



SPACE CYBERSECURITY WEEKLY WATCH

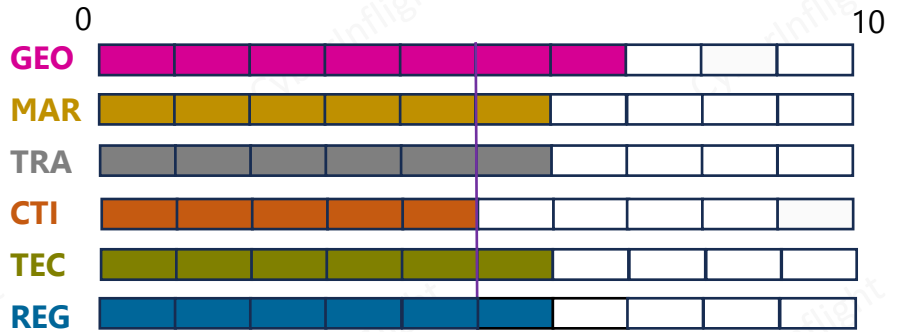
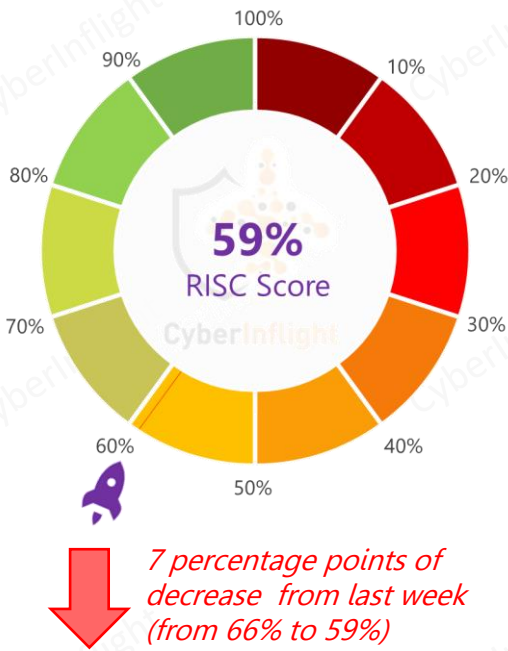
Week 29
July 16 – 22, 2024

Timeframe : Weekly
of articles identified : 38
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.

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

Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score Evolution



After struggling to recover since the drop from W18 and finally rising on W28, the RISC score (the tool used to assess cybersecurity resilience in space) is back down slightly.

This week's RISC score is 59%. In geopolitical news, the US Space Force revealed that the US is installing a new ground-based jammer designed to prevent Chinese or Russian satellites from sharing information, about US forces, during an attack. The first 11 of 24 of these devices will be deployed in undisclosed locations before the end of the year. On the technology front, after two Finnair planes flying to Estonia recently had to return to Helsinki due to GPS spoofing, Finnair is now beginning to implement real quantum navigation systems to prevent such incidents from occurring in the future. On the market front, the US Department of Transportation has awarded contracts to nine suppliers specializing in complementary PNT technologies. These contracts are designed to enhance the safety and reliability of GPS and improve the resilience of PNT by instrumenting, testing, and evaluating complementary PNT technologies at various field test sites. In other news, the Aspen Security Forum was held July 16-19 in Colorado. There was a panel on "Infinity and Beyond: Space and National Security," which focused on opportunities and threats in space. On the regulatory front, the UK will introduce a Cyber Security and Resilience Bill to strengthen the nation's cyber defenses and secure critical infrastructure. This initiative aims to protect businesses that rely on cyberspace. Lastly, 2024 Olympics are approaching, and given their heavy reliance on satellites, this event is an attractive target for malicious actors with different motivations. Strong and broad mitigation measures are needed to address these threats.



GEOPOLITIC

★ US prepares jamming devices targeting Russia, China satellites

The Space Force disclosed that the US is about to deploy a new ground-based jammer designed to blunt Chinese or Russian satellites from transmitting information about US forces during a conflict. These devices aren't meant to protect US satellites from Chinese or Russian jamming but "to responsibly counter adversary satellite communications capabilities that enable attacks. #China #Russia



Link: <https://www.bnnbloomberg.ca/business/international/2024/07/19/us-prepares-jamming-devices-targeting-russia-china-satellites/>

Russia is ready to counter US plans for 'satellite jamming' in space

Russia's space development plan includes a focus on creating a space force and plans to develop satellite technologies. Russia's Ministry of Defense has announced that it will develop a ground-based satellite jamming system to counter US plans to deploy a new ground-based jammer designed to blunt Chinese or Russian satellites from transmitting information about US forces during a conflict. The system is expected to be deployed in the near future.



Link: <https://www.bnnbloomberg.ca/business/international/2024/07/19/russia-is-ready-to-counter-us-plans-for-satellite-jamming-in-space/>

The US Space Force planning America's military dominance in the final frontier

The US Space Force is planning to develop a space force that will be able to control and defend space. The force will be able to control and defend space, and will be able to control and defend space. The force will be able to control and defend space, and will be able to control and defend space.



Link: <https://www.bnnbloomberg.ca/business/international/2024/07/19/the-us-space-force-planning-americas-military-dominance-in-the-final-frontier/>

Russia and China 'both developing weapons to attack US assets in space'

Russia and China are both developing weapons to attack US assets in space. The weapons are designed to attack US satellites and other assets in space. The weapons are designed to attack US satellites and other assets in space. The weapons are designed to attack US satellites and other assets in space.



Link: <https://www.bnnbloomberg.ca/business/international/2024/07/19/russia-and-china-both-developing-weapons-to-attack-us-assets-in-space/>

The latest information on China's cyberwarfare capabilities and the Strategic Support Force

The latest information on China's cyberwarfare capabilities and the Strategic Support Force. The Strategic Support Force is a new military unit that is responsible for cyberwarfare and other operations. The Strategic Support Force is a new military unit that is responsible for cyberwarfare and other operations. The Strategic Support Force is a new military unit that is responsible for cyberwarfare and other operations.



Link: <https://www.bnnbloomberg.ca/business/international/2024/07/19/the-latest-information-on-chinas-cyberwarfare-capabilities-and-the-strategic-support-force/>

Using satellites over outer space - a new diplomatic hot zone

Using satellites over outer space - a new diplomatic hot zone. The use of satellites in space is becoming a major issue in international relations. The use of satellites in space is becoming a major issue in international relations. The use of satellites in space is becoming a major issue in international relations.



Link: <https://www.bnnbloomberg.ca/business/international/2024/07/19/using-satellites-over-outer-space-a-new-diplomatic-hot-zone/>



TECHNOLOGY



Opinion: Reliable GPS is coming to an end – but new quantum technologies could show the path forward

Using a quantum-assured navigation system, a vehicle may be able to position itself precisely even when GPS is not available for very long periods. To prevent a repeat of the Finnair event, real quantum navigation systems are now starting to undergo field testing. **#QuantumNavigation #Finland**

Link: <https://www.thestar.com.my/tech/tech-news/2024/07/19/opinion-reliable-gps-is-coming-to-an-end---but-new-quantum-technologies-could-show-the-path-forward>



MARKET & COMPETITION



US DOT awards contract for complementary PNT technology

The US Department of Transportation (DOT) has awarded contracts to nine vendors specializing in complementary positioning, navigation, and timing (PNT) technologies. These contracts aim to enhance the security and reliability of the GPS, totaling more than \$7.2 million. They will fund the instrumentation, testing, and evaluation of Complementary PNT technologies at various field test ranges. This initiative, executed through the Volpe Center in response to the DOT Complementary PNT Action Plan, aims to facilitate the adoption of these technologies to improve PNT resiliency.

#DOT #PNT

Link: <https://www.militaryaerospace.com/communications/article/55126099/us-dot-awards-contracts-for-complementary-pnt-technology>





TRAINING & EDUCATION

How will space electronics warfare shape the space domain?
Space-based electronic warfare (EW) is not just changing the game – it's rewriting the rules. The advent of space-based EW capabilities creates new opportunities, but also significant challenges. How can we leverage the extended reach and unique perspectives of space-based EW to enhance our national security? The stakes are high, and the opportunities are immense. Join us for an expert panel discussion on this critical topic.



Link: [https://www.defense.gov/News/News-Stories/Article/Article/3843526/military-experts-highlight-space-opportunities-threats-at-aspcon-conference](#)

How will space EW shape the space domain?
The Department of Defense and Space Force's Strategic Plan for Space Operations (SPO) has outlined a comprehensive approach to space operations, including the integration of electronic warfare (EW) capabilities. This report explores the challenges and opportunities of space-based EW, and provides a roadmap for future development.



Space-based electronic warfare (EW) is not just changing the game – it's rewriting the rules. The advent of space-based EW capabilities creates new opportunities, but also significant challenges. How can we leverage the extended reach and unique perspectives of space-based EW to enhance our national security? The stakes are high, and the opportunities are immense. Join us for an expert panel discussion on this critical topic.



How will space EW shape the space domain?
The Department of Defense and Space Force's Strategic Plan for Space Operations (SPO) has outlined a comprehensive approach to space operations, including the integration of electronic warfare (EW) capabilities. This report explores the challenges and opportunities of space-based EW, and provides a roadmap for future development.



Link: [https://www.defense.gov/News/News-Stories/Article/Article/3843526/military-experts-highlight-space-opportunities-threats-at-aspcon-conference](#)

Space-based electronic warfare (EW) is not just changing the game – it's rewriting the rules. The advent of space-based EW capabilities creates new opportunities, but also significant challenges. How can we leverage the extended reach and unique perspectives of space-based EW to enhance our national security? The stakes are high, and the opportunities are immense. Join us for an expert panel discussion on this critical topic.



How will space EW shape the space domain?
The Department of Defense and Space Force's Strategic Plan for Space Operations (SPO) has outlined a comprehensive approach to space operations, including the integration of electronic warfare (EW) capabilities. This report explores the challenges and opportunities of space-based EW, and provides a roadmap for future development.



Link: [https://www.defense.gov/News/News-Stories/Article/Article/3843526/military-experts-highlight-space-opportunities-threats-at-aspcon-conference](#)

★ Military experts highlight space opportunities, threats at Aspen Conference

The 15th Annual Aspen Security Forum was held July 16-19. There was a panel on "Infinity and Beyond: Space and National Security," which focused on opportunities and threats in space. **#Conference #Space**



Link: <https://www.defense.gov/News/News-Stories/Article/Article/3843526/military-experts-highlight-space-opportunities-threats-at-aspcon-conference/>



REGULATION



UK set to debut Cyber Security and Resilience Bill to boost national cyber defenses, secure critical infrastructure

The U.K. government is poised to introduce the Cyber Security and Resilience Bill into Parliament in the coming months. The move is expected to 'strengthen the UK's cyber defenses, ensure that critical infrastructure and the digital services that companies rely on are secure. #UK #CriticalInfrastructure

Link: <https://industrialcyber.co/regulation-standards-and-compliance/uk-set-to-debut-cyber-security-and-resilience-bill-to-boost-national-cyber-defenses-secure-critical-infrastructure/>



THREAT INTELLIGENCE

Chinese hackers long game the shadow threat to critical US infrastructure

Chinese hackers have recently increased their cyber attacks against the power, energy, and critical infrastructure sectors, aiming to disrupt critical infrastructure like power grids and transportation. The ongoing cyber campaign is part of China's broader strategy to undermine global stability and gain a strategic edge. Experts warn that the growing reliance on digital services and interconnected systems, the threat remains, as Chinese state-backed hackers continue to target critical infrastructure worldwide, preparing for potential espionage in case of a major conflict. #China #US

Link: [https://industrialcyber.co/regulation-standards-and-compliance/chinese-hackers-long-game-the-shadow-threat-to-critical-us-infrastructure](#)



America at risk from China, lack of US alternatives - National Security Space Association

The National Security Space Association (NSSA) warns that America is over-dependent on GPS, but no real alternatives exist in the United States and Russia. Both of these nations have satellite technology for space-based navigation and timing signals. Europe, Japan, and other satellite navigation systems are in early development and expected to catch the US at a price in 2030s-2040s.

Link: [https://industrialcyber.co/regulation-standards-and-compliance/america-at-risk-from-china-lack-of-us-alternatives-nsa](#)



Timing satellite attack, GPS jamming now engaged in and around Israel

The state of Israel and its ally, the United States, are engaged in a cyber war against Iran, which is targeting Israel's satellite navigation systems. The attack is a part of a broader campaign to disrupt Israel's military and civilian operations.

Link: [https://industrialcyber.co/regulation-standards-and-compliance/timing-satellite-attack-gps-jamming-now-engaged-in-and-around-israel](#)



Expanding GPS spoofing during flight can be a challenging situation for pilots

A credible security scenario is the expansion of GPS spoofing in flight and ground-based operations. This is a significant threat to the aviation industry, as it can lead to loss of navigation and timing signals.

Link: [https://industrialcyber.co/regulation-standards-and-compliance/expanding-gps-spoofing-during-flight-can-be-a-challenging-situation-for-pilots](#)

Aviation cybersecurity: China dangers and a new tracking solution

In an increasingly interconnected world, aviation cybersecurity is becoming a critical concern. China's growing influence in the global aviation market, particularly in the Asia-Pacific region, has raised concerns about the security of flight operations. The industry is looking for new tracking solutions to address these challenges and ensure the safety of passengers and cargo.

Link: [https://industrialcyber.co/regulation-standards-and-compliance/aviation-cybersecurity-china-dangers-and-a-new-tracking-solution](#)

Widely leaked the details of space technologies

A report states that a significant amount of information about space technologies, a space technology company based in Washington, D.C. The report states that the company's data, which has been leaked, could be used to identify vulnerabilities in the company's systems and infrastructure.

Link: [https://industrialcyber.co/regulation-standards-and-compliance/widely-leaked-the-details-of-space-technologies](#)



Alleged source with lack of Space Exploration Engineering

The alleged source with lack of Space Exploration Engineering is a significant concern for the industry. The source's lack of expertise in this field could lead to serious consequences for the space program.

Link: [https://industrialcyber.co/regulation-standards-and-compliance/alleged-source-with-lack-of-space-exploration-engineering](#)





THREAT INTELLIGENCE

The cybersecurity of space infrastructure: satellites and networks

In the last episode of space, which satellites and networks are the challenges of cybersecurity have become a major concern. As we explore the current, we explore the challenges of cybersecurity in the space domain and how this space domain has been affected by the attack. The article by Dr. John W. R. ...

Link: [https://www.modern-diplomacy.com/2024/07/19/cybersecurity-at-major-global-events-satellite-security-insights-for-the-2024-olympics/](#)

Israel's GPS spoofing: a major challenge, but also commercial plans

In this article, the state of Israel has been a major challenge for its operations regarding GPS spoofing. It also mentions that the attack was to spoof GPS for the state-owned GPS spoofing, which could interfere with the signal received by ...

Link: [https://www.modern-diplomacy.com/2024/07/19/cybersecurity-at-major-global-events-satellite-security-insights-for-the-2024-olympics/](#)

New protections deployed against attacks on navigation systems

A series of GPS spoofing and jamming has been reported against and systems around the world while being used by the Israeli coast and military forces. Using satellites about the safety of all these systems, intelligence agencies are ...

Link: [https://www.modern-diplomacy.com/2024/07/19/cybersecurity-at-major-global-events-satellite-security-insights-for-the-2024-olympics/](#)

Attacks on the compliance with GPS spoofing: a major challenge for GPS spoofing

Attacks on the compliance with GPS spoofing have been reported against GPS spoofing that is also the challenge of ...

Link: [https://www.modern-diplomacy.com/2024/07/19/cybersecurity-at-major-global-events-satellite-security-insights-for-the-2024-olympics/](#)



Cybersecurity at major global events: satellite security insights for the 2024 Olympics

Satellites play a strategic role in supporting various aspects of the Olympics, ranging from communication, navigation, and security surveillance, to broadcasting. However, this dependence also opens up opportunities for various types of cyber-attacks. An event as large as the Olympics will always be a prime target for various motives, such as sabotage, espionage, political disinformation, undermining the host's reputation, spreading fear and anxiety worldwide, and financial gain.

#2024Olympics #SpaceCybersecurity

Link: <https://modern-diplomacy.com/2024/07/19/cybersecurity-at-major-global-events-satellite-security-insights-for-the-2024-olympics/>

Global satellite-based communication systems of GPS spoofing: a major challenge for GPS spoofing

Attacks on the compliance with GPS spoofing have been reported against GPS spoofing that is also the challenge of ...

Link: [https://www.modern-diplomacy.com/2024/07/19/cybersecurity-at-major-global-events-satellite-security-insights-for-the-2024-olympics/](#)

How global satellite operations report on impact from Microsoft outage

Global satellite communications and other communications are a challenge for this area not impacted by the Microsoft outage ...

Link: [https://www.modern-diplomacy.com/2024/07/19/cybersecurity-at-major-global-events-satellite-security-insights-for-the-2024-olympics/](#)

Space sector steps of essential GPS spoofing in Israel

Attacks on the compliance with GPS spoofing have been reported against GPS spoofing that is also the challenge of ...

Link: [https://www.modern-diplomacy.com/2024/07/19/cybersecurity-at-major-global-events-satellite-security-insights-for-the-2024-olympics/](#)

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

