SAFEGUARDING THE US SPACE INDUSTRY

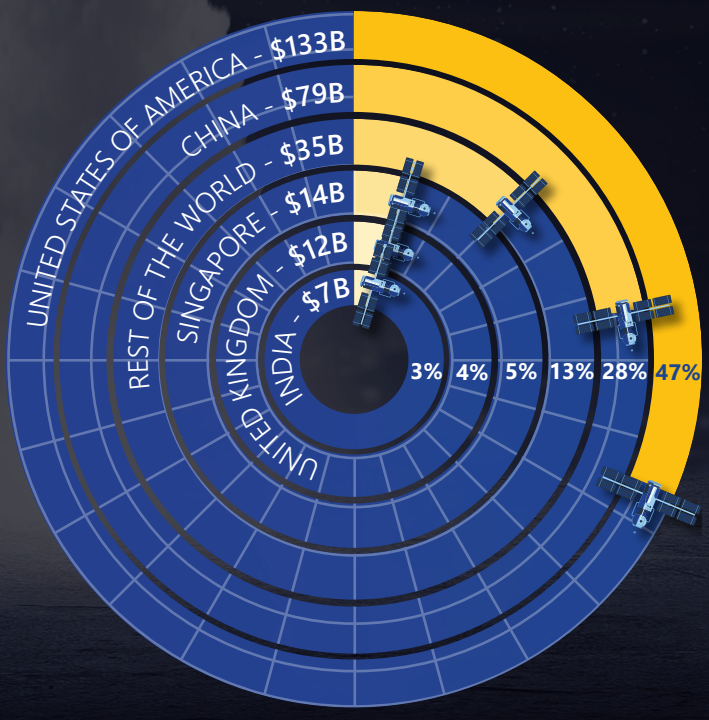
KEEPING YOUR INTELLECTUAL PROPERTY IN ORBIT

THREAT

According to US financial sector estimates, the global space economy is projected to grow from $469 billion in 2021 to more than $1 trillion by 2030. The United States is the main driver of this growth through its role as a global leader in space investment, research, innovation, and production. Space is fundamental to every aspect of our society, including emergency services, energy, financial services, telecommunications, transportation, and food and agriculture. All rely on space services to operate.

Foreign intelligence entities (FIEs) recognize the importance of the commercial space industry to the US economy and national security, including the growing dependence of critical infrastructure on space-based assets. They see US space-related innovation and assets as potential threats as well as valuable opportunities to acquire vital technologies and expertise. FIEs use cyberattacks, strategic investment (including joint ventures and acquisitions), the targeting of key supply chain nodes, and other techniques to gain access to the US space industry.

SPACE EQUITY INVESTMENT 2013-2023 (Q2)



Source: https//www.spacecapital.com/quarterly

IMPACT

FIE efforts to target and exploit the US space industry can harm US commercial firms and broader US national and economic security in several ways.

Global Competition

- Siphoning intellectual property and other proprietary data from US space firms for the benefit of foreign powers' national security programs.
- Leapfrogging innovation that costs US space firms substantial time and resources to generate.
- Using state-backed resources and unfair business practices to disadvantage US space firms.
- Harming US corporate reputations by proliferating counterfeit products or falsely authenticated reproductions.

National Security

- Collecting sensitive data related to satellite payloads.
- Disrupting and degrading US satellite communications, remote sensing, and imaging capabilities.
- Degrading the United States' ability to provide critical services during emergencies.
- Identifying vulnerabilities and targeting US commercial space infrastructure during conflict.

Economic Security

- Harming the US commercial space sector by causing losses of revenue and global market competitiveness.
- Exploiting critical resources and supply chain dependencies.
- Influencing international laws, norms, and host country business regulations governing space to disadvantage US space firms.

INDICATORS

Your employees, contractors, and suppliers are vital to protecting your organization. Be aware of the following indicators and other potential signs of FIEs targeting you.

- Unusually high cyberactivity targeting your company from unknown parties.
- Requests to visit your company facilities from unknown or foreign entities.
- Specific and probing questions about sensitive, internal, and proprietary information.
- Elicitation at conferences or online fora.
- Unsolicited offers to establish joint ventures with companies tied to foreign governments or state-owned enterprises.
- Attempts to recruit your company's technical experts, including through invitations to travel to a foreign country, offers of employment (such as consultancy work), and provision of financial incentives in exchange for proprietary information.
- Acquisition or investment efforts by foreign companies via wholly-owned subsidiaries registered in third countries that are designed to obscure the parent company's connections.

REPORTING INCIDENTS

- If you believe your company's intellectual property has been targeted or is at risk of compromise, contact the Private Sector Coordinator at your local FBI Field Office: **https://www.fbi.gov/contact-us/field-offices**
- You can also submit a tip to the Department of the Air Force Office of Special Investigations at: **https://www.osi.af.mil/Submit-a-Tip/**

MITIGATION

You are not helpless in the face of FIE threats to your organization.

- Develop an "anomaly" log to track peculiar incidents to potentially spot malicious trends against your organization.
- Establish an insider threat program within your organization. Consider appropriate vetting and oversight for those with sensitive positions or access.
- Foster an enterprise-wide security posture at your company, ensuring security, cyber, IT, insider threat, legal, human resources, and procurement offices all collaborate on security efforts.
- Identify your "crown jewels" that are key to your company's competitiveness and develop strategies to prevent or mitigate their loss.
- Conduct robust due diligence on suppliers, understand their security practices, and set and enforce minimum standards for them.
- Incorporate security requirements, such as incident reporting, into third-party contracts and monitor compliance throughout the lifecycle of a product or service.
- Ensure your business is familiar with host country laws and regulations that require the sharing of company data.
- Conduct appropriate due diligence on your investors.
- Build resilience and redundancy into your operations to minimize harm from FIE targeting.

For additional information on NCSC awareness materials or publications, visit our website: **www.ncsc.gov** or contact **DNI_NCSC_OUTREACH@dni.gov**.

Find us on Twitter (X):
@NCSCgov

On LinkedIn:
National Counterintelligence and Security Center

0028188