



SPACE CYBERSECURITY WEEKLY WATCH

Week 34

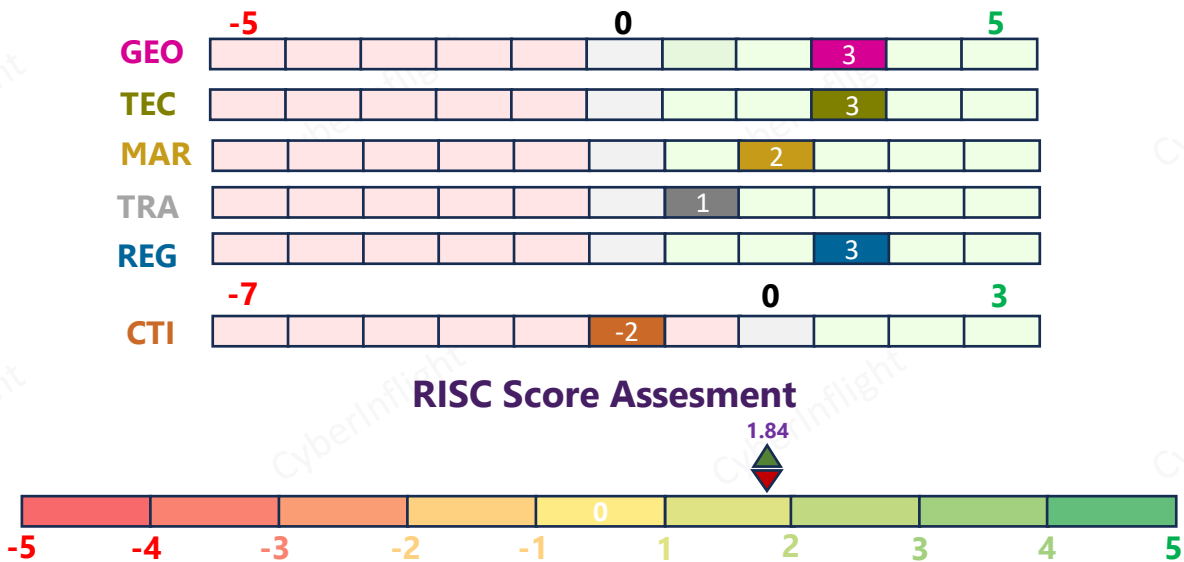
August 20 – 26, 2024

Timeframe : Weekly
of articles identified : 41
Est. time to read : 75 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 INTELLIGENCE**
- **THREAT INTELLIGENCE**
- **REGULATION**
- **TRAINING & EDUCATION**
- ★ **IMPORTANT NEWS**

Overview & Resilience Index for Space Cybersecurity (RISC)



This week's RISC score is 1.84, a slight increase from last week, mainly due to geopolitical factor as nation shows more interest in buying satellite technology.

On the geopolitical front, Japan and India have held their latest "2+2" ministerial dialogue, focusing on cybersecurity cooperation and joint efforts. This partnership is seen as a strategic move to counter regional threats and ensure a free and open Indo-Pacific. On the technological side, Chinese researchers have successfully demonstrated space-to-ground communications using a lightweight quantum satellite, advancing Quantum Key Distribution (QKD) technology. This innovation is a significant leap in secure communications, potentially revolutionizing global cybersecurity. On the market front, the UK is investing £20 million in a state-of-the-art anti-jamming test facility to enhance the resilience of GPS and other critical infrastructure against electronic warfare threats. This facility aims to support the development of advanced anti-spoofing and jamming technologies essential for national security and defense operations. On the Threat Intel side, Defence and Security multinational Thales released its 2024 Critical Infrastructure report, and it makes for some grim reading. One of the key figures is that ransomware attacks on critical infrastructure (CI) entities have increased year on year, with 24% reporting an attack in the last 12 months, compared to 21% for the previous reporting period. On the regulatory front, HR 8965, the Spacecraft Cybersecurity Act which would require NASA acquisition processes to include guidelines and controls for managing cybersecurity risks. Lastly, an informative BALPA's webinar is being organized which covers the important and topical issue of GPS jamming and spoofing.

GEOPOLITICS



Japan, India to accelerate space, cyber security cooperation; set to confirm revision of joint declaration at 2+2 meeting

Japan and India have held their latest "2+2" ministerial dialogue, focusing on cybersecurity cooperation and joint efforts in regional geopolitics. This partnership is seen as a strategic move to counter regional threats and ensure a free and open Indo-Pacific. #Japan #India

Link: <https://japannews.yomiuri.co.jp/politics/defense-security/20240817-205556/>



South Korea, US look off annual drills

South Korea and the United States have looked off annual joint military exercises, setting to boost their joint readiness to fend off North Korea's weapons and cyber threats. The drills will feature "Cyber Shield" across all domains, including the North's cyber threats for cyber espionage, operations, and other threats. South Korea's defense ministry said...

Link: [https://japannews.yomiuri.co.jp/politics/defense-security/20240817-205556/](#)



US 'shorts longer' to battle newly arrived, vehicles used Russian GPS assets

In March, a group comprising US defense officials and other experts in Russia had to GPS assets used as a key tool for Russian military forces operating in Ukraine against its foreign military equipment. These assets often will use to offer GPS users in the area, including commercial aircraft. The US government is responding to the rising threat by building a more advanced GPS system to address the challenge. The "shorts longer" will make it more difficult for Russia to track and intercept US military equipment and operations.

Link: [https://japannews.yomiuri.co.jp/politics/defense-security/20240817-205556/](#)



Iran seeks purchase of advanced spy satellites from China

Iran is seeking to purchase advanced spy satellites from China to expand its intelligence capabilities and to counter US and other regional powers. The deal is expected to be completed by August 20. According to the report, multiple allegations have been made that Iran has been negotiating with the Chinese government to purchase advanced spy satellites. The deal would allow Iran to track and intercept US military equipment and operations.

Link: [https://japannews.yomiuri.co.jp/politics/defense-security/20240817-205556/](#)



Nigerian Federal Government moves to enhance protection of critical national telecom infrastructures

The Nigerian Federal Government has announced plans to strengthen and protect its critical national telecommunications infrastructure. The move is part of a broader strategy to enhance national security and resilience against cyber threats. The government will focus on securing key telecom assets, including fiber optic cables, data centers, and satellite links. A government-owned telecom operator will be established to manage and protect these critical assets.

Link: [https://japannews.yomiuri.co.jp/politics/defense-security/20240817-205556/](#)



Mexico to acquire advanced spy satellites from Israel

Mexico has announced the acquisition of advanced spy satellites from Israel to enhance its intelligence capabilities and to counter US and other regional powers. The deal is expected to be completed by August 20. According to the report, Mexico is seeking to purchase advanced spy satellites to track and intercept US military equipment and operations.

Link: [https://japannews.yomiuri.co.jp/politics/defense-security/20240817-205556/](#)



US Air Force follows study cybersecurity at US

The US Air Force has announced a study on cybersecurity at the US Air Force. The study is part of a broader strategy to enhance national security and resilience against cyber threats. The Air Force will focus on securing key assets, including aircraft, data centers, and satellite links. A government-owned telecom operator will be established to manage and protect these critical assets.

Link: [https://japannews.yomiuri.co.jp/politics/defense-security/20240817-205556/](#)





MARKET & COMPETITION

Space Force to scale up AI monitoring capabilities

Space Force is set to scale up its AI monitoring capabilities to help identify and track threats in the increasingly crowded orbital environment. The service will be using a new set of AI tools to help identify and track threats in the increasingly crowded orbital environment. The service will be using a new set of AI tools to help identify and track threats in the increasingly crowded orbital environment.

Link: [https://www.spaceforce.mil/News/Space-Force-to-scale-up-AI-monitoring-capabilities](#)



US Air Force and Space Force address GPS jamming and spoofing

The US Air Force and Space Force are working together to address GPS jamming and spoofing threats. The service will be using a new set of AI tools to help identify and track threats in the increasingly crowded orbital environment. The service will be using a new set of AI tools to help identify and track threats in the increasingly crowded orbital environment.

Link: [https://www.airforce.mil/News/US-Air-Force-and-Space-Force-address-GPS-jamming-and-spoofing](#)



Using cybersecurity demands college industrial control systems government strategic areas

Security cybersecurity threats and attacks demand the attention of both sectors and operators of critical infrastructure. Security cybersecurity threats and attacks demand the attention of both sectors and operators of critical infrastructure. Security cybersecurity threats and attacks demand the attention of both sectors and operators of critical infrastructure.

Link: [https://www.cisa.gov/news-events/press-releases/details?id=A240814-01](#)

Trajectory Watch 2 SpaceWatch continues to monitor challenge

SpaceWatch has updated Trajectory Watch 2 (SpaceWatch 2) to continue to monitor the complex orbital environment. SpaceWatch has updated Trajectory Watch 2 (SpaceWatch 2) to continue to monitor the complex orbital environment. SpaceWatch has updated Trajectory Watch 2 (SpaceWatch 2) to continue to monitor the complex orbital environment.

Link: [https://www.spaceforce.mil/News/Trajectory-Watch-2-SpaceWatch-continues-to-monitor-challenge](#)



US Space Force's Strategic Plan aligns National Security Strategy in monitoring

The US Department of Defense (DOD) is set to release its Strategic Plan for the next five years. The plan will focus on monitoring and tracking threats in the increasingly crowded orbital environment. The plan will focus on monitoring and tracking threats in the increasingly crowded orbital environment.

Link: [https://www.spaceforce.mil/News/US-Space-Force-s-Strategic-Plan-aligns-National-Security-Strategy-in-monitoring](#)



★ UK to build \$20M anti-jamming test facility

The UK is investing £20 million in a state-of-the-art anti-jamming test facility to enhance the resilience of GPS and other critical infrastructure against electronic warfare threats. This facility aims to support the development of advanced anti-spoofing and jamming technologies essential for national security and defense operations. **#UK #AntiJamming**

Link: <https://rmtfnd.org/2024/08/23/uk-to-build-huge-new-20m-anti-jamming-test-facility-uk-defense-journal/>



TECHNOLOGY

Space Force to test AI AI against its satellite operations

Space Force is set to test its AI capabilities against its satellite operations. The service will be using a new set of AI tools to help identify and track threats in the increasingly crowded orbital environment. The service will be using a new set of AI tools to help identify and track threats in the increasingly crowded orbital environment.

Link: [https://www.spaceforce.mil/News/Space-Force-to-test-AI-against-its-satellite-operations](#)



★ China advances QKD with Lightweight quantum satellite

Chinese researchers have successfully demonstrated space-to-ground communications using a lightweight quantum satellite, advancing Quantum Key Distribution (QKD) technology. This innovation is a significant leap in secure communications, potentially revolutionizing global cybersecurity. **#QuantumSecurity #QKDInnovation**

Link: <https://syntony-gnss.com/news/tech/the-crucial-role-of-gnss-testing-against-spoofing-attacks/>





TECHNOLOGY

Protecting military space technology from bad actors

The new technology comes with a price tag that could be a fraction of what it costs to develop it. It doesn't get more cutting-edge than military space technology, so that means the security standards and checks need to be top-notch and ongoing. It's a priority. It's not just the US going about that, it's all the major military powers at the moment. The US has a lot of space assets, and the military is looking at the future of space. The US is going to be a leader in space. The military is looking at the future of space. The US is going to be a leader in space. The military is looking at the future of space.



[Read more about protecting military space technology from bad actors](#)

The crucial role of AI in testing against spoofing attacks

An AI testing system is being developed to detect spoofing attacks, ensuring the integrity of space systems. The system is being developed to detect spoofing attacks, ensuring the integrity of space systems. The system is being developed to detect spoofing attacks, ensuring the integrity of space systems. The system is being developed to detect spoofing attacks, ensuring the integrity of space systems.

[Read more about the crucial role of AI in testing against spoofing attacks](#)

France to participate in September 2024, the world's largest GNSS resilience testing event

France is participating in a global event to test GNSS resilience. The event is being held in September 2024. The event is being held in September 2024. The event is being held in September 2024. The event is being held in September 2024.



[Read more about France participating in the world's largest GNSS resilience testing event](#)

GNSS spoofing with neural nets

Researchers are using neural networks to detect GNSS spoofing. The system is being developed to detect spoofing attacks, ensuring the integrity of space systems. The system is being developed to detect spoofing attacks, ensuring the integrity of space systems.

[Read more about GNSS spoofing with neural nets](#)

Global updates by navigation from satellite GNSS location into space

The world's largest GNSS resilience testing event is being held in September 2024. The event is being held in September 2024. The event is being held in September 2024. The event is being held in September 2024.



[Read more about global updates by navigation from satellite GNSS location into space](#)

The military applications of artificial intelligence in space

Artificial intelligence is being used in space systems. The system is being developed to detect spoofing attacks, ensuring the integrity of space systems. The system is being developed to detect spoofing attacks, ensuring the integrity of space systems.

[Read more about the military applications of artificial intelligence in space](#)



Space information security to discuss cutting-edge cybersecurity solutions at 2024 US, Space & Cyber Conference

The 2024 US, Space & Cyber Conference is being held in September 2024. The event is being held in September 2024. The event is being held in September 2024. The event is being held in September 2024.



[Read more about space information security to discuss cutting-edge cybersecurity solutions at 2024 US, Space & Cyber Conference](#)

Ground Control to Major Threat: Making the Space Link Extension Protocol

The Space Link Extension Protocol is being developed to detect spoofing attacks, ensuring the integrity of space systems. The system is being developed to detect spoofing attacks, ensuring the integrity of space systems.



[Read more about Ground Control to Major Threat: Making the Space Link Extension Protocol](#)

2024 Africa Aerospace & Defense Conference

The 2024 Africa Aerospace & Defense Conference is being held in September 2024. The event is being held in September 2024. The event is being held in September 2024. The event is being held in September 2024.



[Read more about 2024 Africa Aerospace & Defense Conference](#)



REGULATION



Review - HR 8965 introduced – NASA cybersecurity

Last month, Frost introduced HR 8965, the Spacecraft Cybersecurity Act. The bill would require NASA acquisition processes to include guidelines and controls for managing cybersecurity risks. Frost is a member of the House Science, Space, and Technology Committee to which this bill was assigned for consideration. This means that there may be sufficient influence to see the bill considered in Committee. Nothing in this bill would engender any organized opposition but it is suspected that there would be bipartisan support for the bill to be approved in Committee.

#NASA #Act

Link: <https://chemical-facility-security-news.blogspot.com/2024/08/review-hr-8065-introduced-nasa.html>



TRAINING & EDUCATION



BALPA's GPS Spoofing and Jamming Webinar

BALPA webinar covering the important and topical issue of GPS Jamming and Spoofing. Combined with representatives from Boeing and Airbus, BALPA's Stuart A. Clarke will be moderating the webinar before introducing presentations from Ian Goodwin and Dr. Kirk Vining, followed by a Q&A session. #Webinar #Spoofing

Link: <https://www.youtube.com/watch?v=2kkIA-gRZVw>





THREAT INTELLIGENCE



Report allegedly broadcast by unknown threat actor

In a recent cyber incident, a threat actor group claimed responsibility for breaching the high-profile website, including the official website of SpaceX. The group's claims are backed by the fact that the site of the group's official communications, CyberInflight, was also breached.

[Source: https://www.cyberinflight.com/news/2024/08/19/unknown-threat-actor-broadcasts-report-allegedly-breached-by-unknown-threat-actor](#)



Thales 2024 critical infrastructure report reveals a rise in ransomware and a lack of readiness

Defence and security multinational Thales released its 2024 Critical Infrastructure report last week, and it makes for some grim reading. One of the key figures is that ransomware attacks on critical infrastructure (CI) entities have increased year on year, with 24 per cent reporting an attack in the last 12 months, compared to 21 per cent for the previous reporting period. #Thales #CriticalInfra

Link: <https://www.cyberdaily.au/security/10980-thales-2024-critical-infrastructure-report-reveals-a-rise-in-ransomware-and-a-lack-of-readiness>



Report: 50% of organisations vulnerable to the threat – and 70% lack a plan – The Telegraph

A new report from the National Cyber Security Centre (NCSC) reveals that 50% of organisations are vulnerable to the threat of ransomware attacks. The report also highlights that 70% of organisations do not have a plan in place to respond to such attacks. The report is based on a survey of 1,000 organisations across the UK.

Source: [https://www.telegraph.co.uk/news/technology/2024/08/19/50-of-organisations-vulnerable-to-ransomware-attacks-ncsc-report/](#)



Ransomware attacks on critical infrastructure in the UK – and 70% lack a plan – The Telegraph

A new report from the National Cyber Security Centre (NCSC) reveals that 50% of organisations are vulnerable to the threat of ransomware attacks. The report also highlights that 70% of organisations do not have a plan in place to respond to such attacks. The report is based on a survey of 1,000 organisations across the UK.

Source: [https://www.telegraph.co.uk/news/technology/2024/08/19/50-of-organisations-vulnerable-to-ransomware-attacks-ncsc-report/](#)

50% of organisations vulnerable to ransomware attacks – The Telegraph

A new report from the National Cyber Security Centre (NCSC) reveals that 50% of organisations are vulnerable to the threat of ransomware attacks. The report also highlights that 70% of organisations do not have a plan in place to respond to such attacks. The report is based on a survey of 1,000 organisations across the UK.

Source: [https://www.telegraph.co.uk/news/technology/2024/08/19/50-of-organisations-vulnerable-to-ransomware-attacks-ncsc-report/](#)



50% of organisations vulnerable to ransomware attacks – The Telegraph

A new report from the National Cyber Security Centre (NCSC) reveals that 50% of organisations are vulnerable to the threat of ransomware attacks. The report also highlights that 70% of organisations do not have a plan in place to respond to such attacks. The report is based on a survey of 1,000 organisations across the UK.

Source: [https://www.telegraph.co.uk/news/technology/2024/08/19/50-of-organisations-vulnerable-to-ransomware-attacks-ncsc-report/](#)



50% of organisations vulnerable to ransomware attacks – The Telegraph

A new report from the National Cyber Security Centre (NCSC) reveals that 50% of organisations are vulnerable to the threat of ransomware attacks. The report also highlights that 70% of organisations do not have a plan in place to respond to such attacks. The report is based on a survey of 1,000 organisations across the UK.

Source: [https://www.telegraph.co.uk/news/technology/2024/08/19/50-of-organisations-vulnerable-to-ransomware-attacks-ncsc-report/](#)

