SPACE CYBERSECURITY WEEKLY WATCH

Week 40

## September 26 – October 2, 2023

Timeframe : Weekly

# of articles identified : 42

Est. time to read : 1 h 35 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**
- **REGULATION**
- **THREAT INTELLIGENCE**
- **TRAINING & EDUCATION**
- **MARKET & COMPETITION**
- **TECHNOLOGY**
- ⭐ **IMPORTANT NEWS**

CYBERINFLIGHT'S NEWS :
⭐ 🎉 Introduction of CyberInflight's RISC 🎉 ⭐
Resilience Index for Space Cybersecurity

- GEOPOLITIC: 5
- REGULATION: 8
- THREAT INTEL.: 2
- TRAINING & EDUCATION: 7
- MARKET & COMPETITION: 8
- TECHNOLOGY: 6

60% RISC Index
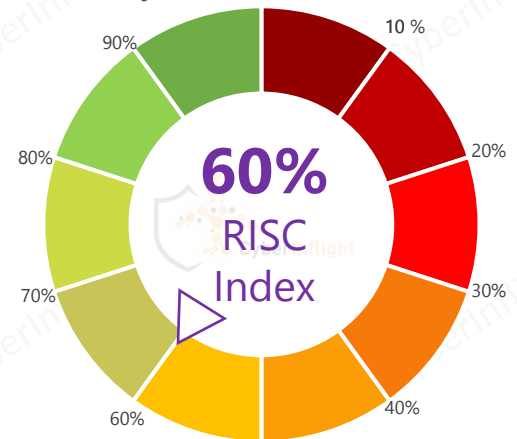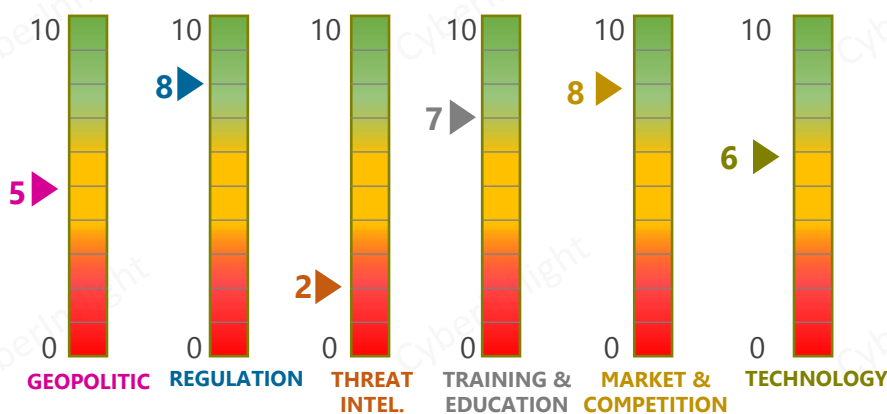
To celebrate the cyber-month, CyberInflight has decided to launch a new feature for its weekly watch: **the Resilience Index for Space Cybersecurity (RISC)!** This cyber resilience index allows us to assess the state of each category identified by CyberInflight. A score is given out of 10 for each section, which is assessed on the information presented in each section. This week, there was more important regulatory news than usual, allowing us to score well. The same reasoning was applied to Market and Training. There was also more jamming and attack news, explaining the threat intel section's low score. This week we have a 60% RISC Index, which is a relatively good score, but leaves room for improvement!

Overview

This week saw the release of 2 important announcements concerning space cybersecurity regulations. Firstly, the NIST National Cybersecurity Center of Excellence published the final version, NIST IR 8441, of the Cybersecurity Framework Profile for Hybrid Satellite Networks. Also this week, the European Commission launched a Targeted Stakeholder Consultation for an EU Space Law, which runs until November 2, 2023, and envisages common EU rules addressing the safety, resilience and sustainability of space activities and operations.

Earlier this week, the USSF and its partners decided to meet next month to discuss a strategy for supply chain resilience. In terms of threat intelligence, the Russian ransomware group Killnet has claimed responsibility for an attack on several US groups, including Lockheed Martin. CyberInflight also reported on a number of jamming-related news, and several attacks that took place. ESA is organizing a hacking contest to take control of a small rover. On the Market front, the USSF awarded several contracts this week, including the main one with John Hopkins University, to evaluate the software and cybersecurity of ground systems being developed for a new classified satellite network. Finally, on the technology front, L3Harris presented its Protected Tactical Waveform, providing warfighters with long-range, higher-bandwidth communication in the presence of jamming across all domains.

GEOPOLITIC

Space Critical Infrastructure Breaking the Binary Debate and a Call for Space Council Action
The question for space is not whether space itself is vital, but what functions in space are "so vital...that their incapacitation or destruction would have a debilitating effect on" the ability to operate and survive in space. **#US #CriticalInfrastructure**
Link: https://spacenews.com/space-critical-infrastructure-breaking-the-binary-debate-and-a-call-for-space-council-action/

The critical role of space technology in improving systems of governance
In his address to the ISRO scientists, Prime Minister Narendra Modi said that space technology was not only for sending satellites to orbit the earth and accomplishing interplanetary travels; it was also for improving the systems of governance in the country. **#ISRO #India**
Link: https://government.economictimes.indiatimes.com/news/digital-india/the-critical-role-of-space-technology-in-improving-systems-of-governance/103958106?redirect...1

Space Force, partners to craft global supply chain strategy
U.S. Space Force officials will meet next month with industry leaders and key international partners to discuss a strategy for supply chain resiliency. **#USSF #SupplyChain**
Link: https://www.defensenews.com/battlefield-tech/space/2023/09/25/space-force-partners-to-craft-global-supply-chain-strategy/

At London arms fair, global war fears are good for business
Those wanting satellite communications were also now requesting to access multiple different satellite systems at different levels in Earth orbit, giving them greater resistance to jamming or other deliberate action. **#Satellite #Jamming**
Link: https://www.reuters.com/world/uk/london-arms-fair-global-war-fears-good-business-2023-09-15/

REGULATION

NIST NCCoE Publishes Final NIST IR 8441, Cybersecurity Framework Profile for Hybrid Satellite Networks
The NIST National Cybersecurity Center of Excellence (NCCoE) has published Final NIST IR 8441, Cybersecurity Framework Profile for Hybrid Satellite Networks (HSN). **#NIST #Cybersecurity**
Link: https://www.nccoe.nist.gov/news-insights/nist-nccoe-publishes-final-nist-ir-8441-cybersecurity-framework-profile-hybrid

Pentagon Discloses Plan For Defending Space Systems
Earlier this month, the Pentagon finally responded to congressional urging by delivering to Capitol Hill a report entitled "Space Policy Review and Strategy on Protection of Satellites." In broad brush strokes, the 16-page document pulls together the various strands of space-defense thinking to provide a menu of options for assuring the survivability of vital space systems. **#US #SpacePolicy**
Link: https://www.forbes.com/sites/lorenthompson/2023/09/26/pentagon-discloses-plan-for-defending-space-systems/?sh=7fc1a2dfd603

Germany adopts new space strategy
The German government on Wednesday adopted a new space strategy that focuses on promoting private sector initiatives in space. **#Germany #SpaceStrategy**
Link: https://www.aa.com.tr/en/europe/germany-adopts-new-space-strategy/3002411

Launch of a Targeted Stakeholder Consultation for an EU Space Law
The Letter of Intent includes an initiative for an EU Space Law (EUSL). The legislative proposal could be adopted by the Commission in the first trimester of 2024. It envisages common EU rules addressing the safety, resilience and sustainability of space activities and operations. It intends to avoid and remove fragmentation and barriers across the single market caused by the heterogeneity or lack of national space legislations, while ensuring the competitiveness of the European space sector in an international trade context. **#EU #SpaceLaw**
Link: https://defence-industry-space.ec.europa.eu/targeted-consultation-eu-space-law_en

THREAT INTELLIGENCE

⭐ **Cyber Attack on Lockheed Martin: Killnet Targets US Defense Giant Amid Geopolitical Tensions**
Lockheed Martin, an international aerospace, arms, defense, and information security corporation is the latest victim of the Killnet ransomware group. The Russian hacktivist group named not one but two U.S. organizations in a Telegram message. They named the Army Transport Corps alongside the claim of cyber attack on Lockheed Martin. **#Russia #Killnet**
Link: https://thecyberexpress.com/cyber-attack-on-lockheed-martin-target-us/

Russian's war system 'likely' behind Ben-Gurion disruptions
The Israel Airports Authority has stated that "unknown factors" are disrupting the GPS systems of planes landing at Ben-Gurion Airport in recent months. The cause of the disruption is highly likely to be Russian electronic warfare systems located in Syria. **#Israel #Russia**
Link: https://www.israeltoday.co.il/read/russian-e-war-system-likely-behind-ben-gurion-disruptions/

Electronic GPS 'spoofing' behind civilian jet navigation failures over Iraq
False electronic signals imitating satellite data from Global Position System satellites recently caused complete navigation failures for 12 aircraft flights near Iran, according to a private aircraft security group. **#Spoofing #GPS**
Link: https://www.washingtontimes.com/news/2023/sep/26/electronic-gps-spoofing-behind-civilian-jet-naviga/

Ransomware attack by 8Base
8Base #ransomware group has announced Absolute Engineering on the victim list. **#Turkey #Ransomware**
Link: https://twitter.com/DailyDarkWeb/status/1706367648309699968

DDoS attack on the NASA website
The post states that the NASA Blogs website has been targeted by a DDoS attack carried out by a threat actor known as DDoS 16). The post provides proof of the downtime of the website and includes a link to a report showing the details of the attack. The post was published on a Telegram network by the threat actor. The victims of this attack are identified as the NASA Blogs website, with the attack affecting the availability of the site. The post categorizes this incident as a DDoS attack and mentions that the targeted industry is Aviation & Aerospace, with the organization being NASA Blogs. The attack is said to have taken place in the USA. **#NASA #DDoS**
Link: https://t.me/menatic_ddos_s/

'All systems need to be hardened': Officials, industry sound the alarm on quantum threat to encryption
New "quantum resistant" encryption standards won't be finalized until next year, but officials and experts say agencies and industry should start hunting vulnerabilities hidden in their software and hardware, including embedded chips critical to US weapons. **#US #Quantum**
Link: https://breakingdefense.com/2023/official-systems-need-to-be-hardened-officials-industry-sound-the-alarm-on-quantum-threat-to-encryption/

North Korean gov't hackers targeted aerospace company in Spain
Hackers connected to a notorious group within the North Korean government launched an attack against an aerospace company in Spain, according to researchers at security company ESET. **#Cyberattack #NorthKorea**
Link: https://therecord.media/north-korean-govt-hackers-spain

'GPS jamming quite routine on long-haul flights, spoofing isn't instantly apparent'
The US Federal Aviation Administration (FAA) issued a memo titled "Iraq/Azerbaijan – GPS jamming and spoofing poses safety risk". Potential spoofing activities reported by various civil air operators in Iraq and Azerbaijan pose flight risk to civil aviation operations in the Baghdad and Baku flight information regions (FIR), the US civil aviation regulator warned. **#Jamming #GPS**
Link: https://timesofindia.indiatimes.com/india/gps-jamming-quite-routine-on-long-haul-flights-spoofing-isnt-instantly-apparent/articleshow/104027744.cms?from=mdr

Russian GPS 'jamming' causing collision risk in Black Sea, Romania says
Romania has claimed Russia is "actively and constantly" jamming ships' GPS communications in its territorial waters. This is causing a risk of collisions in the Black Sea, according to army chief of staff General Daniel Petrescu. **#Jamming #Russia**
Link: https://www.tradewindsnews.com/casualties/russian-gps-jamming-causing-collision-risk-in-black-sea-romania-says/2-1-1528452

Satellite Risks: Navigating A Transforming Risk Environment
Today our reliance on satellites is such that without them every business sector would be brought to a standstill and the world's economy would likely come to a halt. It begs the question: how prepared are satellite operators, institutions and governments to mitigate the risks of malicious actions against satellites? **#Space #Cybersecurity**
Link: https://www.brwinsurance.co/cards/eu/satellite-risks-navigating-transforming-risk-environment/

TRAINING & EDUCATION

⭐ **PWN THE ROVER - Hacking Contest**
The contest allows to take control of a small robotic asset and navigate through obstacles within the station. The goal is to repair the malfunctioning systems, solve challenges, and protect your rover from cyber attacks. **#ESA #Contest**
Link: https://www.pwn-the-rover.space/

Want to hack a satellite?
[blurred text] **#Contest #Satellite**
Link: [blurred link]

Global industry gathered in Norway to test robustness
[blurred text] **#Jammertest #Norway**
Link: [blurred link]

Reflecting on a productive day with the SPD Bundestagsfraktion's visit to #ESOC!
[blurred text] **#ESA**
Link: [blurred link]

Webinar - Mastering GNSS Timing Resilience: The secrets to secure GNSS timing and synchronization
[blurred text] **#Webinar #Septentrio**
Link: [blurred link]

Star wars: "Israel is interested in space weapons. Every one of our satellites is a machine of war"
[blurred text] **#Israel #SpaceWarfare**
Link: [blurred link]

Workshop on the Security of Space and Satellite Systems
[blurred text] **#Conference #US**
Link: [blurred link]

The Final Frontier: Fortifying Cyber Resilience for the Commercial Space Industry
White Paper about the developing commercial space industry **#Whitepaper #SpaceIndustry**
Link: [blurred link]

Space Economy Summit
[blurred text] **#Conference #Economy**
Link: [blurred link]

Securing the Final Frontier: Cybersecurity in Space Technology
[blurred text] **#Space #Cybersecurity**
Link: [blurred link]

4

MARKET & COMPETITION

⭐ **Space Force selects university partner to evaluate classified ground systems software**
The Space Force awarded a $10 million contract to the Johns Hopkins University Applied Physics Lab to evaluate the software and cybersecurity of ground systems being developed for a new classified satellite network.
#USSF #JohnsHopkins
Link: https://spacenews.com/space-force-selects-university-partner-to-evaluate-classified-ground-systems-software/

⭐ **Opportunity: Cybersecurity as Enabler for Secure Satellite Communications and Resilient Applications**

This new Space Systems for Safety and Security (4S) Call for Proposals aims to foster the development of innovative satellite communications technologies, products, systems and downstream applications which address these challenges. **#ESA #CallforProposal**

Link: https://connectivity.esa.int/opportunity-cybersecurity-enabler-secure-satellite-communications-and-resilient-applications

TECHNOLOGY

BlueHalo Backs Space Force's Satellite Control Network Upgrade With Phase Array Antenna Tech Demo

BlueHalo demonstrated its phased-array antenna system in late August and is set to make an initial delivery of the first unit by the spring of 2025 to help the U.S. Space Force upgrade its Satellite Control Network. BADGER, which is short for Broad Area Deployable Ground terminal enabling Resilient communication, is a deployable ground terminal that builds on BlueHalo's Multi-band Software Defined Antenna, a phased- array technology that streamlines mission operations through agile beamforming tiles. **#BlueHalo #GroundSegment**

Link: https://news.phantio.com/2023/09/06/bluehalo-backs-space-forces-satellite-control-network-upgrade-with-phase-array-antenna-tech-demo/

@CDOT_India & @CSIR_NPL sign agreement for development of NavIC

@CDOT_India & @CSIR_NPL sign agreement for development of NavIC based IST traceable Primary Reference Time Clock(PRTC) for time synchronization of Telecom networks. 'One Nation One Time' ensuring cyber security & providing an alternate to GPS. **#India #PNT**

Link: https://twitter.com/CDOT_India/status/1704708027449737107

A Day Without Space: GPS Is Ground Zero For The New Space Race

Alternatives to GPS, categorically called Global Navigation Satellite Systems (GNSS), are growing rapidly because the old GPS system we rely on offers neither the precision nor security needed in an increasingly autonomous, rule-based, and precisely timed world. **#GPS #GNSS**

Link: https://www.forbes.com/sites/charlesbeames/2023/09/20/a-day-without-space-gps-is-ground-zero-for-the-new-space-race/

⭐ **L3Harris breaks barriers in secure SATCOM with HAAM-R Modem at Northern Edge**

L3Harris presented its Protected Tactical Waveform (PTW)-enabled HAAM-R modem. It provide warfighters long-range, higher-bandwidth communication in the presence of jamming across all domains. **#L3Harris #AntiJamming**

Link: https://www.airforce-technology.com/news/l3harris-breaks-barriers-in-secure-satcom-with-haam-r-modem-at-northern-edge/