Australian Government
Department of Home Affairs

CRITICAL INFRASTRUCTURE SECURITY CENTRE

Factsheet for Critical Infrastructure

Space Technology Dependencies

October 2025

Although not always readily apparent, space technology plays a significant role in the operation of Australia's critical infrastructure underpinning essential services that support Australia's economy, society and national security. Increasingly, critical infrastructure leverage, and in some cases, rely on space technology to function efficiently and safely. Disruption to space technology could therefore have widespread consequences.

This factsheet provides critical infrastructure owners and operators with an understanding of these risks, their obligations under the *Security of Critical Infrastructure Act 2018* (SOCI Act) and some potential risk mitigations.

Why is space technology important to critical infrastructure?

The space technology sector provides critical components and services to Australia's critical infrastructure. Across all 11 critical infrastructure sectors there are examples of owners and operators leveraging, adopting or relying on space technology. Identifying dependence on space technology can be challenging – especially when space technology is integrated into the supply chains of service providers. Types of space technology commonly utilised by critical infrastructure include the following.

1. Position, navigation, timing (PNT)

PNT refers to the infrastructure and technologies that provide precise timing and location information. Across society and in the majority of critical infrastructure sectors, PNT data is sourced from Global Navigation Satellite Systems (GNSS) that transmit signals from space. Space-based PNT infrastructure is foundational for many assets including power grids, communication networks, and financial services.

PNT has played an integral role in making our economy more interconnected and autonomous. The Critical Infrastructure Security Centre has released a dedicated PNT Factsheet for Critical Infrastructure.

2. Satellite communications

Satellite communications are increasingly vital to the functioning and resilience of critical infrastructure. Secure and reliable communication systems are used to monitor and control essential networks like energy, maritime and aviation.

Disruptions to communication networks can have serious consequences for these sectors, impacting public safety, economic stability, and national security. Satellite communications also play a central role in supporting critical infrastructure operations in areas where terrestrial networks are unavailable or disrupted. For example, the Sky Muster satellite service provides internet access to regional and remote areas of Australia where other NBN technologies are traditionally inaccessible.

3. Earth observation

Earth observation technologies have a range of strategic and operational applications including weather prediction, intelligence, surveillance, disaster response, and mapping. For example, earth observation enhances agriculture by delivering data on soil moisture, tracking of surface water, groundwater, and environmental changes. Additionally, Earth observation technology plays an essential role during natural hazards, such as bushfires or flooding, to identify hazards and protect critical infrastructure. Earth observation technology enhances decision making for critical infrastructure operators by providing accurate and wide-scale geospatial data.

4. Space observation / space situational awareness

Space observation and space situational awareness (SSA) technologies are used to monitor space-based assets. SSA is particularly important to observe and protect space-based services such as PNT, earth observation and satellite communication. Although many critical infrastructure operators are not directly engaging with space observation, much of their services benefit from it indirectly. SSA is primarily utilised by the defence industry and higher education and research sectors. For example, space observation is used to track space debris and other space assets to detect potential threats to land and other space infrastructure. Space observation is therefore critical to the safety of satellites and the availability of services that are relied on in multiple critical infrastructure sectors.

What can disrupt or degrade space technology?

A disruption or degradation of space technology services – locally or globally – can lead to cascading failures across interconnected systems.

Hazards

Space weather refers to events that occur beyond the Earth's atmosphere, predominantly caused by the Sun. Examples of space weather events include solar flares, particle radiation storms, and coronal mass ejections – the latter of which can produce geomagnetic storms on the Earth. These events can release substantial amounts of energy and radiation into the Earth's magnetic field which can disrupt satellites, overload electrical grids, degrade high frequency radio communications and produce auroral displays. Space weather can affect various space-based technologies, space-related ground systems and space-enabled systems on the Earth, potentially leading to degraded performance, service interruptions, or system failures.

Extreme weather events on the Earth can cause physical damage to antennas, ground infrastructure, and power supplies of space technology, potentially disrupting signal transmission or quality. This can pose significant challenges to ground operations.

Accidental or unintentional disruption can be equally detrimental and have severe impacts on critical infrastructure. Radio frequency interference caused by machinery or electronic devices can generate signal disturbance between ground-based infrastructure and satellites. Unintended disruptions can also occur due to human error, a lack of testing and monitoring and associated equipment failures. With the growing number of launched objects into space, especially into Low Earth Orbit (LEO), there is an increasing risk that collisions could cause major service disruption.

Threats

Critical infrastructure is an attractive target for malicious actors seeking to cause disruption.

Jamming is a deliberate form of signal interference. Jamming is achieved through transmitting electromagnetic waves on the same frequency, overpowering a receiver and reducing its ability to receive legitimate signals. A reduced signal can result in total loss of a transmission which can result in a number of systems failures.

Spoofing occurs when an attacker attempts to trick a user or system into thinking a request or data transmission is legitimate. Jamming and Spoofing attacks are frequently deployed on GNSS signals, rendering them unavailable or erroneous. A disruption to these signals can cause cascading failures within the supply chain for critical infrastructure operators.

Cyber Attacks have targeted space assets in order to degrade or disrupt the use of space technology. Cyber attacks on space technology can be widespread, affecting not only space technology operators but also users who depend on satellite-based services in other sectors.

> Shortly before Russian military attacks commenced in Ukraine in 2022, a series of cyber attacks targeted US-owned communications company, Viasat, operating in Ukraine. Intelligence agencies assessed the cyber-attack as an act of cyber sabotage on Ukraine. While the primary target was assessed to be the Ukrainian military, other critical infrastructure and civilian users were impacted, with cascading consequences, impacting tens of thousands of users across Europe.

A cyber attack on space technology could have a variety of impacts on both the space technology assets and dependent critical infrastructure or users. The Space Attack Research and Tactic Analysis (SPARTA) provides guidance on how spacecraft can be compromised by cyber means and the various segments that may be manipulated.

What can be done to mitigate these risks?

Entities can take a number of actions within their organisation to mitigate risks in relation to their dependency on space technology. This may include adopting a strong and proactive cyber security posture, and implementing redundancy where possible.

1. Implement redundancy strategies

To prevent major disruptions to critical services, critical infrastructure owners and operators should have a thorough understanding of their supply chains and identify which segments of their business depend on or leverage space technology.

Various strategies may need to be employed to protect assets from different threats. In assets with timing systems that may be affected by space weather (e.g. GNSS), critical infrastructure operators should consider having an alternate terrestrial timing source as a backup for their systems, such as Network Time Protocol (NTP). Critical infrastructure owners and operators should determine a tolerable downtime threshold, and build redundancy protocols into business continuity and risk management plans.

Under the *Security of Critical Infrastructure Act 2018,* responsible entities for assets specified in the Critical Infrastructure Risk Management Program (CIRMP) Rules 2023 are required to develop a risk management plan (a CIRMP) that identifies and manages 'material risks' of 'hazards' that could have a 'relevant impact' on the asset. Likewise, responsible entities for critical telecommunications assets may be subject to Telecommunications Security and Risk Management Program Rules (TSRMP Rules). Responsible entities should consider how space technology risks could have a relevant impact on their asset and, where possible, implement mitigations to reduce those risk.

2. Adhering to cybersecurity standards

Critical Infrastructure assets which utilise space systems must have robust encryption and secure communication protocols to protect sensitive data and prevent unauthorised access.

Responsible entities identified in the CIRMP rules are required to meet specific cyber security frameworks and maturity levels. Other ways operators can ensure they are meeting the necessary cyber security standards is by obtaining certifications (NIST and ISO), undergoing audits by a qualified IRAP assessor, and following the advice provided by agencies such as the Australian Signals Directorate's (ASD) Essential Eight or Information Security Manual (ISM). Many standards and certifications offer tailored frameworks to support critical infrastructure operators.

3. Bolstering cyber education

Encouraging and enhancing cyber hygiene can significantly minimise the risk of a cyber incident to CI assets. In 2024 alone, human error accounted for 30% of data breaches in Australia. This includes failing to recognise phishing and social engineering as well as minor oversights in patching, or system misconfiguration. Critical infrastructure owners and operators should conduct regular training and implement refresher courses on cybersecurity practices to build a security-centric culture and mindset. Strategies such as segregation of duties, privileged access management, logging and auditing can all improve the cyber hygiene of a business. ASD encourages critical infrastructure entities to report anomalous activity early and not wait until malicious activity reaches the threshold for a mandatory report. Reporting helps piece together a picture of the cyber threat landscape, and informs ASD's cyber security alerts and advisories for the benefit of all Australian entities. Visit Report:Cyber to report a cybercrime, incident or vulnerability.

4. Physical mitigations and monitoring

Critical infrastructure systems with a reliance on space technology should monitor space weather forecasting resources to stay informed of events that may affect their asset and services. The Bureau of Meteorology's Australian Space Weather Forecasting Centre is Australia's official source of space weather alerts, warnings, and forecasts. Access to timely forecasts of significant space weather events can assist in the implementation of mitigation plans, and differentiating between natural hazards and other threats. This may involve vulnerable infrastructure being switched off, or power being rerouted, while providing time to prepare response and recovery efforts to resupply power in the shortest possible timeframe following the space weather event. Additionally, implementing backup power systems and alternative supply chains is essential to sustain operations running during potential power outages caused by geomagnetic storms.

Where can I find out more?

Within the Department of Home Affairs, the Critical Infrastructure Security Centre (CISC) drives an all-hazards critical infrastructure risk management regime in partnership with government, industry and the broader community. The CISC assists critical infrastructure owners and operators to understand the risk environment and meet their regulatory obligations. More information can be found on the CISC website or by contacting enquiries@CISC.gov.au.

The Australian Signals Directorate provides a range of advice at cyber.gov.au to improve cyber security.