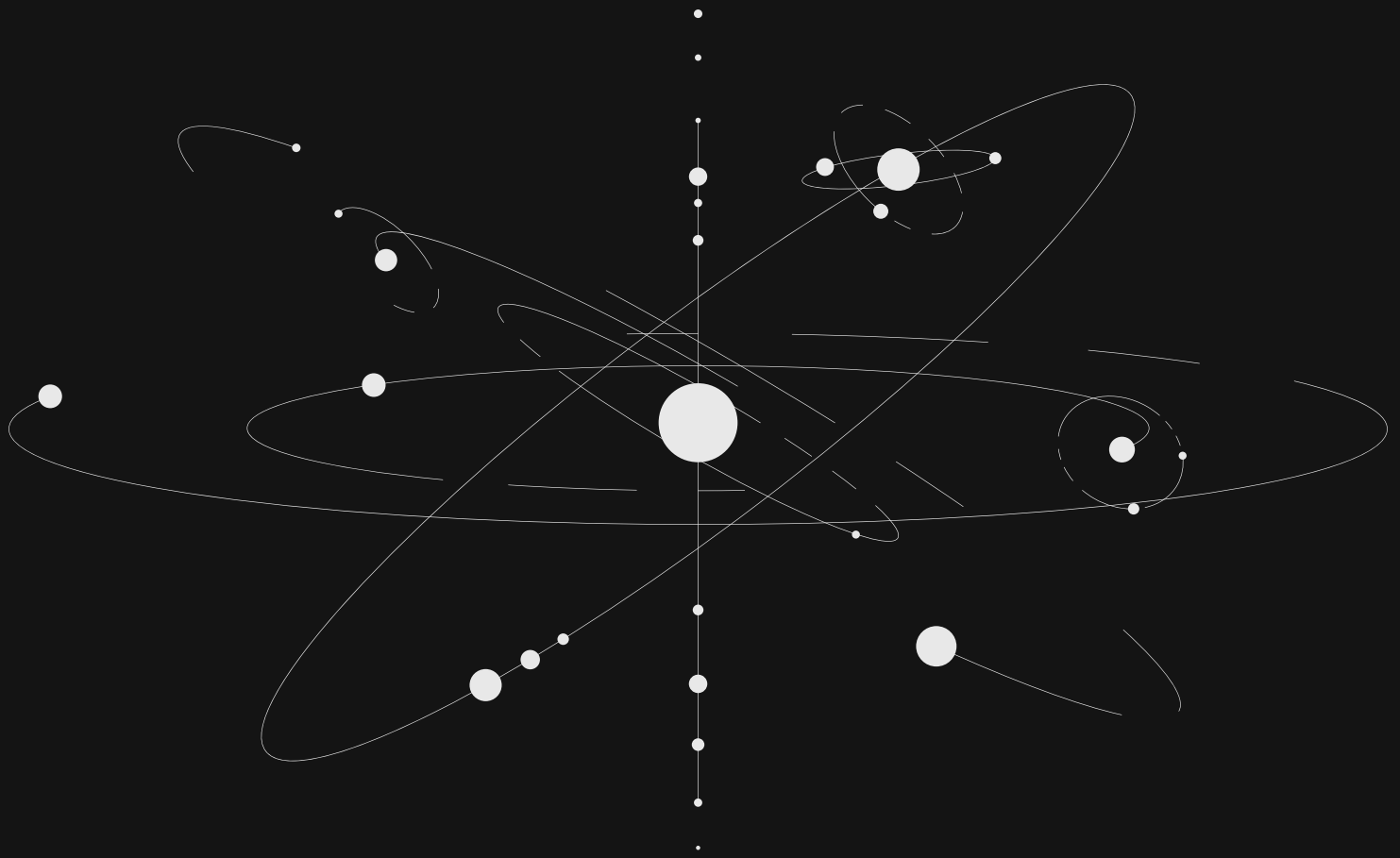




CRITICAL ORBIT: THE CASE FOR DESIGNATING SPACE AS NATIONAL INFRASTRUCTURE IN THE CYBER AGE



**BY
DR. GEORGIANNA
SHEA**



**&
HUMZA
KHAN**

Dr. Georgianna Shea is chief technologist at the Foundation for Defense of Democracies' Center on Cyber and Technology Innovation and its Transformative Cyber Innovation Lab and Humza Khan is a PhD candidate in Public Policy and Political Economy at the University of Texas at Dallas.

CRITICAL ORBIT: THE CASE FOR DESIGNATING SPACE AS NATIONAL INFRASTRUCTURE IN THE CYBER AGE

By Dr. Georgianna Shea & Humza Khan



WHEN DATA BECOMES A U.S. NATIONAL SECURITY ASSET: WHAT COMPANIES NEED TO KNOW

By Michael Bahar & Neal Higgins



STEPPING UP AND GOING PUBLIC: HOW THE FCC AND TEAM TELECOM COULD TAKE A CUE FROM THE ANTITRUST BAR TO PROMOTE NATIONAL SECURITY IN THE TELECOMMUNICATIONS SECTOR

By Elizabeth McIntyre



CAN THE EU DEFEND ITS TECHNOLOGY?

By Claudia Lemus & Ioannis Kokkoris



COMPARATIVE ANALYSIS OF TRANSATLANTIC AI REGULATORY FRAMEWORKS: JURISDICTIONAL CONVERGENCE AND DIVERGENCE IN U.S.-EU COMPLIANCE ARCHITECTURES

By Nema Milaninia & Eve-Christie Vermynck



REFRAMING THE FIGHT: HOW THE JUNE 2025 CYBER EXECUTIVE ORDER ALTERS AMERICA'S STRATEGIC POSTURE

By Cory Simpson



SECURING U.S. AI LEADERSHIP: U.S. EXPORT CONTROLS AND THE TRADE IN ADVANCED CHIPS

By Ya'ara Barnoon



CRITICAL ORBIT: THE CASE FOR DESIGNATING SPACE AS NATIONAL INFRASTRUCTURE IN THE CYBER AGE

By Dr. Georgianna Shea & Humza Khan

The space industry not only underpins the services required for critical infrastructure in everyday life, but it is also distinctly unique as a domain and a target. Space provides indispensable capabilities globally. Yet, despite explicit endorsements from the policy and space experts, space remains unrecognized in the federal and international critical infrastructure framework. This omission leaves space assets and space missions at risk. Formal designation of space as a standalone critical infrastructure sector will secure the resilience of space assets and the services upon which national security and civilian life depend.

Visit www.competitionpolicyinternational.com for access to these articles and more!

Scan to Stay Connected!

Scan here to subscribe to CPI's
FREE daily newsletter.



01

CRITICAL INFRASTRUCTURE

The United States has sixteen designated critical infrastructure sectors, including water, healthcare, finance, and the defense industrial base. These sectors provide “the essential services that underpin American society.”² The Patriot Act of 2001 defines critical infrastructure as “Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”³

Notably missing from the designated sectors of critical infrastructure is the space industry. Space is no longer just the backdrop for science fiction, used solely for entertainment purposes. Space provides data for positioning, navigation, and timing (“PNT”), as well as communication, remote sensing, and missile warning, among other applications. Functions of the space industry directly enable and contribute to all sixteen sectors of critical infrastructure. Without space, the essential services that underpin American society would be severely disrupted if not crippled.

Despite the critical dependency of the domain, the space industry remains an unrecognized gap in the U.S. and global critical infrastructure strategy. The European Space Agency (“ESA”) Director General Josef Aschbacher declared at the international conference on cybersecurity of space assets, CYSAT 2025, that space is critical infrastructure and it needs to be officially designated as so globally.⁴ This sentiment was also expressed in a 2023 report by the Cyberspace Solarium Commission 2.0 which recommends the immediate designation of space as a sector.⁵

Despite repeated warnings, the U.S. has yet to formally designate space systems as critical infrastructure. This omission prevents unified governance, limits resource allocation, and leaves response protocols ambiguous in the event of a cyberattack. However, Executive Order 14144, directs the Committee on National Security Systems (“CNSS”) to review and update policies on cybersecurity of space systems and to identify cyber defense requirements for federal acquisition of space national security systems by fall of 2025.⁶ Hopefully, the CNSS will codify the support and resources needed to ensure the security and reliability required by space.

02

WHY CRITICAL INFRASTRUCTURE DESIGNATION MATTERS

Under the National Security Memorandum on Critical Infrastructure Security and Resilience, which designates which industries fall under critical infrastructure, the White House establishes a unified national effort to ensure the security and resilience of the sectors through eight principles and objectives:⁷

1. Shared-Responsibility
2. Risk-Based Approach
3. Minimum Requirements
4. Accountability
5. Information Exchange
6. Expertise and Technical Resources

2 Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (PPD-21) (Feb. 12, 2013), https://www.cisa.gov/sites/default/files/2023-01/ppd-21-critical-infrastructure-and-resilience-508_0.pdf (last visited June 19, 2025).

3 Pub. L. No. 107-56, 115 Stat. 272 (2001), <https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf> (last visited June 19, 2025).

4 Josef Aschbacher, Director General of ESA: Delivering Secure Space for Europe, Remarks at the CYSAT 2025 Conference on Cybersecurity for Space Assets (May 14, 2025).

5 Cyber Solarium Commission, Time to Designate Space Systems as Critical Infrastructure (2023), <https://cybersolarium.org/csc-2-0-reports/time-to-designate-space-systems-as-critical-infrastructure/>.

6 Strengthening and Promoting Innovation in the Nation’s Cybersecurity, 90 Fed. Reg. 3662 (Jan. 17, 2025), <https://www.federalregister.gov/documents/2025/01/17/2025-01470/strengthening-and-promoting-innovation-in-the-nations-cybersecurity> (last visited June 19, 2025).

7 National Security Memorandum on Critical Infrastructure Security and Resilience, Presidential Actions, The White House (Apr. 30, 2024), <https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/> (last visited June 19, 2025).

7. International Engagement
8. Policy Alignment

These eight principles guide the development and implementation of policies and directives that unlock dedicated federal funding, workforce, and other resources required to keep each designated sector capable of delivering critical services to the population. By formally designating space as critical infrastructure, these principles would strengthen the security and resilience of space, ensuring the continuity of services required for national security and everyday life.

Shared Responsibility is an imperative for space. Earlier this year, the world witnessed the government's inability to bring two astronauts home after being stranded in space for nine months. Through the coordination and partnership with a commercial organization, they safely returned to Earth.⁸ Space is a shared territory. As space operations continue to expand in mission and operations, a coordinated understanding of shared responsibility needs to be established among international partners, the commercial sector, and government organizations.

A risk-based approach assesses the security posture of a sector to ensure minimal impact to services in the case of an adverse event. This principle also drives the national efforts based on the relationship between the sector and national security. Nothing could demonstrate the need for space to be designated as a sector more than the Executive Order 14186, which directs the development of a missile defense system, Golden Dome, to protect the U.S. from incoming ballistic, hypersonic, cruise missiles, and other advanced aerial attacks.”⁹ Without the space-based systems used for sensing and tracking, the Golden Dome will not work, and national security would be compromised. Impaired space operations would also degrade communication, response, and emergency services.

Minimum requirements for risk management are established for sectors. The space industry is expanding in missions and partners. Space tourism, space mining, and space colonization are all current and evolving industries that are being supported through commercial organizations. However, space is not a silo and cannot be compartmentalized; all missions and operations require deconfliction and can have cascading consequences if the

varying levels of security and resilience standards are not established and met. To prevent a vulnerable system from becoming a global problem, minimal cybersecurity standards must be established for trusted supply-chain provenance, strong encryption, rigorous acceptance testing, secure update processes, and proven incident-response plans.

Accountability is another imperative for the space industry. As previously mentioned, public and private organizations are developing space systems that must be safe, secure, and resilient. Without a formal designation as a sector, the space industry risks insecure and vulnerable supply chains that may lead to compromise and disaster for national security. As a designated sector, the space industry would have a Sector Risk Management Agency with an Accountable Senior Officer who would identify best practices and bind every supplier and operator to the same security and resilience standards. This would ensure each component provider is directly responsible for delivering secure and resilient components.¹⁰

A risk-based approach assesses the security posture of a sector to ensure minimal impact to services in the case of an adverse event

Information Exchange for space systems is currently through a membership process under the Space Information Sharing Analysis Center (“ISAC”). Essentially, the Space ISAC has become the central hub of space operations, coordinating and sharing information among its global commercial and government members. During a Space ISAC tabletop exercise held at CYAT 2025, the need for established relationships, communication, and formalized coordination was evident. The exercise revealed gaps in information sharing, jurisdictional confusion, and unaligned response plans.¹¹ As a designated sector, the space industry would establish formal coordination protocols with the government, other commercial organizations, and other nations. This would include sharing and disseminating integrated threat reporting,

8 Stranded Astronauts Butch Wilmore, Suni Williams Safely Return to Earth, N.Y. Post (Mar. 18, 2025), <https://nypost.com/2025/03/18/us-news/stranded-astronauts-butch-wilmore-suni-williams-safely-return-to-earth/> (last visited June 19, 2025).

9 Donald J. Trump, The Iron Dome for America, Presidential Actions, The White House (Jan. 27, 2025), <https://www.whitehouse.gov/presidential-actions/2025/01/the-iron-dome-for-america/> (last visited June 19, 2025).

10 National Security Memorandum on Critical Infrastructure Security and Resilience, *supra* note 7.

11 CYSAT 2025, International Conference on Cybersecurity of Space Assets (May 2025).

tearline-enabled declassification of intelligence, formal notification pathways, and coordination among various sectors and global partners.¹²

Expertise and Technical Resources are critical to the space industry. If space were a designated sector, a Sector Risk Management Agency supported by its partners would be assigned to the sector to provide technical assistance, best practices, government-furnished capabilities, training, and outreach. This would provide the foundation to ensure systems are secure and resilient.

International Engagement has traditionally been government-to-government through diplomatic and established communication channels. Today, however, commercial organizations also operate across borders and require international engagement with other commercial and government organizations. This means creating forums where public and private operators, start-ups, and satellite manufacturers can collaborate directly with foreign regulators, allied space agencies, and organizations like the ESA and Space ISAC.

Policy Alignment ensures that sectors have cybersecurity and resilience initiatives that complement federal and regulatory requirements and frameworks, such as continuity of government, incident response, and spectrum management. This eliminates gaps, reduces duplication, contributes to efficiency, and ultimately enhances mission security and national security. The space industry not only must meet the multiple policies of all sectors, it also possesses many dual-use technologies. Dual use provides civilian and defense capabilities; for example, the Global Positioning System provides civilians with the navigational information needed to get around in a new city and the critical navigational information required for missile defense. The dual-use nature of modern space systems has profound policy implications. Governments can no longer rely on outdated regulatory boundaries that separate civil and military operations. Instead, they must establish governance models that recognize the interdependence of commercial innovation and national security interests.¹³

03 SPACE

Space is not only critical to society, it is unique in many ways. Aschbacher characterized the space industry as hybrid, distributed, remote, and persistent. All of these traits complicate the cybersecurity of space assets by expanding the attack surface area and complicating defense coordination.¹⁴

The hybrid nature of space consists of physical systems with digital infrastructure across various environments and nations. Space architecture integrates space segments, ground stations, user equipment, and various data links that all rely on physical and digital components, creating multiple attack vectors for adversaries. This web of dependencies includes multiple technologies and domains controlled and secured by various system owners, complicating the coordination and uniformity of security. As cyber threats increase, the need for coordinated and cross-disciplinary defense becomes essential.¹⁵

The space industry is also highly distributed. Space assets require global placement of the ground segments, while the space segments are literally out of this world. Space systems rely on multinational architectures, decentralized command hierarchies, and distributed systems, creating multiple critical dependencies.¹⁶

Related to the distribution of the assets is the remoteness of the space segments. Most Earth-based systems rely heavily on physical controls like guns, gates, and guards as a first layer of defense for the system. Cyber protections generally assume an inherent layer of physical defense, which space systems do not have. The lack of physical controls in space allows for adversarial systems to deny, degrade, disrupt, deceive, or destroy space assets through physical and cyber means.¹⁷

The space industry is also persistent. Satellites are built to last decades with minimal manual maintenance. Once launched, physically accessing a space segment or just shutting the mission down to update software and firm-

¹² National Security Memorandum on Critical Infrastructure Security and Resilience, *supra* note 7.

¹³ Josef Aschbacher, *supra* note 4.

¹⁴ *Ibid.*

¹⁵ *Ibid.*

¹⁶ Deloitte Insights, Critical Need for Cybersecurity in Space Systems, Deloitte Insights (Feb. 2025), <https://www2.deloitte.com/us/en/insights/industry/public-sector/critical-need-for-cybersecurity-in-space-systems.html> (last visited June 19, 2025).

¹⁷ *Ibid.*

ware after vulnerabilities are discovered, or replacing hardware, is not feasible in the traditional sense. As a result, vulnerabilities can persist unmitigated for extended periods.

04

IMMEDIATE CYBERSECURITY NEEDS FOR SPACE

In combination with the hybrid, distributed, remote, and persistent nature of space, space enables a distinct set of threats and vulnerabilities, including radio frequency attacks, supply chain vulnerabilities, and encryption concerns.

Although publicly disclosed incidents remain limited, research from Switzerland's leading science and technology university, ETH Zurich, estimates fewer than 600 space attacks have been officially recorded since 2000. Most incidents are confidential. The 600 figure is likely drastically underestimated, as NASA alone reported almost 1,800 incidents in 2020, with most of these remaining unanalyzed in the public domain.¹⁸

A. Radio Frequency Attacks

As discussed earlier, some space assets are remote and lack physical protection. Cyber-attacks on space assets do not require breaching a firewall. Space signals are readily available and accessible, allowing for easy manipulation with no barriers to their use. Inaccurate space signals, known as spoofing, can be generated to deceive receivers by providing them with incorrect data. In May of this year, a container ship ran aground in the Red Sea after what was believed to be a spoofing attack on its global navigation satellite system.¹⁹

Another form of signal manipulation involves generating a high volume of competing signals to drown out legitimate

signals, resulting in jamming. This causes the receiver to receive no signal. In June of this year, an oil tanker collided with another oil tanker in the Straits of Hormuz, which is believed to have been caused by a spoofing or jamming incident.²⁰

In addition to spoofing and jamming attacks, space systems are also susceptible to other radio frequency attacks. Electronic warfare can induce smart frequency hopping, or deceptive pulsing to degrade various channels without jamming them.²¹

B. Supply Chain Vulnerabilities

The supply chain of space assets, coupled with the remote characteristic of the space industry, exacerbates the need for transparency in software and hardware. Modern space systems rely on intricate, multinational supply chains involving dozens, if not hundreds of suppliers. Each layer of the supply chain introduces potential vulnerabilities that adversaries can exploit.

For software, vulnerabilities may be deeply embedded in unverified open-source libraries. Software may also contain dormant or passive nefarious code embedded into supportive components. Without a software bill of materials ("SBOM") requirement when acquiring new software, asset owners are unaware of what they are getting. Unlike Earth-based systems, performing software updates becomes very difficult once the asset has launched.

For hardware, similar problems exist. If the asset owner is not aware of all the components, including provenance, vulnerabilities may be built into the system and cause significant damage once it is deployed. Hardware component risks include the use of counterfeit parts, supply chain availability, and tampering. Space also introduces the element of radiation. Although not an attack, it is a vulnerability of non-resilient systems. The radiation in space causes single-event upsets ("SEUs") in semiconductor devices. SEUs can induce bit-flips in memory or control logic. This means in a system that runs on ones and zeros, some ones will spontaneously turn into zeros and some zeros will turn into ones. This fundamentally changes the instructions provided to the system, degrading system performance or creating exploitable states. ESA notes that many commercial off-the-shelf chips used in small satellites are not radiation-hardened,

18 Steven Soarez, *Le Secteur Spatial Face aux Cybermenaces*, Innovations (June 12, 2025), <https://innovations.fr/le-secteur-spatial-face-aux-cybermenaces/> (last visited June 19, 2025).

19 MSC Antonia Grounding in the Red Sea Attributed to Suspected GNSS Spoofing, Inside GNSS (May 15, 2025), <https://insidegnss.com/msc-antonia-grounding-in-the-red-sea-attributed-to-suspected-gps-spoofing/> (last visited June 19, 2025).

20 Visual Analysis: GPS Interference Raises Risk of Accidents in Strait of Hormuz, Financial Times (June 2025), https://www.ft.com/content/ac3c571f-2c4e-4c57-b582-21e2b27170f8?utm_source=chatgpt.com (last visited June 19, 2025).

21 IEEE Xplore, Document No. 9954562, <https://ieeexplore.ieee.org/document/9954562> (last visited June 19, 2025).

increasing the risk of such incidents being exploited during crises.²²

A resounding theme among the space community at this year's CYSAT conference emphasized that the lack of transparency in both hardware and software components is now a central concern for space resilience posture. Undisclosed or poorly documented dependencies can undermine incident response, delay patching efforts, and introduce unacceptable levels of uncertainty into critical infrastructure operations. In a domain where many systems are physically inaccessible once deployed, visibility at the design and integration points becomes essential.²³

C. Encryption Concerns

ESA has declared quantum-safe communications a strategic priority.²⁴ Space infrastructure must not only be secure from today's threats but also from tomorrow's threats. Space assets must be future-proofed against the emerging era of quantum computing. Quantum computing is a double-edged sword, it promises scientific leaps we can barely imagine, yet it also threatens to upend the very encryption shields we have trusted for decades.²⁵

Modern satellites lean on two work-horse encryption schemes, the venerable Rivest–Shamir–Adleman (“RSA”) protocol and its nimble cousin, Elliptic-Curve Cryptography (“ECC”). Both keep data safe by posing mathematical puzzles that would take today's computers practically forever to solve. RSA hides secrets behind the chore of factoring enormous composite numbers, while ECC buries them inside the equally stubborn elliptic-curve discrete-log problem.²⁶ Both protections could be compromised once sufficiently powerful quantum computers become available.

Analysts warn of a potential “Q-Day” early in the 2030s, when adversaries may use quantum capabilities to defeat current satellite encryption.²⁷ If sensitive down-links are intercepted now and stored for later decryption, future quantum attacks could expose mission-critical telemetry or even

enable remote takeover of spacecraft. Because on-orbit hardware is notoriously hard to patch, crypto-agility, the ability to swap algorithms after launch, has become best practice. In practical terms, that means selecting ciphers that are already quantum-resistant, or at minimum, structuring flight software so that new algorithms can be uploaded when standards mature.

05 CONCLUSION

Space is now an indispensable requirement to global critical infrastructure and should be treated as such. Neither governments nor industry can afford to treat space cybersecurity as an afterthought; complacency in the face of rising multi-vector threats will invite cascading disruptions that ripple across vital sectors worldwide. The case for proactive, risk-informed policy is clear and urgent. Formal global recognition of space as a critical infrastructure sector would not be a symbolic gesture but a pragmatic step to ensure the resources required to establish a secure and resilient capability that national security depends.

If an adversary were to deny, degrade, disrupt, destroy, or deceive satellite systems, the cascading effects could impact national security, as well as other services. The ability to safeguard orbit is not just about technology; it is a matter of national security and strategic survival. The necessary steps are clear, and the means to execute them are at hand. The final challenge is not one of technology or knowledge but of will. Protecting the high ground of orbit in the cyber age is entirely achievable. The tools and frameworks exist; now, all that remains is the political and institutional will to act. ■

²² European Space Agency, ESA Radiation Test Database, <https://esarad.esa.int/> (last visited June 19, 2025).

²³ Josef Aschbacher, *supra* note 4.

²⁴ Eur. Space Agency, ESA Partners with Polish Technology Company to Develop SATCOM Security Solution Using Post-Quantum Algorithms, ESA CONNECTIVITY (May 2025), <https://connectivity.esa.int/news/esa-partners-polish-technology-company-develop-satcom-security-solution-using-postquantum-algorithms>.

²⁵ Cellcrypt, Post-Quantum Cryptography and the Store-Now-Decrypt-Later Threat, CELLCRYPT (Apr. 2025), <https://www.cellcrypt.com/post/post-quantum-cryptography-and-the-store-now-decrypt-later-threat>.

²⁶ *Ibid.*

²⁷ Tech Monitor, Quantum Encryption Seeks Its First and Final Frontier, TECH MONITOR (May 2025), <https://www.techmonitor.ai/hardware/quantum/quantum-encryption-seeks-its-first-and-final-frontier?cf-view&cf-view>.

CPI SUBSCRIPTIONS

CPI reaches more than **35,000 readers** in over **150 countries** every day. Our online library houses over **23,000 papers**, articles and interviews.

Visit competitionpolicyinternational.com today to see our available plans and join CPI's global community of antitrust experts.

