



Securing space: Cyber resilience for the final frontier

Cyber security in space: Safeguarding the final frontier



As our reach extend beyond Earth, our reliance on space based systems and the critical services they provide has become integral to our national security, our future prosperity, economic stability and our very way of life.

However, with this expansion comes an increasing array of cyber threats and electromagnetic targeting our space assets. From satellite communication to data integrity, the cyber domain presents clear, present, deliberate and sustained challenges to the information flows and data integrity which will jeopardise the future of space exploration and operations. We explore the critical cyber security risk in space and outline the strategies to protect your space and assets and the services they provide from cyber-attacks.

The growing cyber threat to space systems

The 2023 National Risk Register identified three space-related risks to UK infrastructure, including one risk of deliberate disruption to UK space systems and services. Cyber and Electromagnetic Activities (CEMA) are of particular concern and pose a significant threat, reflecting the modern reality where space and cyberspace are deeply intertwined. Cyber-attacks on space systems can lead to devastating consequences, including the loss of communications, data corruption, and even the complete seizure and control of a satellite and its services.

Key cyber threats

- **Data interception or monitoring:** Unauthorised access to mission data, which can be used for espionage or future attacks.
- **Data corruption:** Deliberate manipulation of data that can lead to inappropriate decision making forcing missions/service disruption, denial or loss.
- **Seizure of control:** A catastrophic attack where threat actors gain control over satellite systems, potentially leading to irreversible damage.
- **Supply chain compromise:** Insertion of malware or counterfeit components into space systems during production, leading through life operational vulnerability.

Understanding the risks: Failure modes linked to cyber and electromagnetic threats

Cyber and electromagnetic threats are particularly dangerous because they can trigger multiple failure modes, leading to severe disruption of space operations, including:

Loss of communication

- 1 Electromagnetic attacks such as jamming or spoofing can sever the link between ground control and satellites, rendering them inoperable.

Payload failure

- 2 Manipulated data or unauthorised access can disrupt the satellite's mission, causing it to fail in gathering or transmitting critical data.

Data processing errors

- 3 Cyber intrusions can corrupt data processing systems, leading to false data that can have far-reaching operational consequences on Earth and space systems and the services they provide.

Strategic cyber security measures for space systems

To safeguard space assets against cyber threats, it's crucial to implement comprehensive cyber security strategies. This must address the unique challenges of operating in space, where traditional security measures may not be applicable.

Building resilience: The path forward

To protect space systems from cyber threats, it's essential to adopt a proactive and layered approach to cyber security. This includes integrating cyber security measures into every stage of space system development and operations, from design to deployment and beyond.



How CGI protects space

CGI provides a full range of services to protect the design, development, testing and operation of space missions and space companies from Small and Medium Enterprises (SMEs) and space component manufacturers, to large organisations. We can help protect ground and space-based assets.

For expert guidance on supporting your space systems against cyber threats, [contact us today](#).



CGI is a leader in both cyber security and the space domain. We have one of the largest cyber security practices in the UK, with over 1,700 experts helping clients across various sectors manage complex security challenges.

About CGI

Insights you can act on

Founded in 1976, CGI is among the largest IT and business consulting services firms in the world.

We are a true IT Systems Integrator. We work tirelessly to advise, build and operate bespoke, technically complex, mission-critical information systems which help our clients keep us all safe and secure.

We bring innovation to our clients using proven and emerging technologies, agile delivery processes and our deep expertise across the breadth of space, defence, intelligence, aerospace and maritime, all underpinned by our end-to end cyber security capability. We work collaboratively with global technology companies, cutting edge SMEs and academia to deliver the optimal solution for each client.

For more information

Visit [our webpage](#)

Email us at: enquiry.uk@cgi.com