IDSS PAPER

18 August 2025

Critical Infrastructure Designation: A Strategic Approach to Enhancing Space Sector Cybersecurity

Bich Tran

RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

Ponder the Improbable since 1996

RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore
Ponder the Improbable since 1996

IDSS Paper
Ponder. Analyse. Prepare. Engage. Refresh.

www.rsis.edu.sg No.081– 18 August 2025

Critical Infrastructure Designation: A Strategic Approach to Enhancing Space Sector Cybersecurity

Bich Tran

SYNOPSIS

The European Union's decision to designate space systems as critical infrastructure transforms cybersecurity for the sector from a discretionary corporate consideration into a national security imperative. The lessons emerging from this effort will prove invaluable for policymakers worldwide.

COMMENTARY

In June 2025, the European Commission announced a proposal to regulate space activities of European Union member states, commonly referred to as the EU Space Act. This was the first time a single, supranational regulatory framework for space activities was created across an entire regional bloc. Crucially, one of the three key pillars of the act focuses on enhanced cybersecurity requirements.

The drafting of the document began in 2023, following the European Parliament and European Council's Critical Entities Resilience Directive, which recognised the space sector alongside 10 others as critical infrastructure. These developments arose in response to mounting cyber threats facing space systems, as seen most acutely in a cyberattack against Viasat's KA-SAT satellite network, which affected tens of thousands of customers across Europe in February 2022.

The designation of the space sector as critical infrastructure represents a promising pathway to improve the sector's cybersecurity. It essentially transforms cybersecurity practices from discretionary corporate activities into mandatory national security standards. Additionally, when a sector is considered critical infrastructure, it typically gains prioritised access to government resources and support.

Strategic Importance of Space Infrastructure

The space sector provides essential services that underpin key societal functions across multiple sectors. For instance, global navigation satellite systems enable precise navigation for aviation, maritime and ground transportation networks. They also provide critical timing synchronisation for financial markets, electrical power grids and telecommunications networks. For remote regions lacking terrestrial fibre optics infrastructure, satellite communications carry virtually all internet traffic, making these populations entirely dependent on space-based connectivity. This dependency structure means that cyberattacks on space assets can produce effects that extend far beyond the initial target, potentially causing widespread and lasting disruptions for society.

The space sector is also critical to modern military operations and warfare. Space-based intelligence provides commanders with unprecedented situational awareness and real-time threat assessment capabilities that are impossible to achieve through terrestrial means alone. Precision guidance systems rely on satellite navigation to achieve exceptional accuracy in military strikes while minimising collateral damage and maximising operational effectiveness. Furthermore, advanced space systems facilitate seamless coordination of military forces across the air, land, sea and cyber domains. The strategic importance of space assets has simultaneously made them prime targets for adversarial action.

Escalating Cyber Threat Landscape

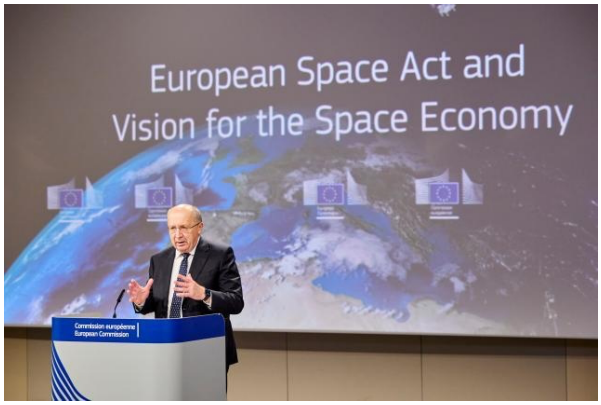
The complexity of the space sector creates a massive surface for cyberattacks. In 2024, the US-based Space Information Sharing and Analysis Center reported over 100 cyberattack attempts per week across the sector. A quick search on the European Repository of Cyber Incidents using “space” as a keyword shows 27 successful cyberattacks between 2000 and 2025, with four in 2024 alone. Victims include state space entities from the United States, Japan, Russia, China and most recently Poland. On 2 March 2025, a cyberattack against the Polish space agency prompted it to disconnect its network from the internet, rendering its website temporarily unavailable. These reported incidents probably represent only a small fraction of actual cyberattacks, as many organisations maintain strict confidentiality regarding cybersecurity.

The 2022 cyberattack on Viasat's KA-SAT network highlighted earlier serves as a stark illustration of the sector's vulnerability and the cascading effects of successful attacks. Coinciding with Russia's invasion of Ukraine, this attack disabled thousands of satellite modems across Ukraine, directly affecting military and government communications during a critical period. The attack's ripple effects extended across Europe, affecting tens of thousands of customers in Germany, France, Hungary, Greece, Italy and Poland. This episode prompted the European Union to recognise the space sector as critical infrastructure and underscored the urgent need for enhanced cybersecurity measures.

Lessons from the EU Space Act

While the EU Space Act does not explicitly define the space sector, its text suggests three primary components. The first is space infrastructure, which includes the ground segment (ground stations, terminals and control facilities), space segment (satellites, space stations, onboard hardware and software systems), and link segment. The second component is space activities, which refer to operations and facilities related to launch sites and space objects. The third one is space operators. This extends the scope of the space sector far beyond satellite communications, enabling consideration of multiple attack vectors that potential adversaries can exploit.

What makes the EU approach noteworthy is that the act centres on the principle of security by design. This requires cybersecurity considerations to be integrated from the earliest stages of system development rather than treated as an afterthought. This proactive approach addresses the reality that retrofitting security measures into existing space systems is often technically challenging and economically inefficient.



The EU Space Act's principle of security by design requires cybersecurity considerations to be integrated from the earliest stages of system development rather than treated as an afterthought.
Image source: European Union, 1995-2025, CC BY 4.0.

Furthermore, the EU Space Act establishes a comprehensive resilience baseline that applies across the entire space sector, moving beyond the fragmented approaches that have characterised previous efforts. In response to the 2022 Viasat cyberattack, European legislators enacted a directive on measures for a high common level of cybersecurity alongside the previously mentioned directive on the resilience of critical entities. Although these directives established mandatory resilience standards for terrestrial space infrastructure, they did not address space-based assets such as satellites and orbital platforms. The EU Space Act remedies this regulatory gap by implementing sector-wide resilience requirements.

The designation of space as critical infrastructure fundamentally reframes cybersecurity from an optional business consideration to a national security imperative. Critical infrastructure status typically results in prioritised government support, including dedicated funding for cybersecurity initiatives, access to specialised expertise, and technical assistance for research and development efforts. Such enhanced resource allocation enables space sector companies to implement more robust cybersecurity measures and develop innovative approaches to address emerging threats.

Global Recognition and Regulatory Response

Despite its benefits, many countries, while recognising the strategic importance of space assets, stop short of formal critical infrastructure designation. For instance, the United States identifies 16 critical infrastructure sectors but does not include space. Similar approaches can be observed in Japan, India, China and Singapore.

This hesitation may stem from several key concerns. First, critical infrastructure designation often means increased regulatory oversight that can potentially stifle innovation and competitiveness. Second, formally designating space assets as critical infrastructure could inadvertently create a "targeting roadmap" for adversaries, effectively advertising the most valuable attack vectors. Third, only sufficiently large and economically influential markets like the European Union possess the leverage to create meaningful regulations that industry cannot simply circumvent by relocating operations. Smaller nations face the difficult reality that unilateral action could drive space companies to more permissive jurisdictions, undermining both economic interests and security objectives.

However, the European Union is not alone in its approach. In 2018, Australia passed the Security of Critical Infrastructure Act, which designated space technology as one of 11 critical infrastructure sectors. The United Kingdom also included space in the list of 13 Critical National Infrastructure sectors, which was last updated in June 2025. As countries contemplate the benefits of critical infrastructure designation, more can be expected to embrace this approach.

Conclusion

As negotiations on the EU Space Act continue, the lessons emerging from this process – both successes and challenges – will prove invaluable for policymakers worldwide. While transnational markets like the European Union are rare, countries including India, China, the United States, Indonesia and Japan possess sufficient market size to regulate their space industries using similar approaches. The European Union's pioneering framework offers valuable insights and serves as a potential blueprint for regulatory innovation across diverse jurisdictions. However, the fundamental first step remains recognising the space sector as critical infrastructure.

Bich Tran *(pronounced "Bik Trahn") is a Research Fellow with the Military Transformations Programme, Institute of Defence and Strategic Studies, S. Rajaratnam School of International Studies (RSIS).*

Please share this publication with your friends. They can subscribe to RSIS publications by scanning the QR Code below.