EXPLAINER SERIES

Indo-Pacific explainer: **Critical infrastructure**

This guide is provided as part of the Perth USAsia Centres 'explainer series' and is intended for education purposes. It is free to use and share but attribution to the Perth USAsia Centre is required. For enquiries relating to the Centre's educational resources please email perthusasiacentre@uwa.edu.au

2509

Perth USAsia Centre
INDO-PACIFIC STRATEGY

What is critical infrastructure?

Critical infrastructure refers to systems, facilities, and assets that are essential to the functioning of society and the economy. What makes infrastructure "critical" is its essential role in maintaining public safety, security, health, or economic stability—its failure would have serious consequences in one or more of these areas.

Critical infrastructure may be physical, such as power stations or transport systems. It can also be virtual, including national banking and communication networks (Box 1). In many cases, these systems combine both physical and virtual components. Data centres, for example, consist of physical buildings and the servers and software they support.

BOX 1: **Examples of physical and virtual infrastructure systems**

Physical

- Power grids
- Gas pipelines
- Cell towers
- Fibreoptic cables
- Water systems
- Roads and highways
- Shipping terminals
- Hospitals

Virtual

- Operating systems like Windows
- Email servers
- Cloud computing
- Encryption and digital certificates
- Society for Worldwide Interbank Financial Telecommunication or SWIFT
- Emergency response systems like Computer-Aided Dispatch (CAD)

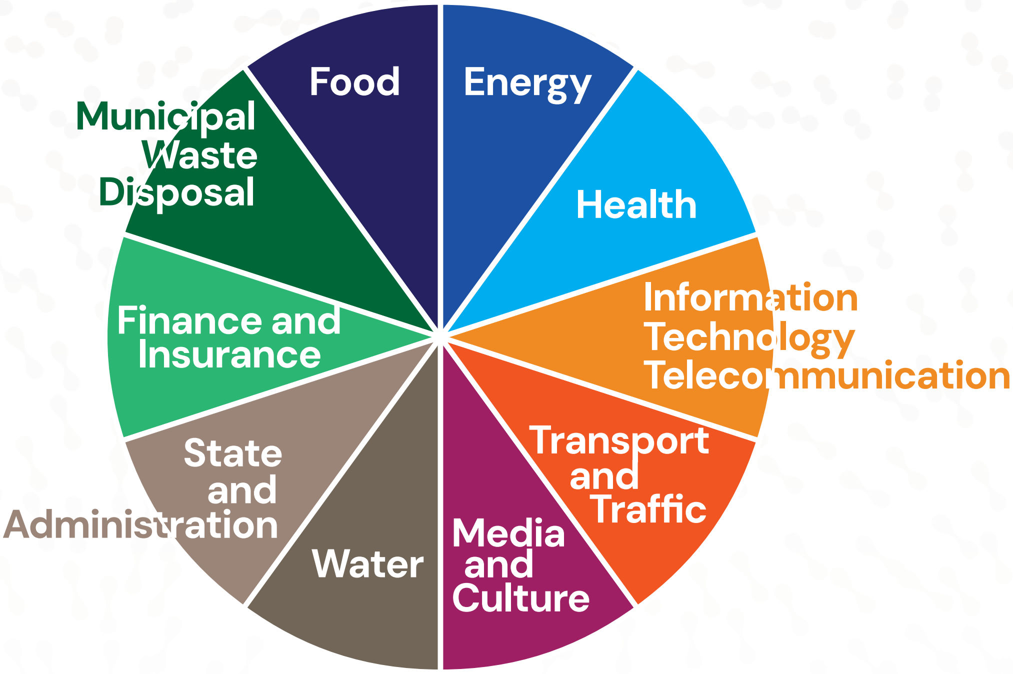
As technology and society evolve, so too does our understanding of what qualifies as critical infrastructure. There is, in fact, no universally accepted definition of critical infrastructure. For example, space is increasingly recognized as a critical infrastructure sector because space systems such as GPS or Earth observation are invaluable for everyday economic activities from agriculture to financial transactions. But determining which space assets are truly critical - and therefore warrant protection - is complex and often contentious.[1]

Protecting critical infrastructure

Advancements in technology and communications networks have made critical infrastructure increasingly interdependent, meaning a disruption in one sector can trigger cascading effects across others. This is why most countries and governing bodies maintain rules around how critical infrastructure is managed, including Australia.

The Security of Critical Infrastructure Act (SOCI), introduced in 2018, is the most important legal framework aimed at enhancing the security and resilience of critical infrastructure. SOCI aims to protect eleven key sectors by ensuring that owners and operators of Australia's most vital infrastructure assets are equipped to identify, mitigate, and manage potential risks.

BOX 2: **Critical infrastructure sectors in Australia**



Source: Australian Government[2]

Meanwhile, national security agencies like the Australian Security Intelligence Organisation (ASIO) play a key role in continuously monitoring and assessing potential threats to critical infrastructure systems.

Common threats to critical infrastructure

Threats to critical infrastructure systems have become more frequent and complex over the past decades (Box 3).

Cyberattacks on essential services such as power grids, water supplies, and healthcare networks are increasingly sophisticated. In 2022, for example, both telecommunications giant Optus and Australia's second-largest health insurer, Medibank, suffered from ransomware attacks that exposed the medical histories, identification documents, and financial information of more than ten million Australians.[3]

Critical infrastructure is also a flashpoint of geopolitical conflict as different states are exploiting vulnerabilities in their adversaries' infrastructure to disrupt economies, degrade military capabilities, or undermine social cohesion.[4] For example, Chinese vessels have repeatedly damaged Taiwan's subsea cables, which carry almost all internet traffic, as part of a broader strategy to project Beijing's influence and test Taiwan's resilience.[5] In the US, hackers linked to China, Russia and Iran have repeatedly targeted water utility systems posing a significant risk of disruption or even shutdown of drinking water supplies.[6]

The physical risks to infrastructure are not only growing because of conflict and competition, however. Climate change is driving more frequent and severe natural disasters. Extreme weather is also putting additional pressure on systems designed around past climate patterns such as cooling systems at power plants, which rely on cold water from surrounding rivers and lakes and may struggle to keep up with rising global temperatures.

BOX 3: Types of threats to critical infrastructure

CYBER ATTACKS

Attackers try to break into control systems or exploit weaknesses in networks and software to disrupt operations, steal sensitive data, or even cause physical damage.

PHYSICAL ATTACKS

Acts like sabotage, terrorism, or vandalism can cause serious damage to critical infrastructure facilities, interrupt essential services, and put lives at risk.

NATURAL DISASTERS

Severe weather events like earthquakes or floods can disrupt essential services and cause physical damage.

HEALTH EMERGENCIES

Disease outbreaks and pandemics can lead to staff shortages, disrupt normal operations, and put additional pressure on public health systems.

SUPPLY CHAIN VULNERABILITIES

Weak spots in the supply chain such as counterfeit or tampered components can create serious risks, disrupting or damaging the systems that rely on them.

TECHNOLOGICAL DEPENDENCIES

As critical infrastructure becomes more connected and dependent on advanced technology, it also becomes more reliant on complex systems and software, making it more vulnerable to disruption.

Adapted from: IBM[7]

CASE STUDY: Australia's 5G network and the Huawei ban

Australia's 5G network is a key example of how critical infrastructure plays a strategic role in national security, economic growth, and diplomacy.

Unlike previous generations of mobile networks, 5G supports advanced technologies like autonomous vehicles, smart cities, telemedicine, and defence communications. Because of this, the government considers the integrity and security of 5G infrastructure as critical to both everyday life and national security.

In 2018, Australia became one of the first countries to ban the Chinese telecom giant Huawei from building its 5G network, because the government worried the Chinese Communist Party could exploit its access to Australia's telecommunications for foreign interference or espionage.[8] While the ban increased costs and slowed deployment, it was seen as a necessary step to protect the country's technological sovereignty and national security.

Australia has also actively supported the development and deployment of 5G technology in other Indo-Pacific countries to ensure their critical infrastructure remains secure and resilient. For example, in 2021, the government helped fund a deal to acquire Digicel, the Pacific's largest mobile carrier, with the aim of upgrading internet infrastructure in regional countries like Papua New-Guinea and Fiji while countering China's growing influence in regional telecommunications.[9]

Further reading:

- ↗ What is sabotage and why is the ASIO chief worried about it?
- ↗ 2023-2030 Australian Cyber Security Strategy
- ↗ Beneath the surface of Pacific digital infrastructure investments

Endnotes

[1] Industrial Cyber Co (2025), "US House debuts Space Infrastructure Act to designate space systems as critical infrastructure", https://industrialcyber.co/regulation-standards-and-compliance/us-house-debuts-space-infrastructure-act-to-designate-space-systems-as-critical-infrastructure/

[2] Australian Government (2024), 'Critical infrastructure', https://www.nationalsecurity.gov.au/protect-your-business/critical-infrastructure

[3] Queensland Government (2025), "Medibank Private Cyber Incident", https://www.qld.gov.au/community/your-home-community/cyber-security/cyber-security-for-queenslanders/case-studies/medibank-private-cyber-incident; BBC (2022), "Optus: How a Massive Data Breach Exposed Australia", https://www.bbc.com/news/world-australia-63056838

[4] Mike Burgess (2025), '2025 Annual Threat Assessment', https://www.oni.gov.au/news/asio-annual-threat-assessment-2025

[5] Gahon Chia-Hung Chiang (2025), "Countering China's Subsea Cable Sabotage", https://globaltaiwan.org/2025/03/countering-chinas-subsea-cable-sabotage/

[6] Trevor Jockims (2024), 'America's drinking water is facing attack, with links back to China, Russia and Iran', https://www.cnbc.com/2024/06/26/americas-drinking-water-under-attack-china-russia-and-iran.html

[7] IBM (n.d.), 'What is critical infrastructure?', https://www.ibm.com/think/topics/critical-infrastructure

[8] ABC (2018), 'Huawei banned from 5G mobile infrastructure rollout in Australia', https://www.abc.net.au/news/2018-08-23/huawei-banned-from-providing-5g-mobile-technology-australia/10155438

[9] ABC (2021), 'Telstra to buy Pacific arm of telecommunications giant Digicel with Canberra's support amid China's rising influence', https://www.abc.net.au/news/2021-10-25/telstra-digicel-pacific-telecommunications-deal-finalised/100564976

This guide is provided as part of the Perth USAsia Centres 'explainer series' and is intended for education purposes. It is free to use and share but attribution to the Perth USAsia Centre is required. For enquiries relating to the Centre's educational resources please email perthusasiacentre@uwa.edu.au

Australia and the Indo-Pacific:
Understanding our strategic
connections to Asia

@ perthusasiacentre@uwa.edu.au
@PerthUSAsia
PerthUSAsia
linkedin.com/company/perth-usasia-centre
perthusasia.edu.au

Perth USAsia Centre
INDO-PACIFIC STRATEGY

EXPLAINER
SERIES