

SPACE CYBERSECURITY WEEKLY WATCH

Week 31

July 25 – 31, 2023

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



Overview

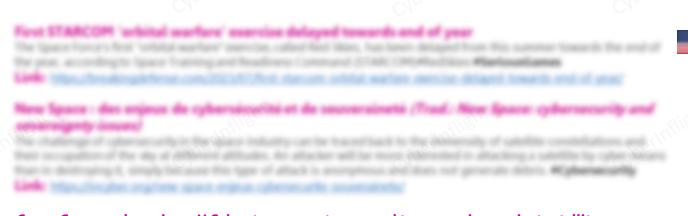
Timeframe: Weekly

of articles identified: 27

Est. time to read: 45 minutes

One of this week's highlights is the publication of the introductory report "Cybersecurity for Commercial Satellite Operations", NIST IR 8270. On the geopolitical front, the US government and the US Space Force are seeking cooperation with the rest of their European allies, including a proposed partnership around Anti-Satellite Attacks. A US-Italy summit also took place this week. Regarding satellite attacks, the US is challenged by China's rapid advances in space technology. New details of the Dozor-Teleport attack were published this week, and a new Russian attack on Brazilian satellites occurred. The attacker claims to have hacked into the cyber systems of INPE, the Brazilian research institute. Furthermore, this week Thales announced its participation in the European Galileo project with Quantum-Ready Cybersecurity measures. Quantum sensors is foreseen as a tool that will eventually replace GPS systems, according to research by the Naval Research Laboratory. For the European Commission, finding alternatives to GNSS is also a project for which tests are underway. Finally, on the market side, the EU, via EDF, has provided funding for 18 projects run by Leonardo. The EU has also awarded a contract to Spire as part of the Euralio project (within ARTES). CyberOps has won a major \$2.5 million contract with the Australian Department of Defense. In parallel, the Australian's Defense Research Funding Applications are currently open.

GEOPOLITIC





Space Command nominee: U.S. has to prepare to respond to aggression against satellites

The U.S. military is being challenged to counter China's rapid advances in space technology, Lt. Gen. Stephen Whiting told the Senate Armed Services Committee. **#US #SPACECOM**

Link: https://spacenews.com/space-command-nominee-u-s-has-to-prepare-to-respond-to-aggression-against-satellites



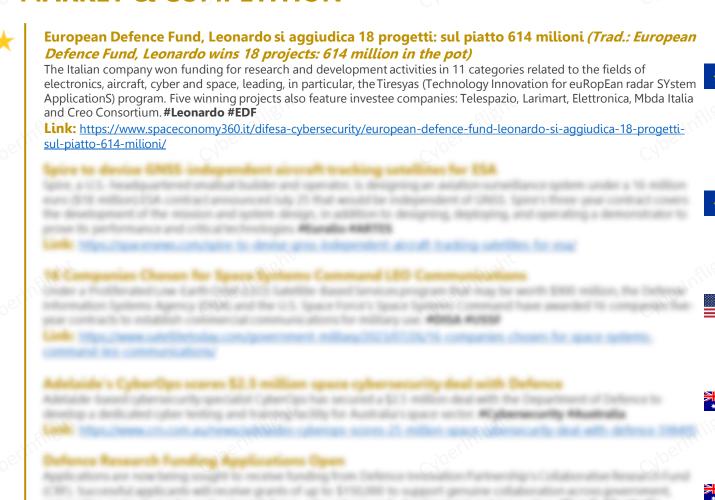




#USSF #Cooperation

Link: https://i-hls.com/archives/120122

MARKET & COMPETITION





Week 31 | July 25-31, 2023 Page 3/4

THREAT INTELLIGENCE



Briefing 11: Russian Satellite Service Provider Dozor-Teleport Targeted by Cyberattack

Briefing about the Dozor-Teleport cyberattack. This attack represents the second major cyber incident affecting a satellite communications company; following the major disruption of a US satellite company in February 2022, when Viasat's KA-sat was disrupted at the onset of the Russian invasion of Ukraine. **#Cyberattack**

Link: https://www.kratosdefense.com/constellations/space-isac





Hacker russo diz ter invadido satélites do INPE (Trad.: Russian hacker says he hacked INPE satellites)

A cybercriminal known as Samurai (from the Russian group SecDet) claims to have hacked into the cyber systems of INPE (National Institute for Space Research) last week. In addition to gaining access to confidential data, the attacker allegedly managed to access information from Brazilian satellites. **#Hacker #Russia #Brazil**

Link: https://www.tecmundo.com.br/seguranca/266902-hacker-russo-diz-ter-invadido-satelites-inpe.htm



TRAINING & EDUCATION



Space Cafe Radio – EUSPA Ep.01 – with Piotr Sitek

In this Space Café Radio – SpaceWatch.Global's Dr. Emma Gatti spoke with Piotr Sitek, governmental and new components, security governance officer in the security authority department of EUSPA. #EUSPA #Podcast Link: https://spacewatch.global/2023/07/space-cafe-radio-euspa-ep-01-with-piotr-sitek/







REGULATION



Introduction to Cybersecurity for Commercial Satellite Operations



NIST Interagency Report (IR) 8270, Introduction to Cybersecurity for Commercial Satellite Operations, presents a specific method for applying the Cybersecurity Framework (CSF) to commercial space business and describes an abstract set of cybersecurity outcomes, requirements, and suggested controls. **#NIST #Cybersecurity**

Link: https://csrc.nist.gov/pubs/ir/8270/final



TECHNOLOGY



Thales announces Quantum-Ready Cybersecurity measures for Galileo



Thales's solution is set to be based on a scalable, flexible architecture, derived from its Cybels security supervision products, and equipped with big data capabilities. The objective is to protect the system against increasingly sophisticated threats, including the potential vulnerabilities introduced by quantum computing. **#Quantum #Galileo**

Link:

https://www.spacedaily.com/reports/Thales announces Quantum Ready Cybersecurity measures for Galileo 999.html







Backing Up GNSSThe Joint Research Centre of the European Commission tested seven advanced alternative sources of positioning navigation and timing (A-PNT) platforms through a performance assessment campaign, proving there are viable alternatives to GNSS available in the commercial market today. **#GNSS #EuropeanCommission**



Link: https://insidegnss.com/backing-up-gnss/

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