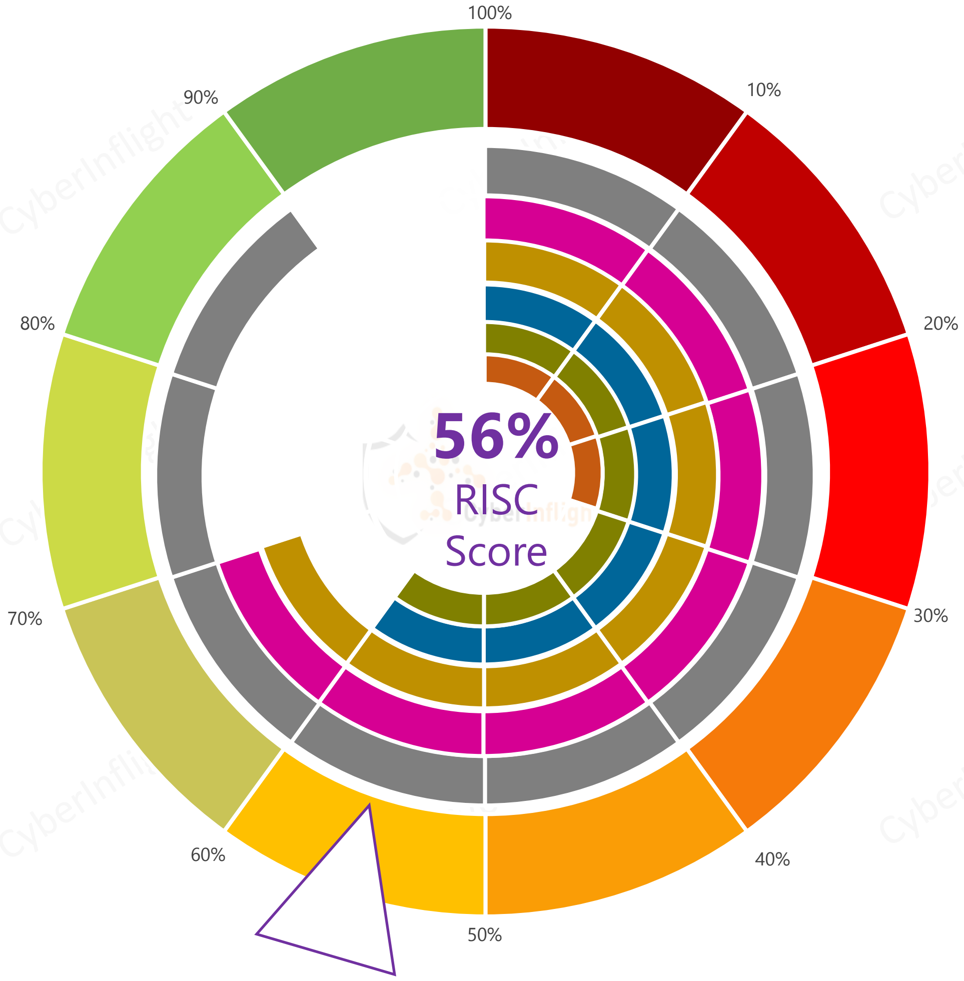
SPACE CYBERSECURITY WEEKLY WATCH

Week 41
October 3 – 9, 2023

Timeframe: Weekly
# of articles identified: 40
Est. time to read: 1 h 30 min

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

■ **GEOPOLITIC**
■ **TECHNOLOGY**
■ **MARKET & COMPETITION**
■ **THREAT INTELLIGENCE**
■ **TRAINING & EDUCATION**
■ **REGULATION**
★ **IMPORTANT NEWS**



Overview & RISC Score

This week's RISC score is 65% for several reasons, the first one being the launch by EUSPA and DG DEFIS of a Call for Expression of Interest for the creation of an EU Space ISAC. This Call for Interest must be completed by November 3, 2023, for those interested in becoming founding members, but it will be possible to apply to become a member of the EU Space ISAC until October 31, 2025.
Also on the regulatory front, the DoD, GSA and NASA are currently examining how to implement new revisions to the Federal Acquisition Regulation (FAR) to standardize cybersecurity requirements for government contractors.
Meanwhile, Booz Allen won a contract with the USSF to support Space Systems Command's Program Executive Office for Space Sensing.
On the Market Intel front this week, several contracts with US authorities were won, and an ESA Call for Proposal is underway for the 4S mission.
On the Threat Intel front, there were several attacks this week, more than we've reported in recent weeks. One of these was an attack on Infrasat which was asked for $60,000 not to disclose sensitive data.
On the technology front, the US DoT is looking for industry insight on how to best complement and support its PNT functions with new technology that does not depend on traditional GPS tech.
Lots of Training & Education news this week, including the BE-CYBER Conference on October 26 and the launch of a two-day workshop on Cybersecurity Principles for Satellite and Space Systems by Tonex.

GEOPOLITIC

Reinforcing European space autonomy with the EU Space Information Sharing Centre (ISAC)

Launch by EUSPA and the DG DEFIS, a Call for Expression of Interest for the new #EUSpace ISAC (Information Sharing Analysis Centre). The ISAC will serve as the primary communication channel for the #EUSpace sector regarding security-related information and sharing of best practices. It will be a membership-driven platform looking to engage industry, public sector and academia. **#EUSPA #SpaceISAC #CallforInterest**

Link: https://www.euspa.europa.eu/newsroom/news/reinforcing-european-space-autonomy-eu-space-information-sharing-centre-isac

Taiwan ramps up backup satellite network plans in island defence strategy

Taiwan is developing a backup satellite network to secure its communications with the outside world in the event of a cross-strait conflict. **#Taiwan #Satellite**

Link: https://www.scmp.com/news/china/military/article/[illegible]/taiwan-ramps-backup-satellite-network-plans-island-defence-strategy

ISRO chairman calls for strong cybersecurity knowledge base

Indian Space Research Organisation (ISRO) Chairman S. Somanath has called for a strong cybersecurity understanding and knowledge base to ensure the security of the nation. **#ISRO #Cybersecurity**

Link: https://www.thehindu.com/news/cities/Kochi/isro-chairman-calls-for-strong-cybersecurity-knowledge-base/article[illegible].ece

TECHNOLOGY

DoT Looking For Industry Input on GPS Tech Alternatives

The U.S. Department of Transportation (DOT) is looking for industry insight on how to best complement and support its Positioning, Navigation, and Timing (PNT) functions with new technology that does not depend on traditional Global Positioning System (GPS) tech. **#DoT #RFI**

Link: https://www.meritalk.com/articles/dot-looking-for-industry-input-on-gps-tech-alternatives/

Trasferimento dati fra satelliti: via al super cloud Leonardo-Cubbit *(Trad.: Data transfer between satellites: off to the Leonardo-Cubbit super cloud)*

Leonardo will be the first company in the aerospace, defense and security industry to use the geo-distributed cloud technology developed by Cubbit, a kind of "cloud" that is super-protected from cyber attacks and natural disasters, with even the exploration of some next generation designs, such as data transfer between satellites. **#Cloud #Cybersecurity**

Link: https://www.spaceconomy360.it/difesa-cybersecurity/trasferimento-dati-fra-satelliti-via-al-super-cloud-leonardo-cubbit/

The University of Alabama in Huntsville demonstrates cybersecurity software aboard a Lockheed Martin technology demonstrator CubeSat

The University of Alabama in Huntsville today announced that it developed a cybersecurity software for the U.S. Army Space and Missile Defense Command. The software began performance testing on one of Lockheed Martin's In-space Upgrade Satellite System (LM LINUSS™) technology demonstrator CubeSats. The software, Small Satellite Defender, is an intrusion detection system designed for small satellites. **#UniversityofAlabama #LockheedMartin**

Link: https://www.uah.edu/[illegible]/news/[illegible]-the-university-of-alabama-in-huntsville-demonstrates-cybersecurity-software-aboard-a-lockheed-martin-technology-demonstrator-cubesat

Russian Cyberwarfare at Space & S-550 Capabilities

S-550 are primarily designed to be comprehensive defense improving aerospace security. failure to undermine the cybersecurity within S-550 changes the game of the war, and dominance of space and technology, dynamics of the conflict can be changed with sophisticated defense and electronic sabotage cyber attacks, so cyber security of S-550 air defense missile systems is prominent. **#Russia #CyberWarfare**

Link: https://www.linkedin.com/pulse/cyberwarfare-space-s-550-capabilities-[illegible]

ISRO focused on developing onboard cyber technology for spacecraft

The Indian Space Research Organisation (ISRO) is taking proactive steps to address the growing threat of cyber attacks by developing onboard cyber technology. ISRO chairman S Somanath unveiled this strategic initiative during his keynote address. **#ISRO #CyberTechnology**

Link: https://www.newindianexpress.com/cities/kochi/2023/oct/08/isro-focused-on-developing-onboard-cyber-technology-for-spacecraft-[illegible].html

MARKET & COMPETITION

★ **Booz Allen nabs $630M integration contract for Space Force missile warning, weather programs**

The contract, will support Space Systems Command's Program Executive Office for Space Sensing, which is responsible for the service's missile warning, weather monitoring and "persistent tactical surveillance" programs, according to a Space Force fact sheet. Disciplines include but are not limited to: Cybersecurity, Architecture/Design, Integration Planning & Execution, Test & Evaluation, Technical Baseline Management, Risk Management, Digital Engineering & Modeling Simulation & Analysis. **#BoozAllen #USSF**

Link: https://breakingdefense.com/2023/10/booz-allen-nabs-630m-integration-contract-for-space-force-missile-warning-weather-programs/

THREAT INTELLIGENCE

Addressing Canada's Exposure to Space-Cyber Threats

[illegible] **#Canada #SpaceCyberThreats**

Link: [illegible]

DGCA sets up panel to check GPS spoofing in Indian airspace

[illegible] **#India #Spoofing**

Link: [illegible]

Moscow Jamming Causing As Much Anxiety as Protection?

[illegible] **#Russia #Jamming**

Link: [illegible]

Attack of BAE Systems by NoName

[illegible] **#BAESystems #NoName**

Link: [illegible]

Russian Luch (Olymp) 2 Satellite Approaching Multiple GEO Spacecraft

[illegible] **#Satellite #LuchOlymp**

Link: [illegible]

★ Hackers threaten Infrasat with demand of 60 thousand USD to not disclose sensitive data

Infrasat, a telecommunications company, was the victim of a computer attack last week, as determined by an internal source to the newspaper Valor Económico. **#Infrasat #Ransomware**

Link: https://www.menosfios.com/en/hackers-ameacam-infrasat-com-exigencia-de-60-mil-usd-para-nao-divulgar-dados-sensiveis/

Major Cyber Incident KA-SAT 9A

[illegible] **#Cyberattack #Report**

Link: [illegible]

Starlink Account Hacking Sparks Calls for Multi-Factor Authentication

[illegible] **#Starlink #Hacking**

Link: [illegible]

ISRO fights over 100 cyber attacks every day, reveals chairman Somanath

[illegible] **#ISRO #Cyberattacks**

Link: [illegible]

Attack of Rafael Advanced Defense Systems by Ganosec Team

[illegible] **#Israel #Cyberattack**

Link: [illegible]

TRAINING & EDUCATION

Protecting the Space Economy: Cyber Defenses and National Security

[illegible] **#Podcast #SpaceCybersecurity**

Link: [illegible]

Building more cyber-resilient satellites begins with a strong network

[illegible] **#Satellite #Cybersecurity**

Link: [illegible]

★ Cybersecurity Principles for Satellite and Space Systems | Training Workshop

Cybersecurity Principles for Satellite and Space Systems, Training Workshop is a 2-day interactive workshop designed to provide a unique learning experience on space and satellite vulnerabilities that are commonly exploited. Participants will discover techniques and strategies for integrating cybersecurity measures into space and SATCOM systems, networks, products and critical missions from the start. **#Workshop #SpaceCybersecurity**

Link: https://www.tonex.com/training-courses/cybersecurity-principles-for-satellite-and-space-systems-training-workshop/

Global defence and space program kicks off

[illegible] **#Australia #Course**

Link: [illegible]

SES workshop about the "Secure Communications via Satellite: Regulation and Technology"

[illegible] **#Workshop #Satellite**

Link: [illegible]

SPACEHACK 2023: Cybersecurity Edition

[illegible] **#SpaceHack #Competition**

Link: [illegible]

Space grand challenge: sandbox series October 16-21, 2023

[illegible] **#CalPoly #Competition**

Link: [illegible]

NDSS 2023 - SpaceSec Highlights

[illegible] **#NDSSSymposium #SpaceSec**

Link: [illegible]

Top ISRO, NTRO officials to share knowledge on cybersecurity at Cocon in Kochi

[illegible] **#ISRO #Conference**

Link: [illegible]

Space remains vulnerable to cyber attack

[illegible] **#Research #SpaceCybersecurity**

Link: [illegible]

Satellite Open Source Intelligence with ChatGPT
A quick video about using ChatGPT to accelerate your Satellite Open Source Intelligence gathering.
#EthicallyHackingspace #ChatGPT
Link: [illegible]

A Decade of Cybersecurity Challenges and Solutions for Satellite Systems
This article delves into the dynamic landscape of cybersecurity attacks on satellites over the last ten years, shedding light on the escalating risks faced by these indispensable space assets. This exploration not only highlights the evolving threat landscape but also offers insights into the vulnerabilities and countermeasures that define the contemporary satellite cybersecurity landscape. **#Satellite #Cybersecurity**
Link: [illegible]

BE-CYBER Experience Sharing Day
Conference on the 26th of October, 2023, in Brussels about Security in Space **#Conference #BE-CYBER**
Link: https://be-cyber.be/

REGULATION

"Government must lead" on PNT - UK Preparedness Commission Report
For the first time, the UK's 2023 National Risk Register (NRR) includes a section on the risks from a loss of positioning and timing services. The previous NRR only highlighted the risk to positioning and timing services from extreme space weather. This wider recognition is a welcome and important step in government leadership and national preparedness. A government announcement is anticipated with further details. **#UK #PNT**
Link: [illegible]

Agencies Looking to Standardize Cyber Requirements for Federal Contractors
The Department of Defense (DoD), the General Services Administration (GSA), and NASA are looking to implement new revisions to the Federal Acquisition Regulation (FAR) to standardize cybersecurity requirements for government contractors. The proposed rule, published in the Federal Register today, would develop standardized contract language for unclassified Federal Information Systems (FIS) and help to mitigate any potential risks associated with having no streamlined requirements. **#US #CyberRequirements**
Link: https://www.meritalk.com/articles/agencies-looking-to-standardize-cyber-requirements-for-federal-contractors/

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