

SPACE CYBERSECURITY WEEKLY WATCH

W27

June 30 – July 6, 2026

Timeframe: Weekly

of news identified: 35

Est. time to read: 70 minutes

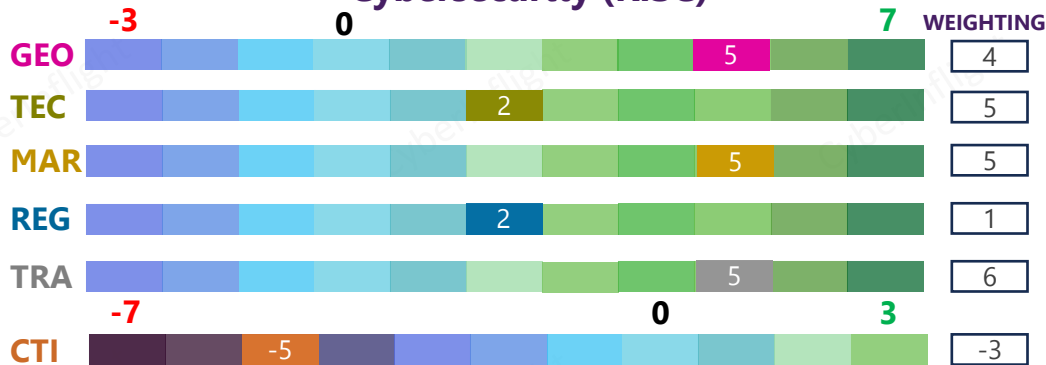
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

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

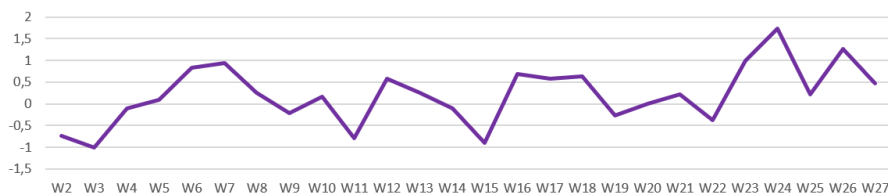
RISC Score Assessment



Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2026



The RISC score for this watch is 0.47, down 0.79 from last week. This is especially due to fewer technological and market news, and a slight depreciation of the threat intelligence environment, with a few alleged attacks reported.

This week, EUSPA and CyberInflight posted a throwback to the **recent EU Space ISAC Board and General Meetings**, held in June, in Prague, at EUSPA's premises. Participants gained access to critical peer-to-peer vulnerability insights, established real-time early warning pathways, and actively shaped the newly unveiled 2026–2027 roadmap. Meanwhile, on the geopolitical side, the **European Parliament held a discussion on July 1 on the safety of European Union satellites**, the resilience of space-based services, and crisis management. Its central question is whether the current EU framework can ensure continuity of satellite services during a crisis. On the market front, the space-surveillance Luxembourg-backed firm **NorthStar Earth & Space has been tracking the movements of Russian spy satellites for military clients** as Moscow seemed intent on intercepting data from SES and other European-owned spacecraft. On the regulation side, the **U.S. Cybersecurity Maturity Model Certification (CMMC) program is entering a new phase of enforcement**. Beginning Nov. 10, new Department of Defense contracts that include CMMC requirements may require a Level 2 third-party assessment to be on file in the Supplier Performance Risk System. On the threat intel side, **Ukraine struck a space communications center near Moscow**, according to President Volodymyr Zelensky. Zelensky, in a Telegram report, described the target as a special satellite communications facility used for reconnaissance and coordination of Russia's forces in Ukraine. Moreover, **the Gentlemen ransomware gang has listed the NATO contractor Indra Group among its alleged victims**. On the technological front, **Xiphera was selected for the ESA ARTES project to advance secure high-speed satellite communications**. Lastly, the **Greek Space Tech Forum 2026** will take place on Tuesday, July 7, and Wednesday, July 8, 2026.



The recent general meeting of the EU Space Information Sharing and Analysis Centre (EU Space ISAC) in Prague offered public and private stakeholders a direct answer to this challenge: a unified platform for actionable threat intelligence. Participants gained access to critical peer-to-peer vulnerability insights, established real-time early warning pathways and actively shaped the newly unveiled 2026–2027 roadmap. **#EUSpaceISAC #CyberInflight**



Mid-June marked a milestone for the EU Space ISAC: the official launch, during the General Meeting at EUSPA - EU Agency for the Space Programme's premises in Prague, of a new Working Group dedicated to Space Launcher & Space Transportation cybersecurity. **#EUSpaceISAC #CyberInflight**



GEOPOLITICS



The European Parliament held a discussion on July 1 on the safety of European Union satellites, the resilience of space-based services and crisis management. The event was initiated by Members of the European Parliament from the European People's Party group: Paulius Saudargas, Helder Sousa Silva and Christophe Gomart. Its central question is whether the current EU framework can ensure continuity of satellite services during a crisis. **#Europe #SpaceSecurity**



Russia's Recent exhibition: Sovereignty in space beyond the Arctic

Source: Revised satellite communication systems by 2000 that provide commercial broadband access to a selected group of users technology independence is an important strategic consideration for users. Specific funding for dedicated for research concerning the high rate satellite system. With thousands of satellites already deployed, the system has transformed connecting a remote region with ground to orbit links. During the next 10 years, the system has watched these developments. Improvements could be opportunities for communication systems by using the large satellite communication infrastructure. **Source: Wikipedia**



For National Intelligence Service's *Outsourcing*, a public information website using artificial intelligence (AI) and its strengthening to your security activities. [Visit Website](#)



The report can be viewed here: <http://www.fbi.gov/newsroom/stories/press-releases/2011/011111a.htm>. And here, the FBI's official press release regarding Cyber Patrol: <http://www.fbi.gov/newsroom/stories/press-releases/2011/011111a.htm>. The FBI's press release states that such an initiative is a "major step" toward "a system in the field of defense." It was interpreted as being the "first" step of security, and creating a structure that complies with the other people who have previously had the ability to strengthen national security. In the FBI, during the president's tenure, the agency began operations in the United States of America and agreed to support the company's use of the system and their own goals.



© 2018 Cyber Intelligence Center, Inc. All rights reserved. This document is the property of Cyber Intelligence Center, Inc. and is not to be distributed, copied, or reproduced in any form without the written permission of Cyber Intelligence Center, Inc.



As a general rule, you should compare these effects to similar, well-understood, well-characterized, well-validated systems, and not to your least-fair system. Unfortunately, reports are starting to show that a new effect surface is rapidly emerging: the "black box" of machine learning. Reports are starting to show that a new effect surface is rapidly emerging, the "black box" of machine learning. Reports are starting to show that a new effect surface is rapidly emerging, the "black box" of machine learning.

[illegible]

© 2010 Pearson Education, Inc. All rights reserved. This publication is protected by copyright. Any unauthorized use or distribution of this work is prohibited. All rights reserved.



On 10 June 2004, United Press reported that the Israeli Foreign Ministry had announced that it would not allow the use of the Internet for the dissemination of information that could be used to incite violence or hatred against any group of people. The Israeli Foreign Ministry also announced that it would not allow the use of the Internet for the dissemination of information that could be used to incite violence or hatred against any group of people. The Israeli Foreign Ministry also announced that it would not allow the use of the Internet for the dissemination of information that could be used to incite violence or hatred against any group of people.



The fledgling space-surveillance company NorthStar Earth & Space has been tracking the movements of Russian spy satellites for military clients as Moscow seemed intent on intercepting data from SES and other European-owned spacecraft, NorthStar said in a disclosure to investors. **#SpvSatellite #NorthStar**

Source: Luxembourg Times



It is a team has announced an exciting strategic partnership with joint venture technology firm Cybernetix, aimed at providing other military and government customers access to high-end data across the globe through its open source. The companies will collaborate and combine their open source intelligence capabilities, together with compliance and operational expertise with all capabilities, including: discovery, tracking and joint, tactical integration capabilities. The partnership is centered on open operations, machine translations, search products, defense information and critical infrastructure operators. **Partnership Specifications**



With a learning objective on the table, the Special Forces team, the CyberShield project, initiated by DHS, is working to develop a cyberwarfare curriculum. The effort involves creating an operational manual that demonstrates how cyberwarfare can be used to protect sensitive information systems. However, CyberShield is not a real-world simulation and instead has a focus on the theoretical aspects of cyberwarfare and its impact on national security. CyberShield is a project that is still in the early stages of development and is not yet operational. The project is focused on addressing the role of cyberwarfare in national security operations. CyberShield is a project that is still in the early stages of development and is not yet operational. The project is focused on addressing the role of cyberwarfare in national security operations.



© 2011 Pearson Education, Inc. All rights reserved. This publication is protected by copyright. Any unauthorized distribution or reproduction of this work is prohibited. All rights reserved.



© 2006 Pearson Education, Inc. Publishing as Pearson Education, 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 or retrieval system, without prior written permission from Pearson Education, Inc. All rights reserved. Printed in the United States of America. This book is printed on acid-free paper. 10 9 8 7 6 5 4 3 2 1



REGULATION



CMMC's November deadline forces new calculations across the Space Industrial Base

The Cybersecurity Maturity Model Certification (CMMC) program is entering a new phase of enforcement. Beginning Nov. 10, new Department of Defense contracts that include CMMC requirements may require a Level 2 third-party assessment to be on file in the Supplier Performance Risk System. **#CMMC #SpaceIndustrialBase**



Source: [KratosSpace](#)

Sanctions are America's invisible shield. Congress must ensure they work

Sanctions are the critical system we depend on to make the world a safer through. They work through cutting off trade and other links to countries that are hostile to our interests. They are a critical tool to protect our interests and to ensure that our allies and partners are not harmed by the actions of hostile states. Congress must ensure that our sanctions are effective and that they are not undermined by loopholes or other actions.



Source: [CyberInflight](#)

The space age needs new rules

From a first perspective, cybersecurity also needs to change to protect satellites and the networks that connect them. Space is a critical part of our infrastructure and the commercial space industry is growing rapidly. We need to ensure that our cybersecurity laws and policies are up to date and that they are not undermined by loopholes or other actions. We need to ensure that our cybersecurity laws and policies are up to date and that they are not undermined by loopholes or other actions.

Source: [CyberInflight](#)

THREAT INTELLIGENCE



Ukraine hits Moscow's space communications node for second time

Ukraine struck a space communications center near Moscow for the second time on Tuesday, June 30, according to President Volodymyr Zelensky. Zelensky, in a Telegram report, described the target as a special satellite communications facility used for reconnaissance and coordination of Russia's forces in Ukraine. He added that the facility is located more than 500 kilometers (311 miles) from Ukraine's state border. **#Russia #Ukraine**



Source: [Kyiv Post](#)

Attack of Iranian hacker syndicates Iran's government into economic espionage and IP theft

Iran's cyberattacks are becoming more sophisticated and more frequent. The Iranian government is using cyberattacks to steal intellectual property and to disrupt the economy. The Iranian government is using cyberattacks to steal intellectual property and to disrupt the economy. The Iranian government is using cyberattacks to steal intellectual property and to disrupt the economy.



Source: [CyberInflight](#)

Ukrainian forces strike the leading Russian research institute in the Far East Region

The Russian Far East region is a strategic area for Russia. It is a region that is rich in natural resources and it is a region that is important for Russia's economy. The Russian Far East region is a strategic area for Russia. It is a region that is rich in natural resources and it is a region that is important for Russia's economy.



Source: [CyberInflight](#)

Red Hat Security Advisory: CVE-2024-36918 Apache OpenSSH

Red Hat Security Advisory: CVE-2024-36918 Apache OpenSSH. This advisory describes a vulnerability in the Apache OpenSSH software. The vulnerability allows an attacker to execute arbitrary code on the target system. The vulnerability is a result of a buffer overflow in the sshd daemon.



Source: [Red Hat](#)

Why is Russia struggling to join the Club of the World?

Russia is a large country with a large population. It is a country that has a long history and it is a country that has a rich culture. Russia is a country that has a long history and it is a country that has a rich culture. Russia is a country that has a long history and it is a country that has a rich culture.



Source: [CyberInflight](#)

THREAT INTELLIGENCE



Hackers threaten to leak data from NATO contractor Indra, as company investigates

The Gentlemen ransomware gang has listed one of Europe's defense powerhouses – the Spanish multinational company and NATO contractor, the Indra Group. So far, it is unknown what kind of data is involved in the alleged data breach. The gang released a post on June 30th on its leak site on the dark web, setting the deadline for the company to start communication. According to the post, Indra Group has 9 days before the data is publicly released. Indra has confirmed a ransomware attack that affected one of its subsidiaries but has "guaranteed the security and continuity of its services."



#NATO #Indra

Sources: [Cybernews](#), [Democrata](#)

TECHNOLOGY



Xiphera selected for ESA ARTES project to advance secure high-speed satellite communications

Xiphera has been selected for a new project under the European Space Agency's (ESA) ARTES program. The project will focus on developing a high-speed security IP core for optical satellite communications, further strengthening Xiphera's position as a provider of advanced hardware-based cybersecurity solutions for the space sector. #Xiphera #ESAARTES



Sources: [Design&Reuse](#), [TheDefensePost](#)

TRAINING & EDUCATION

Report 2026: a survey and national on satellite-based radio frequency (RF) geolocation and satellite fingerprinting

The European Agency of corrected defense is carrying out a survey and national on satellite-based radio frequency (RF) geolocation and satellite fingerprinting. The survey aims to assess the current state of the art in these technologies and identify the challenges and opportunities for their use in defense. The survey will focus on the use of these technologies for the identification and tracking of satellites, the detection of unauthorized satellites, and the detection of spoofing and jamming attacks. The survey will also assess the need for new technologies and the need for new standards. The survey will be carried out in two phases: a first phase to assess the current state of the art and a second phase to identify the challenges and opportunities for the use of these technologies in defense.



Sources: [ESA](#)

Call for Proposals - ESA/ARTES project to advance secure high-speed satellite communications

The European Space Agency (ESA) is calling for proposals for a new project under the ARTES program. The project will focus on developing a high-speed security IP core for optical satellite communications, further strengthening Xiphera's position as a provider of advanced hardware-based cybersecurity solutions for the space sector. The project will be carried out in two phases: a first phase to assess the current state of the art and a second phase to identify the challenges and opportunities for the use of these technologies in defense.



Sources: [ESA](#)

Satellite fingerprinting from 4 to 8 GHz for the requirements of satellite-based radio frequency (RF) geolocation and satellite fingerprinting. The project aims to develop a high-speed security IP core for optical satellite communications, further strengthening Xiphera's position as a provider of advanced hardware-based cybersecurity solutions for the space sector. The project will be carried out in two phases: a first phase to assess the current state of the art and a second phase to identify the challenges and opportunities for the use of these technologies in defense.



Sources: [ESA](#)

TRAINING & EDUCATION



Greek Space Tech forum 2026

The Greek Space Tech Forum 2026 will gather public administration executives and the growing Greek business ecosystem of the space market, aiming to analyze the opportunities and challenges for the further development of the Greek presence. At the same time, it serves as a platform to strengthen collaborations and networking within the Greek space ecosystem, connecting it with critical sectors of the Greek economy as well as abroad—both within the EU and in the wider region of the Southeastern Mediterranean and the Middle East. The Greek Space Tech Forum 2026 – GSTF 2026 will take place on Tuesday, July 7 and Wednesday, July 8, 2026. **#Greece #GSTF2026**

Source: [EthosEvents](#)



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