of constellations of satellites in orbit, space stations, and launch vehicles. These systems are vulnerable to different kinds of cyberattacks. Spacecraft may be susceptible to command interference (giving bad instructions to destroy or manipulate basic controls). Additionally, malicious payload control and assaults like Denial of Service (DoS) are possible and may result in system overload via traffic flooding. Malware may also be used to compromise links between systems on the ground (such as user systems and satellite control centres), impersonate signals from an unreliable source, or replaying, halting, or delaying communications.

**Communications:**

The connecting section has fewer tactical possibilities since it is more understood and fortified. It has long been standard procedure for satellite providers to secure the link segment using Communications Security (COMSEC) to protect the privacy of data while it is in use (transmission) or at rest. Transmission Security (TRANSEC) is used to guarantee transmission availability and restrict intelligence gathering. Without these safeguards, the satellite might be affected by techniques like jamming, spoofing, command link instructions, or radio frequency replay assaults.

Jamming is the most frequent hazard to communication channels (uplink and downlink channels). To block or degrade the signals from the GPS satellites, GPS jammers transmit signals at the same frequency as the GPS device. GPS spoofing, which includes modifying the GPS signal, is riskier than GPS jamming since it gives the user the impression that the GPS is operating as intended. Additionally, the attacker might intercept and listen in on the satellite transmission if the traffic is not encrypted. As additional communications capabilities via space are made available, it is anticipated that these types of attacks will continue in the near future, emanating not just from nation-state players but also from well-resourced non-state actors (such as criminal organisations seeking financial benefit).

**Supply Chains:**

The difficulty of the government-funded systems' supply chains and vendor ecosystems leads to another significant problem with space system security. The specialised components required for space assets are typically not all created by a single manufacturer. In reality, space companies frequently buy parts from global authorised vendor catalogues to reduce costs. Cybersecurity vetting requirements may or may not be explicitly included in the clearance process for these suppliers. For instance, when a space organisation buys a component from a vendor, it has minimal influence on the software developed for that component. This lack of understanding introduces significant cyber security risks. System downtime is typically not an option since space assets are designed to survive, are mission-critical and function in the field for extended periods. Patching and remediation of vulnerabilities in space assets are problematic. Furthermore, assaults on space satellites might seriously disrupt communication channels, compromising national and international security, given the growing use and interconnection of Internet of Things (IoT) devices.

**Responding to threats against the energy sector in Australia:**

Most Space sector entities won't be able to share 'machine to machine' intelligence, so an industry partner is needed as the enabler/facilitator for cyber threat intelligence (CTI) and collective defence via other means. By taking on the role of the trusted advisor/facilitator for the intelligence exchange, an industry organisation would ensure the overall quality of information flowing through its systems and out to the CI members.

'Forewarned is Forearmed', and by joining a trusted cyber community of Critical Infrastructure owners and operators responsible for protecting their space assets, you can join the movement to share contextual intelligence and proactively approach cyber defence. Cyber threat activity shared into the CI-ISAC ecosystem by one member has the potential to help others across the sector and the broader CI community stop similar attacks before they impact operations.

CI-ISAC, as a not-for-profit, member driven organisation, with a mission to serve its members and in turn their customers by building a trusted community and leveraging the best technology in its intelligence platform, and drawing on resources and resilience through its industry peer-to-peer network to anticipate, mitigate, and respond to cyber threats.

More information on CI-ISACs sovereign intelligence-sharing capability can be found on the official website: https://www.ci-isac.com.au , or by emailing info@ci-isac.com.au.

**Published:** 15th February 2023