

SPACE CYBERSECURITY WEEKLY WATCH

W23

June 2 – June 8, 2026

Timeframe: Weekly

of news identified: 43

Est. time to read: 85 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.

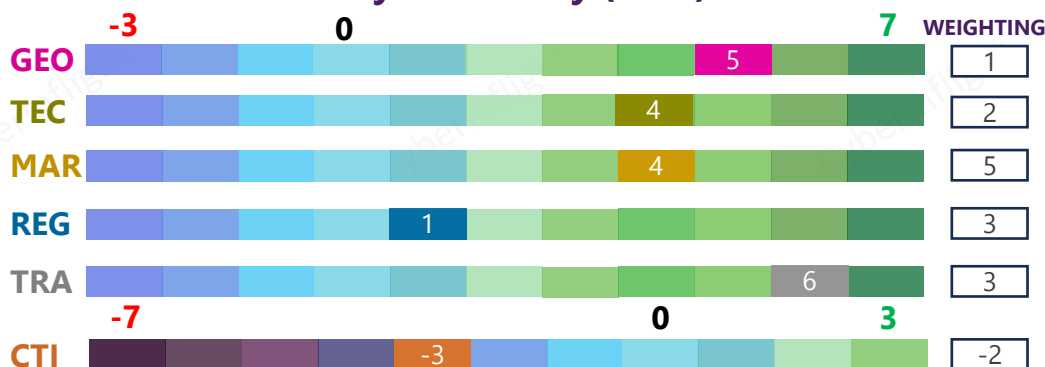
- GEOPOLITICS
- TECHNOLOGY
- MARKET & COMPETITION
- REGULATION
- TRAINING & EDUCATION
- THREAT INTELLIGENCE
- ★ IMPORTANT NEWS

RISC Score Assessment

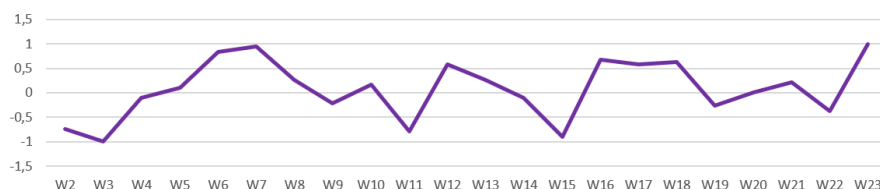


The RISC score for this watch is 1.0, up from 1.37 last week. This strong increase is especially due to a better threat climate, and several positive news, notably in Training and education.

Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2026



This week, on the geopolitical front, Commander of the Peruvian Air Force Space and Cyberspace Command, Maj. Gen. Rodríguez, spoke during the Space Conference of the Americas 2026, held in Miami, Florida, about the **development of Peruvian sovereign space capabilities, the protection of critical infrastructure, cooperation with the United States, and the growing role of cyberspace in regional security**. On the regulation side, an article examines the link between **commercial space technology shaping the Iran war, and the law that struggles to keep up**. The United Nations' Outer Space Treaty, the UN Charter itself, and international humanitarian law all apply to warfare in orbit. But **the Iran war shows how real-world practice is advancing faster than these legal frameworks**. On the market front, the Canadian Department of National Defense (DND) and the Canadian Armed Forces (CAF) are seeking **innovative research and development (R&D) solutions to provide a flat-satellite (flatsat) platform for cybersecurity experimentation**. On threat intelligence-related topics, on 12 May 2026, the newspaper Haaretz revealed that **two Israeli-linked companies had developed systems capable of locating Starlink terminals worldwide and linking many of them to identifiable users** without intercepting communications or breaking Starlink's encryption, therefore compromising Starlink's anonymity. On the technological side, **QuDef has launched SQOUT**, a platform designed to assess, model, and monitor security risks in Quantum Key Distribution (QKD) and other quantum communication systems as deployments expand across government and enterprise networks. Lastly, in the training category, **an interview with one of the major cybersecurity experts of the French Space Agency (CNES), Julien Airaud, Senior Cybersecurity Expert at CNES**, was released within the MISC magazine.

GEOPOLITICS

Cyber war wars focusing satellites and critical infrastructure

Cyber war wars are now considered a critical infrastructure, and often with a high technological and military use, increasing the risk of cyber war wars. The cyber war wars are now considered a critical infrastructure, and often with a high technological and military use, increasing the risk of cyber war wars. The cyber war wars are now considered a critical infrastructure, and often with a high technological and military use, increasing the risk of cyber war wars.

Source: [CyberInflight](#)

Spatial data has become a weapon of war in the U.S. from war

The collection of images by U.S. satellites in 2011, reported a fundamental change in the way the U.S. military and intelligence community view the world. The collection of images by U.S. satellites in 2011, reported a fundamental change in the way the U.S. military and intelligence community view the world. The collection of images by U.S. satellites in 2011, reported a fundamental change in the way the U.S. military and intelligence community view the world.

Source: [CyberInflight](#)

Self wants to integrate cyber in all operations, and integrate security into it

Information is becoming more and more important in the battlefield, so having the ability to integrate space cyber and other war domains efforts to be able to degrade that information advantage is something that's going to be critical and fundamental to any future conflict going forward. [Mikael Malm](#)

Source: [CyberInflight](#)

In space, we can't defend what we can't see

The idea of seeing, from any point in space, is what we can't see. The idea of seeing, from any point in space, is what we can't see. The idea of seeing, from any point in space, is what we can't see. The idea of seeing, from any point in space, is what we can't see.

Source: [CyberInflight](#)

★ Peru bets on sovereign capabilities in the space and cyber domains

With more than 30 years of service in the Peruvian Air Force, Major General Mariano Nieves Rodríguez Llerena now leads the country's efforts in two of the most strategic and emerging domains of modern defense: space and cyberspace. Commander of the Peruvian Air Force Space and Cyberspace Command and a fighter pilot with extensive international cooperation experience, Maj. Gen. Rodríguez spoke with Diálogo during the Space Conference of the Americas 2026, held in Miami, Florida, about the development of sovereign space capabilities, the protection of critical infrastructure, cooperation with the United States, and the growing role of cyberspace in regional security. [#Peru #Defense](#)

Source: [Diálogo Américas](#)

Cyber dimension of war and implications for Bangladesh

The ongoing cyber war has introduced a new and alarming dimension to modern warfare. The deep integration of cyber war with conventional war has created a new and alarming dimension to modern warfare. The deep integration of cyber war with conventional war has created a new and alarming dimension to modern warfare.

Source: [CyberInflight](#)

The silent battlefield: How cyber vulnerabilities are shaping modern space warfare

Space has become the growing convergence between cyber war and space infrastructure. The space has become the growing convergence between cyber war and space infrastructure. The space has become the growing convergence between cyber war and space infrastructure.

Source: [CyberInflight](#)

Space has never been more important for global security and prosperity

Space is one of the most important and yet least understood areas of global affairs. Space is one of the most important and yet least understood areas of global affairs. Space is one of the most important and yet least understood areas of global affairs.

Source: [CyberInflight](#)

High profile drone and cyber warfare: The new face of modern conflict - Spain

Drone war and cyber war are now a part of modern conflict. Drone war and cyber war are now a part of modern conflict. Drone war and cyber war are now a part of modern conflict.

Source: [CyberInflight](#)



GEOPOLITICS

The space domain and the defense of Europe

Europe is getting more aware of the defense of Europe than it used to be. In recent years, a number of factors have contributed to this: the growing importance of space in military operations, the need to protect Europe's air, sea, and land forces, the increasing competition in space, the rise of China and Russia as space powers, and the growing awareness of the importance of space for Europe's security. As a result, Europe is now investing more in space defense capabilities.

Source: [EPA](#)



REGULATION



Commercial space technology is shaping the Iran war – the law can't keep up

This combination of advanced battlefield tactics and the rapid commercialization of space technology, as well as the erosion of the old rules-based order in general, means international law is now falling well behind. **#EpicFury #SpaceLaw**

Source: [News Daily](#)



India with its technology the cyber gateway to Russia

India is a major cyber power. It is a technical power, a cyber power that is able to develop, produce, and use cyber weapons. India is also a strategic power, a power that is able to use cyber weapons to achieve its strategic goals. India is a cyber power that is able to use cyber weapons to achieve its strategic goals. India is a cyber power that is able to use cyber weapons to achieve its strategic goals.

Source: [The Indian Express](#)

MARKET & COMPETITION



Cybersecurity in satellite systems

The Department of National Defense (DND) and the Canadian Armed Forces (CAF) are seeking innovative research and development (R&D) solutions to provide a flat-satellite (flatsat) platform for cybersecurity experimentation.

#DND #Canada

Sources: [Government of Canada](#), [SpaceQ](#)



Space on board and secure control center for future satellite communications systems (SSTC) is a key to success

The objective of the project is to develop a secure control center for future satellite communications systems (SSTC) that is able to provide secure control and management of the system. The project is a key to success for the future of satellite communications systems.

Source: [ESA](#)



SpaceX will provide local organizations with a three pillar approach

SpaceX will provide local organizations with a three pillar approach to secure control and management of the system. The project is a key to success for the future of satellite communications systems.

Source: [ESA](#)



New year contract targets 100% modernization for U.S. military 2025 enterprise

The new year contract targets 100% modernization for U.S. military 2025 enterprise. The project is a key to success for the future of satellite communications systems.

Source: [The United States Air Force](#)



ESA's European Space 10, according to its position on the control center and SpaceQ's 100% modernization

ESA's European Space 10, according to its position on the control center and SpaceQ's 100% modernization. The project is a key to success for the future of satellite communications systems.

Source: [ESA](#)



MARKET & COMPETITION

Space Security and Global Information Market Research Report 2026

A general overview of the space cybersecurity market by Market name: [Market Research](#)

Source: [Market name](#)

THREAT INTELLIGENCE

Space Force wants to use tactical GPS systems for electronic warfare

The Space Force wants to make its electronic warfare capabilities more visible by building the new tactical GPS system in the next few years. The system will be used to track and identify GPS signals in order to identify and track GPS signals. [Department of Defense](#)

Source: [Department of Defense](#)

The uplink of GPS jamming

In May 2026, a GPS jammer was found in the sky over the Pacific Ocean. The jammer was found to be a GPS jammer. The jammer was found to be a GPS jammer. The jammer was found to be a GPS jammer. [Department of Defense](#)

Source: [Department of Defense](#)

Researchers attack the National Aeronautics Research Institute of Thailand

In May 2026, the National Aeronautics Research Institute of Thailand was attacked by a group of researchers. The researchers were from the National Aeronautics Research Institute of Thailand. [Department of Defense](#)

Source: [Department of Defense](#)

What attack targeting the Ukrainian satellite system

In May 2026, the Ukrainian satellite system was targeted by a group of researchers. The researchers were from the Ukrainian satellite system. [Department of Defense](#)

Source: [Department of Defense](#)



Digital kill chain: Starlink anonymity compromised

On 12 May 2026, Haaretz revealed that two Israeli-linked companies had developed systems capable of locating Starlink terminals worldwide and linking many of them to identifiable users without intercepting communications or breaking Starlink's encryption. [#Starlink #KillChain](#)

Source: [The Cradle](#)

Reported Russian hackers breach US Space Force official's Instagram, share geo-tagged content and other data

A report from a US Space Force official's Instagram account was hacked by Russian hackers. The hackers were from the Russian satellite system. [Department of Defense](#)

Source: [Department of Defense](#)

Russian satellites have been jamming GPS signals across Europe, according to

Russian satellites have been jamming GPS signals across Europe, according to a report from a US Space Force official. The report was from the US Space Force official. [Department of Defense](#)

Source: [Department of Defense](#)

TECHNOLOGY

Antenna array could provide protected tactical satellite communications in low Earth orbit

A new antenna array could provide protected tactical satellite communications in low Earth orbit. The antenna array is a new technology. [Department of Defense](#)

Source: [Department of Defense](#)

TECHNOLOGY

Space Space Technologies successfully performed an in-orbit demonstration of their software-defined radio (SDR) and RF system

Space Space Technologies successfully performed an in-orbit demonstration of their software-defined radio (SDR) and RF system. The demonstration represents an important step towards interoperable networks in space and will be followed by further demonstrations and experiments, paving the way for robust and secure space communications, including high-speed quantum cryptography (QKD) around orbital data operations. [SDR SDRS SDR](#)

Source: [SDR SDRS SDR](#)



Sweden may secure the transport, but also secure (SDR) data?

Sweden may secure the transport, but also secure (SDR) data? The article discusses the challenges of securing space communications, from a cryptographic system to operations infrastructure, including network security and data protection. It also mentions the need for a secure (SDR) data.

Source: [Sweden SDR](#)

Sweden performing interference at different flight altitudes combined with a prototype device - results already reported before Helsinki

Sweden performing interference at different flight altitudes combined with a prototype device - results already reported before Helsinki. The article discusses the challenges of securing space communications, from a cryptographic system to operations infrastructure, including network security and data protection. It also mentions the need for a secure (SDR) data.

Source: [Sweden SDR](#)



Source: [Sweden SDR](#)

Small supercharges in space power suggest 40 systems with 100W SDR flow

Small supercharges in space power suggest 40 systems with 100W SDR flow. The article discusses the challenges of securing space communications, from a cryptographic system to operations infrastructure, including network security and data protection. It also mentions the need for a secure (SDR) data.

Source: [Small supercharges in space power suggest 40 systems with 100W SDR flow](#)



RF cryptography is increasingly vital in securing space defense

RF cryptography is increasingly vital in securing space defense. The article discusses the challenges of securing space communications, from a cryptographic system to operations infrastructure, including network security and data protection. It also mentions the need for a secure (SDR) data.

Source: [RF cryptography is increasingly vital in securing space defense](#)

The public you can't push

The public you can't push. The article discusses the challenges of securing space communications, from a cryptographic system to operations infrastructure, including network security and data protection. It also mentions the need for a secure (SDR) data.

Source: [The public you can't push](#)



QuDef launches Quantum Threat Intelligence Platform for QKD and quantum communication systems

QuDef has launched SQOUT, a platform designed to assess, model, and monitor security risks in Quantum Key Distribution (QKD) and other quantum communication systems as deployments expand across government and enterprise networks. **#QKD #QuDef**

Source: [Quantum Insider](#)



Sweden Quantum Communications

Sweden Quantum Communications. The article discusses the challenges of securing space communications, from a cryptographic system to operations infrastructure, including network security and data protection. It also mentions the need for a secure (SDR) data.

Source: [Sweden Quantum Communications](#)



An interview with one of the major cybersecurity experts of the French Space Agency within the MISC magazine.



© 2000 Cybernetics, Inc. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or by any information storage and retrieval system, without prior written permission from Cybernetics, Inc. For more information, contact Cybernetics, Inc., 10000 Cybernetics Way, Suite 100, San Diego, CA 92121, USA. Tel: 619-591-1000. Fax: 619-591-1001. E-mail: info@cybernetics.com. Web: <http://www.cybernetics.com>

© 2000 The McGraw-Hill Companies. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or by any information storage and retrieval system, without prior written permission from The McGraw-Hill Companies, Inc.

University of Seattle Communications 2011-2012 Training Course is designed to equip professionals with advanced knowledge and practical skills to protect sensitive information and associated systems from emerging cyber threats.

© 2014 John Wiley & Sons, Ltd. *J. Forecast.* **34**, 1–12 (2015)
DOI: 10.1002/for

[illegible]

© 2015 Crossmark LLC. Republishing for physical and network attack detection is Strong, 2015

This is a book of real-world data on 100 innovations, and testing real-time security approaches from early on physical layer security, testing third party coverage of network layer and computer attacks in the paper, we present a new layer, lightweight enhanced fingerprinting framework that from various physical layer measurements will network layer data to detect possible of the computational network **9780 955 002**

TRAINING & EDUCATION

International Space Station (ISS) is the largest human-made structure in space, orbiting Earth at an altitude of approximately 400 kilometers. It serves as a laboratory for conducting scientific research, testing new technologies, and observing Earth from space. The ISS is a complex of modules, solar panels, and antennas, and it is the only artificial structure in space that has been continuously occupied by humans since its launch in 1998. The ISS is a symbol of international cooperation and the potential of space exploration.



CyberInflight is a Market Intelligence company dedicated to the topic of Space Cybersecurity. The company provides strategic market and research reports, bespoke consulting, market watch & OSINT researches and cybersecurity awareness training.

Contact us at: research@cyberinflight.com