



SPACE CYBERSECURITY WEEKLY WATCH

W10

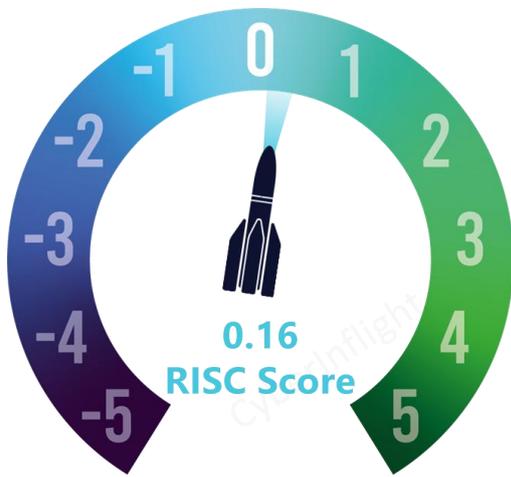
March 3 – 9, 2026

Timeframe: Weekly
of articles identified: 27
Est. time to read: 65 minutes

Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

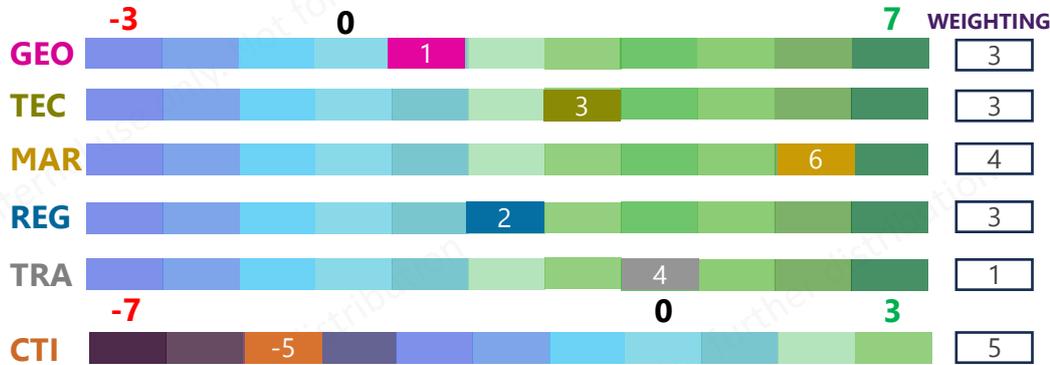
- **GEOPOLITICS**
- **TECHNOLOGY**
- **MARKET & COMPETITION**
- **REGULATION**
- **TRAINING & EDUCATION**
- **THREAT INTELLIGENCE**
- ★ **IMPORTANT NEWS**

RISC Score Assessment



↑ The RISC score for this watch is 0.16, up from last week, due to a good market balanced with an active threat and geopolitical climate

Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2026



This week, **Israel claimed a targeted strike on a Tehran compound housing Iran's cyber warfare headquarters and Intelligence Directorate.** While the operational impact on Iran's cyber capabilities remains unclear, the attack underscores the blurring line between kinetic and cyber warfare. On the regulatory side, the **Trump Administration unveiled a new U.S. Cyber Strategy,** prioritizing offensive cyber operations, federal network security, and critical infrastructure protection. The strategy also includes an executive order to combat cybercrime and fraud, signaling a shift toward proactive cyber deterrence and workforce strengthening to counter evolving digital threats. On the market front, **Lockheed Martin secured a contract to supply an anti-jamming payload for Japan's next-generation defense communications satellite,** developed by Mitsubishi Electric. This payload will enhance interoperability with allied nations and bolster resistance to electronic interference, reflecting Japan's commitment to securing its military satellite communications in an era of growing orbital threats. On the threat landscape, a **penetration test revealed over 20 security flaws in a satellite receiver widely used by the U.S. Department of Defense, ESA,** and global critical infrastructure operators. The manufacturer, International Data Casting Corporation (IDC), failed to respond to disclosure attempts, exposing a critical gap in supply chain security and the urgent need for vendor accountability in space systems. On the technological side, **DARPA's ROCKN program is advancing GPS-free timekeeping for contested battlefields.** On the academic front, a **Chinese paper proposed a comprehensive literature review of cybersecurity in satellite networks** to propose the Sat-ATT&CK knowledge matrix to model attack chains across physical, network, and user layers.



GEOPOLITICS

Iranian hackers are forced to stay online during conflict

Iranian hackers were forced to stay online during conflict, according to reports. The conflict between Iran and Israel has led to a cyber war, with both sides launching attacks on each other. According to reports, Iranian hackers were forced to stay online during the conflict, as they were unable to disconnect from the grid. This was due to the fact that the grid is a critical part of Iran's infrastructure, and it is essential for the country's economy and military operations.

Source: [InfosecWiki](#)



Report: 2026 The Great Game falls

The 2026 report on the Great Game falls, according to reports. The report, which was published by the RAND Corporation, examines the global power struggle between the United States and China. It argues that the Great Game, a term used to describe the competition for power and influence between the United States and Russia in the late 19th and early 20th centuries, is being played out again between the United States and China. The report predicts that the United States will emerge as the winner of the Great Game, but it also warns that the competition will be intense and could lead to a global conflict.

Source: [InfosecWiki](#)



★ Israel claims it 'struck' Iran's cyber warfare headquarters

Israel has claimed a successful strike on a Tehran-based compound that housed Iran's "cyber warfare headquarters" and the "Intelligence Directorate," among others. The impact of this, however, on Iran's cyber capabilities remains unclear.

#Israel #Iran

Source: [The Cyber Express](#)



The US says it destroyed Iran's space command. Reports say it wasn't much of a threat.

The US says it destroyed Iran's space command, reports say it wasn't much of a threat. The US military announced that it had destroyed a facility in Iran that it claimed was a space command center. The facility was said to be a key part of Iran's space program, and its destruction was seen as a significant blow to Iran's space capabilities. However, some experts argue that the facility was not as important as the US claimed, and that Iran's space program is still in its early stages.

Source: [InfosecWiki](#)



South Korea, U.S. Navy hold off annual joint freedom of navigation exercises

South Korea and the U.S. Navy have held off annual joint freedom of navigation exercises. The exercises, which are a key part of the alliance between the two countries, were postponed due to concerns over the safety of the ships involved. The exercises are a way for the two countries to demonstrate their commitment to freedom of navigation in the South China Sea, a region of strategic importance.

Source: [InfosecWiki](#)



REGULATION

The Trump DOJ announces regulations over 5G space tech use

The Trump DOJ has announced regulations over 5G space tech use. The regulations, which were announced on Friday, require 5G providers to disclose to the DOJ any information that they receive from their customers that could be used for national security purposes. The regulations also require 5G providers to take steps to protect their networks from cyberattacks.

Source: [InfosecWiki](#)



★ Trump Administration Unveils New Cyber Strategy for America

President Donald Trump released his administration's cyber strategy Friday, promoting offense operations in cyberspace, securing federal networks and critical infrastructure, streamlining regulations, leveraging emerging technologies and strengthening the cybersecurity workforce. Trump also signed an executive order Friday directing agencies to take action to combat cybercrime and fraud. #CyberStrategy #US

Sources: [CyberScoop](#), [White House](#), [Infosecurity Magazine](#)



MARKET & COMPETITION

European Commission leads partners with joint capital to support next generation defense and space technologies in Europe

The European Commission has led a group of partners to launch a joint capital fund to support next generation defense and space technologies in Europe. The fund, which is being managed by the European Investment Bank, will provide financing for a wide range of projects, including the development of new technologies and the strengthening of the defense and space sectors. The fund is seen as a key part of the European Union's strategy to become a global leader in defense and space technologies.

Source: [InfosecWiki](#)





MARKET & COMPETITION



Lockheed Martin to support Japan's next-generation defense communications satellite with anti-jamming capability

Lockheed Martin, will provide a robust anti-jamming payload for Japan's Next-Generation Defense Satellite Communication System which was awarded to Mitsubishi Electric by the Japan Ministry of Defense. Serving as a mission partner to Mitsubishi Electric, Lockheed Martin's advanced payload will help maximize the satellite's capabilities. The payload will provide interoperability with allied and partner nations and enhance the satellite communications' resistance to interference. **#Contract #AntiJamming**

Sources: [Lockheed Martin](#), [Market Screener](#)



Spain's satellite communications capabilities: a European alternative for secure space-based connectivity & operational resilience

Spain's satellite communications capabilities are a European alternative for secure space-based connectivity & operational resilience. The satellite communications capabilities are a European alternative for secure space-based connectivity & operational resilience. The satellite communications capabilities are a European alternative for secure space-based connectivity & operational resilience.

Sources: [For Internal Use Only](#)



European partners advance coverage defense space capability with Starlink

European partners advance coverage defense space capability with Starlink. The satellite communications capabilities are a European alternative for secure space-based connectivity & operational resilience. The satellite communications capabilities are a European alternative for secure space-based connectivity & operational resilience.

Sources: [For Internal Use Only](#)



Spain aims to make up and align its efforts with government backing for better coverage

Spain aims to make up and align its efforts with government backing for better coverage. The satellite communications capabilities are a European alternative for secure space-based connectivity & operational resilience. The satellite communications capabilities are a European alternative for secure space-based connectivity & operational resilience.

Sources: [For Internal Use Only](#)



Lockheed Martin becomes the only USMC (and) certified electronics distributor supporting U.S. strategic and defense programs

Lockheed Martin becomes the only USMC (and) certified electronics distributor supporting U.S. strategic and defense programs. The satellite communications capabilities are a European alternative for secure space-based connectivity & operational resilience. The satellite communications capabilities are a European alternative for secure space-based connectivity & operational resilience.

Sources: [For Internal Use Only](#)



USMC and USNavy (and) certified electronics distributor

USMC and USNavy (and) certified electronics distributor. The satellite communications capabilities are a European alternative for secure space-based connectivity & operational resilience. The satellite communications capabilities are a European alternative for secure space-based connectivity & operational resilience.

Sources: [For Internal Use Only](#)



USMC and USNavy (and) certified electronics distributor in the US

USMC and USNavy (and) certified electronics distributor in the US. The satellite communications capabilities are a European alternative for secure space-based connectivity & operational resilience. The satellite communications capabilities are a European alternative for secure space-based connectivity & operational resilience.

Sources: [For Internal Use Only](#)



THREAT INTELLIGENCE

Portuguese defense system space threat counter role in base operations

Portuguese defense system space threat counter role in base operations. The satellite communications capabilities are a European alternative for secure space-based connectivity & operational resilience. The satellite communications capabilities are a European alternative for secure space-based connectivity & operational resilience.

Sources: [For Internal Use Only](#)





THREAT INTELLIGENCE

ESA's Galileo is emerging as an increasingly prominent — and troubling — source of spy

... of the first of these satellites, which is the system's main ground station, has been found to have

... indicating that the satellite's data is being used to spy on other satellites. The satellite

... a host of other spy-related activities, including the tracking of other satellites and the

... of the satellite's data.



European space launch failures further undermine US infrastructure and defense supply chain

... of the European Space Agency (ESA) has been found to have a number of security flaws

... of the satellite's data.



A satellite receiver trusted by Pentagon, ESA has more than 20 security flaws — and the maker never responded

A penetration tester found more than 20 vulnerabilities in a satellite receiver deployed by the U.S. Department of Defense (also referred to as the Department of War), the European Space Agency, and other critical infrastructure operators worldwide — and the device's manufacturer, International Data Casting Corporation (IDC), did not respond to a single disclosure attempt over several months. **#CVE #SFX2100**

Sources: [The Cyber Express](#), [CyboWatch](#)

The US Space Force satellite communication provider is 'no longer in touch' — Russian hackers

... of the satellite's data.



TECHNOLOGY



U.S. Defense Program Advances GPS-free timekeeping for contested battlefield

The U.S. DARPA is advancing the ROCKN (Robust Optical Clock Network) program to develop highly precise timekeeping systems that can operate without GPS. The initiative aims to ensure reliable synchronization for military operations in environments where GPS signals may be jammed or denied. By using advanced optical clocks and networked timing technologies, the program seeks to maintain ultra-precise coordination of sensors, communications, and targeting systems on contested battlefields. **#ROCKN #GPS**

Source: [Defense Mirror](#)



Russian military's first satellite will have 40% battery performance

... of the satellite's data.



TRAINING & EDUCATION

... of the satellite's data.



