

# CYBER DEFENSE MONTHLY WATCH

October 2025

Number of articles identified: 80

- # **Geopolitics**: 16
- # **Technology**: 19
- # **Market**: 19
- # **Regulation**: 7
- # **Threat intelligence**: 15
- # **Training & Education**: 4

Tags and themes

- EW** Electronic Warfare
- UV** Unmanned Vehicles (UAV, USV)
- ISR** Intelligence, Surveillance & Reconnaissance
- AI** Artificial Intelligence
- QT** Quantum Technologies
- ★ IMPORTANT NEWS

Over the past weeks, the defense landscape has been marked by intensified strategic competition and rapid technological alignment across major powers, reflecting a decisive shift toward multi-domain integration and information dominance. **Russia and China are deepening their cooperation through the joint development of new anti-drone and electronic warfare systems** aimed at countering Western and Ukrainian capabilities. Meanwhile, the U.S. Army is elevating cyber and electronic warfare oversight to a strategic priority under its principal cyber advisor. Simultaneously, **China's recently established Aerospace Force** demonstrates Beijing's intent to transform space into an operational battlefield central to its modernization and hybrid warfare doctrine.

On the regulatory front, defense institutions are accelerating governance reforms. The **U.S. Army's ALARACT 099/2025 standardizes electromagnetic spectrum access** for unmanned operations, while the **U.S. Coast Guard leverages \$25 billion in new funding to modernize maritime cybersecurity** under Force Design 2028. Ukraine has streamlined procurement of drones and electronic warfare equipment, reducing frontline delays.

In the defense market, investment patterns point to a strong focus on intelligence, quantum security, and information resilience. **Leonardo's ESA-backed Quantum Security Validation Platform** reflects Europe's focus on post-quantum defense, while the U.S. Air Force's SIFTER program advances signal processing and cybersecurity in SIGINT. Meanwhile, **Spain is advancing the design phase of its next-generation naval intelligence ship** to strengthen maritime EW and intelligence capacity, reinforcing national industrial autonomy.

Technological advances integrate electronic, cyber, and space domains. Raytheon's successful milestone for its **Advanced Electronic Warfare (ADVEW) system signals progress toward replacing the F/A-18's** legacy protection suite, aligning with the U.S. Navy's modular modernization strategy. **Airbus's launch of the SpainSat NG-II satellite** finalizes Europe's most advanced secure communications program, strengthening transatlantic autonomy in military space infrastructure. At the same time, the Pentagon's pursuit of "RF-enabled cyber" capabilities marks a significant convergence of electronic warfare and hacking designed to deliver non-kinetic battlefield effects.

Recent threat intelligence highlights growing sophistication of cross-domain challenges. In the South China Sea, **Chinese sources claim that their forces successfully deceived a foreign reconnaissance aircraft using advanced spoofing technology**, underscoring the evolving counterintelligence capabilities. USSF leadership has expressed alarm over China's accelerated progress in space-based defense systems, framing it as a defining contest for orbital superiority. Meanwhile, **CISA has issued a critical advisory over active exploitation of vulnerabilities in Dassault Systèmes' DELMIA Apriso platform**, exposing the expanding attack surface of industrial control systems.

Finally, training and education are evolving to address multi-domain challenges. **India's Northern Command exercise Vidyut Vidhwans** simulated cyber, space, electromagnetic, and cognitive threats, engaging military, government, and private actors in a whole-of-nation approach. Complementing these efforts, a **French IRSEM study** emphasizes spectrum and orbital resources as strategic commodities amid growing low-Earth orbit competition, underscoring the importance of cross-domain expertise and technological literacy for modern defense readiness.

# GEOPOLITICS

## AIR



### Russia, China team up on new anti-drone systems

A confidential letter from the Russian company TSK-Vektor, addressed to Rostec CEO Sergey Chemezov, reveals Moscow's efforts to develop and mass-produce new electronic warfare (EW) systems in partnership with Chinese firms to counter Ukrainian drones and Western satellite communications. Hactivist collective Black Mirror has released another data dump containing internal correspondence related to the Russian state defense conglomerate Rostec, exposing communication from the email address vektor\_tsk@mail.ru, which appears to belong to personnel affiliated with Russian defense industrial enterprises. **#Cooperation #AntiDrone**

**Source:** [Defence Blog](#)     



### How China's Air Force is preparing to challenge U.S. dominance over the Pacific

In a hypothetical Sino-American war, such as over Taiwan or the South China Sea (SCS), China's new fifth-generation J-20A fighter would challenge American air dominance by exploiting real quantitative and qualitative advantages. At the same time any war is occurring on Earth, the Chinese will have launched sweeping counterspace attacks against sensitive U.S. and allied satellite constellations—all while disrupting American operations in the cyberspace domain and across the electromagnetic (EM) spectrum. As far as the air war component of any such fight between American and Chinese forces, though, all Chinese forces would be operating very close to Chinese shores. Meanwhile, Chinese warplanes and warships would be shielded from the full brunt of America's power projection by China's vast and comprehensive anti-access/area-denial (A2/AD) defensive network in the South China Sea. **#Pacific #Strategy**

**Source:** [The National Interest](#)     



### Commission and High Representative present new Defense Roadmap to strengthen European defense capabilities

On October 16, the Commission and the High Representative have proposed to EU Member States the 'Preserving Peace - Defence Readiness Roadmap 2030', a comprehensive plan to strengthen European defense capabilities. The Roadmap sets out clear objectives and milestones to achieve defense readiness by 2030, as outlined in the White Paper for European Defense. Among its key proposals are four flagship projects: the Eastern Flank Watch, the European Drone Defense Initiative, the European Air Shield, and the European Space Shield. **#EuropeanDefense #Roadmap**

**Source:** [European Commission](#), [European Commission](#)     



### Germany's €377bn defense blueprint expands NATO air, space, and long-range strike power

Politico disclosed that Berlin has mapped a €377bn multiyear procurement blueprint that stretches across land, air, sea, space and cyber, that will anchor the Bundeswehr's 2026 budget cycle and beyond. The plan lists roughly 320 new projects, underpinned by a political decision to ease Germany's debt brake for defense after the near exhaustion of the €100bn special fund, and requires parliamentary committee approval for each tranche above €25m. **#Germany #NATO**


**Sources:** [Army Recognition](#), [Politico](#)     



## LAND

### Army eyes larger all-source intelligence support to EW

Electronic warfare has come to dominate the modern battlespace, and the Army is going to need greater all-source intelligence — using information from humans, signals, satellites and more — according to an Army official. "We have to look at how all-source is supporting EW. We have to look at how HUMINT [human intelligence] is supporting EW through battle letter and through how their questions are flowing out to individuals that they're interviewing," Col. John Shemer, Army capability manager for intel sensors at the Intelligence Center of Excellence, said during a presentation at the annual AUSA conference. **#USArmy #Intelligence**

**Source:** [Breaking Defense](#)     



### Electronic warfare and information advantage added to Army principal cyber advisor portfolio

The Army secretary's top advisor on cyber issues has now also been tasked with providing advice on electronic warfare and information advantage, elevating the focus on those topics at the highest level of the Army. "From a civilian oversight perspective as it relates to cyber, EW, electronic warfare, and information advantage will now fall to our office," Brandon Pugh, the Army's principal cyber advisor, said in an interview. According to him, the move attempts to align civilian oversight with uniformed roles. Currently, the Department of the Army's Management Office for Strategic Operations within the Army's G-3/5/7 is tasked with overseeing cyber, EW and information advantage. **#USArmy #CEMA**

**Source:** [Breaking Defense](#)     



### Army National Guard soldiers are readying to defend cities from hackers

As U.S. cities struggle to protect themselves from hackers, the Army National Guard is launching a new effort in five cities to strengthen local defenses against digital attacks. "We depend on everything outside of our wires — power, water. And we know that if that's affected while we're going to the fight, our families are going to be at risk," Lt. Gen. Jeth Rey, deputy chief of staff G-6, told reporters during a media roundtable at the annual Association of the United States Army conference in Washington, DC. **#NationalGuard #Hacking**

**Source:** [Business Insider](#)     



# GEOPOLITICS

## SPACE

### ESA tests GNSS resilience during jamming test in the Arctic

In its pursuit of strengthening European resilience in navigation, the European Space Agency (ESA) took part in Jammertest 2025, which brought together 360 participants from 120 organizations across more than 20 countries, spanning academia, industry and governmental institutions. In a complex coordination exercise among seven Norwegian public authorities and facilitator Testnor, the organizers broadcast real satellite navigation interference for participants to observe how their equipment (on vehicles, drones, aircrafts, helicopters and vessels) responds. **#Jammertest2025 #Exercise**

Sources: [GPS World](#), [ESA](#)     



### Cyber resilience in the age of commercial space and AI kill webs

As the Pentagon increasingly relies on commercial space capabilities for sensing, transportation, and resilience, a new frontier is emerging, where commercial satellites not only inform the battlefield but also enable its most critical operations. This includes scenarios where commercial space assets help close kill webs, provide primary, contingency, alternative, and emergency (PACE) communications and sensing, and increasingly feed AI models in real-time. But while proliferated Low-Earth Orbit (LEO) may secure the orbits through resiliency, the cyber terrain above and below them is a glaring weak point waiting to be exploited. **#Resilience #SpaceWarfare**

Source: [Via Satellite](#)     



### How China's Aerospace Force is taking shape a year after its formation

China's newly established Aerospace Force, formed in April 2024, marks a strategic reorganization of the People's Liberation Army (PLA) by unifying satellites, radars, and counterspace weapons under one command. Emerging from the dissolution of the Strategic Support Force, the Aerospace Force now reports directly to the Central Military Commission, reflecting its central role in China's military modernization. This structural shift demonstrates Beijing's ambition to transform space from a supporting domain into an operational battlefield central to its hybrid and information warfare strategy. **#PLA #SpaceWarfare**

Source: [Swarajya](#)     



### Unpacking Ukraine's Future Cyber and Space Forces




Confronted with escalating cyber and space threats, Kyiv is now working to create centralized structures dedicated to defending Ukraine from future multi-domain attacks. On October 9, Ukraine's parliament approved a bill to establish a Cyber Force, which would unite its offensive and defensive military cyber capabilities under a single command. This legislation comes alongside Ukraine's parallel effort to create a Space Force by the end of 2025. **#Ukraine #SpaceWarfare**

Source: [CSIS](#)     



### €1.2bn for the ESA's ERS project to strengthen Europe's autonomy and resilience in space

The European Space Agency (ESA) has unveiled details of its €1.2bn European Resilience from Space (ERS) program, presented in Brussels. ERS aims to create an integrated network of Earth observation, navigation, and secure communications satellites to support defense, crisis management, and critical infrastructure resilience. The program includes a €250m Low Earth Orbit PNT constellation to reinforce Galileo against cyber and signal interference and a €200m secure communications segment evolving from IRIS<sup>2</sup>. **#ESA #ERS**

Sources: [Astrospace](#), [ESA](#)     



### Space Force eyes aggressor satellites to add realism to test and training

In a push to make testing and training more realistic, Chief of Space Operations Gen. Chance Saltzman said he wants to put live aggressor satellites in orbit to mimic adversary tactics. USSF has live ranges on the ground for electronic warfare testing and training, and it plans to establish more live training venues for cyber as part of its future National Space Test and Training Complex. **#USSF #AggressorSatellites**

Source: [Air & Space Forces Magazine](#)     



## CYBER

### U.S. Strategic Command nominee acknowledges shortfalls in electronic warfare operations, training

During his Senate confirmation hearing, Vice Adm. Richard Correll, nominee to lead the U.S. Strategic Command (USSTRATCOM), admitted that the Department of Defense remains behind in testing, exercising, and integrating electronic warfare (EW) operations. While Stratcom is primarily responsible for overseeing the Defense Department's nuclear capabilities and global strike missions, it is also charged with leading the military's joint electromagnetic spectrum operations. But Correll stressed to lawmakers that there is still much work to be done to integrate EW into the Defense Department's operational plans. **#USSTRATCOM #Readiness**

Source: [Defense Scoop](#)     



# GEOPOLITICS

## CYBER

### Defense experts welcome Nacsa's cybersecurity enhancements

Defense analysts have lauded the establishment of the Cybersecurity and Cryptology Development Centre under the National Cyber Security Agency (Nacsa), calling it an important step to strengthen Malaysia's digital defenses under Budget 2026. Senior economics lecturer at the National Defense University of Malaysia (UPNM), Nur Surayya Saudi, said the initiative shows that cybersecurity has become a pillar of national security and economic resilience. She said investment in digitalization, surveillance systems and drone integration will enhance situational awareness and strengthen Malaysia's cybersecurity ecosystem under Nacsa. **#NACSA #Budget2026**

Source: [Malaysia Today](#)     

### Accelerating the next generation of electromagnetic warfare

Warfare is being redefined. As the UK's 2025 Strategic Defence Review (SDR) outlines, rapid advances in technology and changing conflict dynamics are transforming both the threat and the way nations need to respond. A new Cyber and Electromagnetic (CyberEM) Command and a commitment of £1bn to develop a 'Digital Targeting Web' to link UK armed forces' weapon systems underlines this fundamental shift in defense strategy. **#SDR #Strategy**

Source: [Cambridge Wireless](#)     



# REGULATION

## AIR

### UN aviation assembly closes with rebuke of Russia over satellite navigation jamming

The U.N. aviation agency's assembly concluded with delegates agreeing to condemn Russia for disturbances to critical satellite navigation systems that they say violate international rules. Estonia and neighbour Finland have blamed Russia for jamming GPS navigation devices in the region's airspace, charges that Moscow has denied. ICAO's triennial assembly overwhelmingly backed a resolution condemning recurring global navigation interference originating from Russia and its "harmful impact on the safety and security of international civil aviation." **#ICAO #Resolution**

Source: [Reuters](#)     



### Army issues UAS spectrum access rules

The U.S. Army has released ALARACT 099/2025, a service-wide directive defining procedures for electromagnetic spectrum access to support unmanned aircraft system (UAS) operations. The policy aligns with Department of Defense and Army regulations governing radio frequency authorization and electromagnetic environmental effects. It requires Army units to coordinate and obtain proper spectrum-use authorization to prevent interference with other systems and ensure electromagnetic compatibility across operational, training, and testing environments. **#SpectrumManagement #Directive**

Source: [Executive Gov](#)     



## MARITIME



### CSIS: USCG poised for 'generational change' in maritime cybersecurity with new tools, \$25bn funding

A new analysis from the Center for Strategic and International Studies (CSIS) highlights a "generational change" in U.S. maritime cybersecurity as the U.S. Coast Guard (USCG) gains nearly \$25bn in funding through the One Big Beautiful Bill Act. The report outlines expanded USCG cyber authorities, new regulatory powers, and major investments under the Force Design 2028 plan to modernize legacy systems, implement zero-trust architecture, and establish a dedicated C5I (Command, Control, Communication, Computer, Cyber, and Intelligence) office. The CSIS warns that sustained investment and congressional approval of the USCG Authorization Act of 2025 will be critical to secure long-term maritime cyber resilience. **#USCG #Report**

Sources: [Industrial Cyber](#), [CSIS](#)     



## LAND



### Ukrainian government simplifies procedure for purchasing drones and electronic warfare equipment for the front

The Cabinet of Ministers of Ukraine has approved amendments to the regulatory framework that simplify the procedure for purchasing unmanned systems, electronic warfare (EW) equipment and their components for the needs of the front. This was reported by the Ministry of Defense of Ukraine. From now on, units of the Armed Forces of Ukraine will be able to directly purchase both ready-made systems and individual components for them — electric motors, batteries and other unified parts. This should eliminate bureaucratic barriers that previously slowed down the delivery of equipment to the front. **#EquipmentPurchase #Amendments**

Source: [Oboronka](#)     



# REGULATION

## SPACE

### With space infrastructure at risk, experts call for cybersecurity by design, tight governance, and supply chain accountability

Space infrastructures are increasingly exposed to cyberattacks, jamming, and software vulnerabilities. In an article published by the World Economic Forum, experts call for the integration of cybersecurity principles from the earliest stages of spacecraft and satellite system design (a “cybersecurity by design” approach), along with stronger global governance and supply chain accountability. They emphasize that as space becomes a critical yet contested domain, end-to-end protection and transparency across all components, from orbital assets to ground networks, are essential to ensure resilience, reliability, and trust in the space ecosystem. **#Resilience #Governance**

Sources: [Industrial Cyber](#), [World Economic Forum](#)     

## CYBER

### World Economic Forum paper tells firms to get ready for quantum-ready manufacturing

A new World Economic Forum (WEF) white paper produced with Accenture warns that quantum computing, sensing, and security are rapidly moving from research labs to industrial applications, reshaping how manufacturers design, operate, and secure global supply chains. Analysts describe a looming “quantum imperative,” urging firms to invest in quantum-safe cybersecurity, workforce training, and international standards to prevent future vulnerabilities and maintain competitiveness. With global supply chain disruptions up 38% in 2024, the WEF emphasizes that quantum readiness will soon determine industrial resilience and data protection against quantum-enabled cyber-threats.

**#Quantum #WhitePaper**

Sources: [The Quantum Insider](#), [World Economic Forum](#)     

### Pentagon to cut back on mandatory cybersecurity training

Defense Secretary Pete Hegseth issued a new edict to reduce the time personnel spend on cybersecurity training, among other reforms. The directive came in a memo to senior Pentagon leadership and DoD agency and field activity directors, ordering the military departments, in coordination with the Pentagon’s chief information officer, to “Relax the mandatory frequency for Cybersecurity training”. **#TrainingFrequency #Directive**

Source: [DefenseScoop](#)     



# TECHNOLOGIE

## AIR

### ★ Raytheon’s new F/A-18 EW system clears key review



Raytheon has completed a major review of its Advanced Electronic Warfare (ADVEW) prototype for the U.S. Navy’s F/A-18E/F Super Hornet, a step the company said validates both hardware and software progress toward replacing the aircraft’s current self-protection suite. The checkpoint, the firm say, assessed integration of the system’s software with flight-representative hardware and other defensive subsystems, ensuring alignment with government reference architecture. Raytheon described the milestone as critical for advancing the program on the Navy’s accelerated fielding schedule. **#Raytheon #ADVEW**

Source: [UK Defence Journal](#)     



### China reports mass production of quantum radar components capable of detecting stealth aircraft

Chinese researchers claim to have begun mass-producing a single-photon detector, a critical component for quantum radar systems potentially able to detect stealth aircraft such as the U.S. F-22 and F-35. Developed at the Quantum Information Engineering Technology Research Center in Anhui province, the four-channel “photon catcher” is designed to isolate individual photons and resist electronic warfare interference. The technology could, in theory, make radar systems immune to spoofing and jamming by relying on quantum-state correlations. **#China #Quantum**

Sources: [Quantum Insider](#), [China South Morning Post](#)     



### South Korea’s missing link: why stand-off electronic warfare aircraft are critical to deterring North Korea

South Korea’s armed forces have modernized at impressive speed, from fifth-generation fighters to advanced missile defense and a growing blue-water navy. Yet one critical vulnerability remains: control of the electromagnetic spectrum. That is why leading air forces have normalized stand-off electronic attack aircraft and embraced electromagnetic spectrum operations (EMSO)—the doctrinal umbrella that fuses electronic attack, electronic protection, and electronic support with spectrum management and multi-domain planning. **#EMSO #Deterrence**

Source: [Defence talk](#)     



# TECHNOLOGIE

## AIR

### Safran unveils Skydel NAVWAR counter-UAV software solution

Safran Electronics & Defense announced the launch of Skydel NAVWAR: a software solution designed to strengthen national defense capabilities against hostile unmanned aerial vehicles (UAVs). As the core of Safran's counter-UAV (C-UAV) systems, Skydel NAVWAR disrupts UAV navigation by simulating authentic GNSS signals, providing armed forces and other organizations with advanced protection for their most critical assets and events. Skydel NAVWAR empowers integrators to build sovereign spoofing systems. **#Safran #SkydelNAVWAR**

Source: [European Security & Defence](#)     



### Türkiye's Akinci drone shifts to electronic warfare role with Aselsan's new pod suite

On 24 October 2025, Türkiye's unmanned airpower took a substantive step toward electronic-warfare led air campaigns as announced by Baykar and further detailed by Aselsan, with fresh evidence that the Bayraktar Akinci is flying with a dedicated Electronic Support pod and an Electronic Attack pod. The pairing shifts a HALE-classUCAV from ISR and strike into emitter discovery, jamming and deception roles that traditionally depended on scarce crewed aircraft. The development is timely as integrated air defenses harden across multiple theaters, making EW the entry ticket for any strike package. **#Akinci #PodSuite**

Source: [Army Recognition](#)     



### Swedish Army receives first Gripen E fighters as rollout enhances sensor range and EW resilience



The Swedish Armed Forces announced on X the official receipt of the first JAS 39 Gripen E, a key step for the Flygvapnet and for the modernization of national air defense. The acceptance ceremony is taking place at the Skaraborg Air Wing F 7, the operational entry point for the new standard, with a clear objective: to reinforce Sweden's air defense and begin the rollout of the Gripen E system across units. Defense Minister Pål Jonson stated that Sweden will receive a total of 60 Gripen E and noted that the aircraft includes advanced electronic-warfare equipment, flight-tested AI functions, and the ability to load new software in a matter of hours to support agility and rapid updates. **#GripenE #Resilience**

Sources: [Army Recognition](#), [Swedish Armed Forces](#)     



### Small-form-factor EW scales from exquisite strike weapons to affordable mass drones

In an interview with Breaking Defense, BAE Systems' Ed Leonard and Dan Mooney, product line director and business development director for small form factor solutions, discussed how advances in unmanned systems are transforming the electronic warfare landscape. As swarms of small expendable drones and larger armed platforms redefine battlefield dynamics, EW capabilities such as jamming, spoofing, and spectrum control have become mission-critical. The executives highlight the need for rapidly adaptable, small-form-factor solutions to keep pace with evolving threats and ensure tactical superiority. **#MassDrones #Interview**

Source: [Breaking Defense](#)     



## MARITIME

### Introducing PntGuard – the ultimate safeguard against GNSS spoofing and jamming at sea

Tschudi Shipping Company, NAL Research, and SGM Technology AS commercially launched PntGuard™, a maritime-security solution that provides pinpoint situational awareness. It supports navigational integrity at a time when GNSS signals can no longer be taken for granted. A standalone navigational aid independent of all other bridge systems, PntGuard delivers instant alerts the moment a vessel's position is falsified, providing true position data when other bridge systems are compromised. **#PntGuard #Resilience**

Source: [The AI Journal](#)     



## LAND

### Leonardo DRS spells out its latest approach to counter-UAS for the U.S. Army

Leonardo DRS has revealed a new capability in its range of what it calls Maneuver Air Defense payloads. The new Air Defense Light Variant (ADLV) is based on the Joint Light Tactical Vehicle (JLTV) as a lighter-weight member of its counter-unmanned aerial system (C-UAS) and short-range air defense family. The AV Titan 4 provides electronic warfare support, and a Skyview system offers passive detection of unmanned aircraft. This is all packed into an extremely mobile and supportable platform that the JLTV provides. **#ADLV #USArmy**

Source: [TWZ](#)     



### Trends driving offensive and defensive cyber warfare

In this Breaking Defense eBRIEF, the evolution of U.S. cyber warfare strategy is examined as the Pentagon adapts to new forms of conflict that extend beyond traditional networks. Facing adversaries capable of infiltrating through the radio spectrum and disrupting weapon systems, the U.S. Army is developing "RF-enabled cyber," which merges electronic warfare and hacking to deliver non-kinetic effects such as sensor disruption and data manipulation. Simultaneously, the Department of Defense is advancing its Zero Trust framework across both IT and operational technology systems, including SCADA networks and platforms like HIMARS, to secure command-and-control pathways and maintain combat resilience in future conflicts. **#USArmy #RF**

Source: [Breaking Defense](#)     



# TECHNOLOGIE

## LAND

### Navigation warfare is about the battle to assure positioning, navigation, and timing

Through the Army's Mounted Assured Positioning, Navigation, and Timing program of record called MAPS Gen II, soldiers, Marines and allied forces have a fielded system they can depend upon to provide an authoritative and reliable source of truth for positioning, navigation, and timing. MAPS Gen II augments M-Code with a variety of alternate sources of navigation data and signals of opportunity, all brought together by a multi-source sensor fusion engine. Collins Aerospace, an RTX business, has delivered MAPS Gen II systems to the U.S. Army and U.S. Marines and will continue deliveries under Full Rate Production. **#USArmy #MAPSGenII**

Source: [Breaking Defense](#) (EW) (UV) (ISR) (AI) (QT)



### Iran unveils upgraded Emad and Qadr ballistic missiles with electronic warfare in hidden tunnels

Iran's state television carried a rare look inside an IRGC "missile city" on October 18, with commanders presenting an upgraded Emad and a Qadr fitted with counter-EW measures intended to protect the launch chain and complicate hostile fire control. The segment emphasized operational missiles mounted on TELs and readied for quick moves between covered galleries and pre-surveyed firing points, a message aimed at domestic audiences and foreign militaries watching Iran's post-conflict reset. While the broadcast offered limited technical detail, it singled out Qadr's anti-jamming package and described Emad as modernized and in service. **#Iran #BallisticMissiles**

Source: [Army Recognition](#) (EW) (UV) (ISR) (AI) (QT)



### Advanced Navigation expands PNT capabilities with EW resilient INS

Advanced Navigation, a global leader in Assured Positioning, Navigation and Timing (APNT) and autonomous systems, has introduced a new line of defense-ready Inertial Navigation Systems (INS), featuring integrated Electronic Protection (EP) capabilities. Purpose-built to counter Electromagnetic Warfare (EW) threats, the EP product range ensures mission continuity and confidence amidst a global surge in GNSS jamming and spoofing engagements. **#INS #Jamming**

Source: [Advanced Navigation](#) (EW) (UV) (ISR) (AI) (QT)



## SPACE

### Neuraspace boosts defense resilience with new system to respond to threats to space assets

Neuraspace has announced its increased investment and renewed commitment to the defense and civil protection sector with the launch of "Neuraspace DEF". The new system is designed to provide rapid, autonomous responses to the growing range of risks and threats facing space assets. These risks and threats include jamming and spoofing of communications and navigation, cyberattacks on satellites and control stations, collisions with space debris, anti-satellite weapons (ASAT), orbital espionage, and potentially intrusive orbital technologies. **#NeuraspaceDEF #Resilience**

Source: [Satcom.digital](#) (EW) (UV) (ISR) (AI) (QT)



### Poland pushing back: Initiatives tackling GNSS jamming and spoofing

Poland has emerged as one of the most active European states confronting real-world GNSS interference. Over the past two years Polish researchers, government labs and commercial teams have moved from descriptive studies to operational pilots, deploying sensors, building monitoring networks and developing mitigation tools that protect aviation, maritime operations and critical infrastructure. **#Poland #Jamming**

Source: [Inside GNSS](#) (EW) (UV) (ISR) (AI) (QT)



### WISeKey's WISeSat.Space to test post-quantum communication from space during SpaceX launch on November 10

WISeKey International Holding Ltd announced that its subsidiary, WISeSat.Space, in collaboration with its other subsidiary, SEALSQ Corp, is set to launch its next-generation post-quantum-secure satellite aboard a SpaceX Falcon 9 rocket. This satellite will serve as a testbed for post-quantum communication protocols from space, a pivotal step in developing quantum-resilient satellite-based IoT connectivity via satellite infrastructure. **#Quantum #SecureConnectivity**

Source: [WISeKey](#) (EW) (UV) (ISR) (AI) (QT)



### Airbus-built SpainSat NG-II launched, completing Spain's most advanced secure space program

Airbus has successfully launched the SpainSat NG-II secure communications satellite, the second of two next-generation spacecraft built for Spain's Ministry of Defense. The launch took place from the Kennedy Space Center, completing the SpainSat NG program. This milestone marks the culmination of Spain's most ambitious space project to date and delivers the most advanced government communications system in Europe. **#SpainSatNG-II #SecureCommunications**

Source: [Defence Industry Europe](#) (EW) (UV) (ISR) (AI) (QT)



## TECHNOLOGIE

### SPACE

#### **Anvil Secure and D-Orbit outline steps to advance satellite cybersecurity across mission operations**

Cybersecurity specialist Anvil Secure and the space logistics firm D-Orbit have jointly unveiled a comprehensive white paper addressing the application of cybersecurity measures throughout the lifecycle of satellite missions. The new publication centers on D-Orbit's ION Satellite Carrier, describing operational stages and providing strategic direction for manufacturers of small satellites. The guide recommends specific mitigations including encryption of radio communications, thorough validation of hosted payloads, and robust firmware protection. **#Resilience #WhitePaper**

Source: [SpaceWar](#)     



### CYBER

#### **FIU Cybersecurity researchers develop midflight defense against drone hijacking**

Florida International University (FIU) computer scientists unveiled SHIELD, a defensive system that can detect and neutralize cyberattacks on drones in real time and, crucially, allow the drone to finish its mission. Mohammad Ashiqur Rahman, lead researcher and associate professor in FIU's Knight Foundation School of Computing and Information Sciences, said, "Without robust recovery mechanisms, a drone cannot complete its mission under attacks, because even if it is possible to detect the attacks, the mission often gets terminated as a fail-safe move. What's important about our framework is that it helps the system recover, so the mission can be completed." **#SHIELD #DroneHijacking**

Source: [Design Development](#)     



## MARKET & COMPETITION

### AIR

#### **General Atomics boosts U.S. Army Gray Eagle drone with new EW upgrade**

The U.S. Army has contracted General Atomics Aeronautical Systems (GA-ASI) to add a new electronic warfare system to its MQ-1C Gray Eagle unmanned aerial system (UAS), expanding the aircraft's ability to detect and disrupt enemy communications and radar. It uses an open architecture design called the C5ISR Modular Open Suite of Standards, or CMOSS, which lets the service rapidly install and update technology across different systems. The new equipment is the third electronic warfare package added to the Gray Eagle, joining features for electronic attack, communications relay, counter-UAS operations, and signal gathering. **#GreyEagle #Contract**

Source: [The Defense Post](#)     



#### **Air Force asks industry for digital signal processing and cyber security for signals intelligence (SIGINT)**

U.S. Air Force researchers are asking industry for electronic warfare (EW) algorithms and techniques to enhance signals intelligence (SIGINT) and analytics of existing and emerging enemy systems. Officials of the Air Force Research Laboratory Information Directorate in Rome, N.Y., re-issued an advanced research announcement earlier this month for the Signals Intelligence Focused Technologies for Exploitation and Reporting (SIFTER) project. SIFTER seeks to mature, prototype, demonstrate, and evaluate algorithms, methodologies, techniques, and capabilities to enable enhanced digital signal processing (DSP), exploitation, dissemination, and analytics of existing and emerging enemy systems. **#SIFTER #Industry**

Source: [Military Aerspaced Electronics](#)     



#### **L3Harris promotes Viper Shield electronic warfare system for South Korean KF-16 upgrade program**

L3Harris is pitching its Viper Shield electronic warfare (EW) system for Lockheed Martin KF-16 fighters operated by the Republic of Korea Air Force (ROKAF). "The world has changed," says Travis Ruhl, L3Harris's international sales leader for the Viper Shield product. "It's no longer a permissive EW environment when it comes to advanced threats and what you need. Viper Shield is an advanced all-digital EW self-protection system for the F-16," he says. The ROKAF is upgrading 134 KF-16 Block 52s to the KF-16V standard. The work includes the addition of the Northrop Grumman AN/APG-83 active electronically scanned array (AESA) radar, an updated cockpit, new weapons integration, a structural life extension, and other improvements. **#ROKAF #Promotion**

Source: [FlightGlobal](#)     



#### **Pramatra Space + Infostellar sign strategic MoU for QKD ground station services**

Pramatra Space and Infostellar Inc. have signed a Memorandum of Understanding (MoU) to partner to establish and conduct joint development for networks to link Quantum Key Distribution (QKD) ground stations that offer secure space communications. Infostellar will provide access to its global ground station network, spanning optical and RF systems, to support Pramatra's upcoming satellite missions. **#QKD #MoU**

Source: [Satnews](#)     



# MARKET & COMPETITION

## AIR

### IAF's Advanced Self-Protection Jammer (ASPJ) procurement to boost Su-30MKI electronic warfare capabilities

The Indian Air Force has issued a Request for Information (RFI) for 100 Advanced Self-Protection Jammer (ASPJ) pods as part of the Super Sukhoi upgrade to enhance Su-30MKI survivability. The ASPJ procurement represents a major market opportunity and capability enhancement, using Digital Radio Frequency Memory (DRFM) techniques to deceive enemy radars and Gallium Nitride (GaN)-based Active Electronically Scanned Array (AESA) transmitters for higher power density, better efficiency, and rapid beam steering. The system will ensure 360° threat coverage and seamless integration with existing Radar Warning Receivers, Missile Approach Warning Systems, and secure data links. **#IAF #Procurement**

Source: [Indian Defence News](#)     



## MARITIME

### Spain moves forward with next-generation naval intelligence ship

Spain is advancing its naval modernization efforts with the launch of the definition phase for a new intelligence ship, designed to enhance the Spanish Navy's capabilities in electronic warfare, cyber defense, and intelligence gathering at sea. Spain's Council of Ministers has authorized the start of the definition phase for the new Spanish Navy Intelligence Ship (BAM-AGI), to be designed and built by Navantia as a replacement for the ageing Alerta A-111. The ship will incorporate systems derived from the Santiago program, which modernizes the Spanish Armed Forces' ability to collect and analyze electromagnetic emissions and signals across all branches. The project forms part of Spain's Industrial and Technological Plan for Security and Defence, reinforcing the Navy's maritime intelligence and EW capabilities.

**#AlertaA-111 #Modernization**

Sources: [Defence Industry Europe](#), [Naval Today](#)     



## LAND

### Indian Army accelerates modernization of its electronic warfare and communication systems with several contracts

The Indian Army is advancing several major programs to strengthen its electronic warfare and secure communication capabilities. The Dharashakti Integrated EW System, approved by the Defence Acquisition Council and valued at ₹5,150 crore (around \$618m), will enhance the Army's control of the electromagnetic spectrum and protect communication networks. In parallel, a new Ground-Based Mobile Electronic Intelligence System (GBMES), worth over ₹1,000 crore (about \$120m), will intercept, track, and analyze enemy radar and communication signals in real time. Additionally, the Army has signed its first-ever contract for indigenously developed Software Defined Radios (SDRs), co-designed by DRDO and BEL and valued at ₹732 crore (around \$88m), to deliver encrypted, high-speed, and interoperable battlefield communications.

**#IndianArmy #Contracts**

Sources: [Defence Capital](#), [SSB Crack](#), [SSB Crack](#)     



### U.S. Army to solicit "electromagnetic warfare rapid integration system" proposals

The U.S. Army's Program Executive Office for Intelligence, Electronic Warfare & Sensors (PEO IEW&S) is planning to release a solicitation for a new program dubbed the Electromagnetic Warfare Rapid Integration System (ERIS). Within PEO IEW&S, the Project Manager Electronic Warfare & Cyber (PM EW&C), Product Lead Electronic Attack (PL EA), is seeking develop "a suite of electromagnetic warfare capabilities to protect Army forces against a wide range of radio frequency-controlled threats, by countering Command and Control (C2) links and other communications links from air and ground".

**#USArmy #Solicitation**

Source: [JED](#)     



## SPACE

### UK Space Agency goes global with 23 new projects

A new batch of 23 projects will strengthen international space partnerships, develop national capabilities and boost economic growth, the UK Space Agency announced. Representing a £6.5m investment under the International Bilateral Fund (IBF), these collaborations unite UK companies and universities with partners from Australia, Canada, France, Germany, India, Japan, Lithuania, and the USA and cover fields such as orbital threat detection, in-orbit servicing and deep-space radar. The selected initiatives span domains including secure communications, satellite manufacturing, biotechnology, space domain awareness, and quantum and AI-enabled technologies. **#UKSA #Projects**

Source: [Gov UK](#)     



### Pramatra Space + Infostellar sign strategic MoU for QKD ground station services

Pramatra Space and Infostellar Inc. have signed a Memorandum of Understanding (MoU) to partner to establish and conduct joint development for networks to link Quantum Key Distribution (QKD) ground stations that offer secure space communications. Infostellar will provide access to its global ground station network, spanning optical and RF systems, to support Pramatra's upcoming satellite missions. **#QKD #MoU**

Source: [Satnews](#)     



# MARKET & COMPETITION

## SPACE

### UK Space Agency goes global with 23 new projects

A new batch of 23 projects will strengthen international space partnerships, develop national capabilities and boost economic growth, the UK Space Agency announced. Representing a £6.5m investment under the International Bilateral Fund (IBF), these collaborations unite UK companies and universities with partners from Australia, Canada, France, Germany, India, Japan, Lithuania, and the USA and cover fields such as orbital threat detection, in-orbit servicing and deep-space radar. **#UKSA #Projects**

Source: [Gov UK](#)     



### Thales Alenia Space and ESA sign contract for SAGA mission to demonstrate Europe's first quantum key distribution governmental service

The European Space Agency (ESA) has signed a €50m contract with aerospace company Thales Alenia Space to begin the preliminary design phase of the Security And cryptoGrAphic (SAGA) mission. This agreement enables SAGA to continue to its preliminary design review, marking a relevant step towards establishing secure, space-based communications using quantum technologies. **#SAGA #Contract**

Sources: [ESA](#), [Satcom.Digital](#)     



### Mercury Systems and Nightwing collaborate to enhance cybersecurity for aerospace and defense systems

In a significant move for the aerospace and defense sector, Mercury Systems Inc. has teamed up with Nightwing to bolster cybersecurity measures in mission-critical hardware. The partnership aims to integrate Nightwing's advanced cyber resiliency technology directly into Mercury's processing systems, which are pivotal for edge computing in high-stakes environments like military operations and intelligence gathering. **#Hardware #Partnership**

Source: [WPN](#)     



### Spanish industry aims to position itself in the QKD league of quantum keys

Two consortia of Spanish companies are working flat out on two projects to develop quantum encryption systems via satellite to create a barrier that will curb cyberattacks and cyber espionage on communications. On the one hand, there is the consortium led by Sener Aeroespacial, which is working to bring a LEO QKD demonstrator to fruition, to be operated from low Earth orbit or LEO. In contrast, the industrial group led by Thales Alenia Space Spain is committed to developing a GEO QKD prototype that will operate from geostationary orbit. **#QKD #Industry**

Source: [Atalayar](#)     



### Securing the final frontier: the need for public-private collaboration on space cybersecurity

This article by Lauryn Williams (CSIS) argues that protecting space systems from cyber-threats requires stronger public-private collaboration. Despite growing risks, industry and government still operate in silos due to classification barriers and limited information sharing. She calls for renewed cross-sector cooperation, urging government to declassify relevant threat data and industry to prioritize cybersecurity in space operations. **#Policy #PublicPrivatePartnership**

Source: [Via Satellite](#)     



### JPMorgan to invest \$1.5tn in U.S. national security

The nation's largest bank announced a 10-year plan to invest up to \$10bn in companies it calls "critical" to economic security and resiliency. The money will target four key areas: defense and aerospace, frontier tech like AI and quantum computing, energy technology including advanced batteries, and supply-chain and manufacturing.

**#Investment #NationalSecurity**

Source: [The Street](#)     



### Airbus, Leonardo, and Thales sign a memorandum of understanding (MoU) to create a leading European space player

Airbus, Leonardo, and Thales have signed a memorandum of understanding (MoU) to combine their space activities within a new company. This new European space player aims to multiply the strike force of the three companies by combining their satellite production activities and related services. The new company could be operational in 2027.

**#NewCompany #MoU**

Source: [Thales](#)     



### ESA backs Leonardo-led program to test quantum-secure space communications

Leonardo will lead a new European initiative to develop a platform for assessing quantum-secure communications, following the award of a multi-year contract from the European Space Agency. The work brings together a consortium including Thales Alenia Space, Telespazio Belgium, ThinkQuantum, and DamoTech. The contract covers the creation of a Quantum Security Validation Platform, an architecture intended to test emerging quantum and post-quantum technologies for space systems. **#ESA #Contract**

Source: [Orbital Today](#)     



# MARKET & COMPETITION

## CYBER

### Peraton books contract to prototype cyber tech platforms for Air Force missions

The Air Force Life Cycle Management Center has tapped Peraton to design, integrate and prototype advanced cyber infrastructure platforms that enable critical Air Force and joint cyber operations. The successful completion of the efforts under the Other Transaction Authority – Prototype, or OTA-P, contract will pave the way for a potential five-year production award. The OTA-P contract’s deliverables include systems engineering, infrastructure and network support, and cyber mission technologies to help operators meet evolving mission needs. **#USAF #Contract**



Source: [Peraton](#)     

# THREAT INTELLIGENCE

## AIR

### Chinese military force tricked a foreign spy plane in South China Sea

According to Chinese sources, one of its electronic warfare (EW) systems has successfully deceived a foreign spy plane over the South China Sea. No mention is made of which kind of aircraft or its nation of origin, but the aircraft was likely American or one of its allies. According to reports, the EW jamming/spoofing was achieved using a vehicle-mounted electronic jamming system. As reported, the Chinese system was able to create fake radar targets, for example, an “imaginary” aircraft carrier or large ship. **#Espionage #SpyPlane**



Source: [Interesting Engineering](#)     

### Ukrainian F-16 pilots sustain air defense amid Russian attacks and electronic warfare threats

One of Ukraine’s top F-16 fighter pilots, call sign “AB,” shared insights into Ukraine’s evolving air war during an appearance at the Mitchell Institute for Aerospace Studies on 6 October. As vice commander of a Ukrainian fighter wing credited with downing more than 1,000 Russian Shahed-type drones and cruise missiles, AB detailed the challenges and progress of Ukraine’s transition to Western air systems. **#F-16 #UkraineWar**



Source: [Defence Industry Europe](#)     

### Decoding the invisible war: India’s rise in EW and SIGINT drones

In this discussion, Air Veteran Dr. Sheikh Akhter from DefenceXP speaks with Mr. Gajendra Kashyap, Co-founder and CTO of NextLeap Aeronautics, to explore how India is building next-generation drone systems capable of Electronic Warfare (EW), Signals Intelligence (SIGINT), and spectrum control. From AI-driven mesh networks to indigenous SDR innovations, this conversation offers deep insights into how India’s defense ecosystem is preparing for the invisible wars of the future – where speed, data, and electromagnetic dominance will define power. **#India #SIGINT**



Source: [Defense XP](#)     

## MARITIME

### Indian minister warns maritime infrastructure could face cyberattacks

India’s Minister of State for Electronics and Information Technology Jitin Prasada warned that the country’s maritime infrastructure is increasingly exposed to cyberattacks, including ransomware, GPS spoofing, and OT system intrusions that could threaten national security. Speaking at a Cyber Security Seminar, he emphasized the economic and strategic importance of India’s maritime sector, through which over 95% of the nation’s trade volume passes. Indian Navy Chief Admiral DK Tripathi underlined that while digitalization enhances efficiency, it also introduces vulnerabilities, making cybersecurity a critical priority for the country’s maritime future. **#India #Awareness**



Source: [The New India Express](#)     

### Pakistan’s air defenders jam, force back Indian intelligence aircraft near maritime border

Pakistan’s electronic warfare units forced back Indian Bombardier Global 5000 surveillance jet attempting to snoop near Pakistan’s maritime frontiers. The sleek, high-altitude aircraft, officially listed as a civilian flight but packed with top-tier electronic intelligence systems, was en route from Abu Dhabi to India when its suspicious flight path triggered Pakistan’s defense alarms. The jet is believed to have been on covert mission to intercept Pakistan’s radar and communication signals near the Special Economic Zone (SEZ) and Air Defense Identification Zone (ADIZ). As aircraft neared these critical zones, Pakistan’s air defense network went into action. State-of-the-art electronic countermeasures jammed the intruder’s communication and navigation systems, leaving the jet effectively blind and deaf in the sky. **#Pakistan #Jamming**



Source: [Pakistan Observer](#)     

# THREAT INTELLIGENCE

## LAND

### Army says it's mitigated 'critical' cybersecurity deficiencies in early NGC2 prototype

The U.S. Army says it has mitigated several cybersecurity risks discovered in an early iteration of its nascent Next Generation Command and Control (NGC2) platform, as detailed in a blunt memo obtained by Breaking Defense. Penned on Sept. 5 and signed by Army Chief Information Office Chief Technology Officer Gabriele Chiulli, the document said the NGC2 platform "in its current state, exhibits critical deficiencies in fundamental security controls, processes, and governance." "These issues collectively create a significant risk to data, mission operations, and personnel by rendering the system vulnerable to insider threats, external attacks, and data spillage," the document said. **#NGC2 #Awareness**

Source: [Breaking Defense](#)     



## SPACE

### China accuses U.S. NSA of 2022 cyberattack on key timing center

China's Ministry of State Security accuses the U.S. NSA of a 2022 cyberattack on the National Time Service Center, exploiting mobile messaging vulnerabilities to steal data and compromise critical timing systems for telecom, finance, and defense. Amid escalating U.S.-China tensions, this highlights mutual cyber espionage risks and calls for enhanced global tech security. **#NSA #Espionage**

Source: [WPN](#)     



### Iran minister rules out claim of HOD-HOD satellite hack

Iran's Minister of Communications and Information Technology Sattar Hashemi has rejected allegations that the HOD-HOD satellite was hacked before the 12-day war imposed by the Israeli regime. He stressed the importance of transparency in cyberspace while also underscoring the need for robust security for these systems. He noted that vulnerabilities may still exist and need to be addressed gradually. **#HOD-HOD #Hack**

Source: [Islamic Invitation Turkey](#)     



### U.S. Space Force general says it's 'concerning' just how fast China is closing the gap on the space tech that backs modern armies

According to Brig. Gen. Brian Sidari, the deputy chief of space operations for intelligence with the U.S. Space Force, China is rapidly catching up on the space-based capabilities that enable modern armies to fight effectively. Beijing has spent years investing in its space operations, and a recent reorganization of the military branch that oversaw space, along with other strategic domains like cyberspace and information warfare, suggested an interest in a more streamlined approach to space-related missions. **#China #SpaceWarfare**

Source: [Business Insider](#)     



## CYBER

### The evolution of Russian physical-cyber espionage

A new analysis by Trellix highlights how Russian state-sponsored hackers, particularly those affiliated with the GRU's APT28 group, continue to blend cyber operations with physical espionage tactics. The report traces this hybrid approach from past incidents such as the Rio Olympics data leaks and the 2018 Hague operation, to recent cases involving teenagers allegedly recruited to place Wi-Fi sniffers near EU institutions. These close-access operations demonstrate Moscow's enduring strategy of merging digital intrusions with on-the-ground tradecraft, blurring the boundaries between cyber and physical domains in pursuit of intelligence objectives. **#GRU #APT28**

Source: [Trellix Industrial Cyber](#)     



### Ransomware group claims breach of Boeing supplier DCS, threatens data leak

Ransomware group J Group claims to have breached Dimensional Control Systems (DCS), a software provider to Boeing, Samsung, Volkswagen, and Airbus, stealing sensitive files and demanding ransom via dark web posts. This unverified incident underscores vulnerabilities in global supply chains, potentially risking intellectual property and national security. Enhanced vendor security measures are urgently needed. **#JGroup #Breach**

Source: [WebProNews](#)     



### CISA Warns of Dassault Systèmes vulnerabilities actively exploited in attacks

CISA has added two critical vulnerabilities affecting Dassault Systèmes DELMIA Apriso to its Known Exploited Vulnerabilities catalog, warning that threat actors are actively exploiting these security flaws in real-world attacks. The alert, issued on October 28, requires federal agencies to implement mitigations by November 18, 2025, while urging all organizations using the affected software to take immediate action. DELMIA Apriso, a widely deployed manufacturing operations management platform used by enterprises worldwide, has become the target of sophisticated cyberattacks exploiting two distinct vulnerabilities. **#Dassault #Vulnerabilities**

Sources: [Cyber Security News](#), [CISA](#)     



# THREAT INTELLIGENCE

## CYBER

### Ex-L3Harris exec guilty of selling cyber exploits to Russian broker

Peter Williams, an Australian national and a former general manager at U.S. defense contractor L3Harris Trenchant, has pleaded guilty in U.S. District Court to stealing and selling confidential cybersecurity information to a Russian vulnerability exploit broker. The illegal activity took place between 2022 and 2025, when Williams stole at least eight protected exploit components from Trenchant intended for the exclusive use of the U.S. government and select allies, and sold them to a broker that, among other clients, works with the Russian government. **#DataLeak #Espionage**



Source: [Bleeping Computer](#)     

### Ex-Mossad chief, behind ICJ blackmail campaign, brags Israel has installed a global sabotage network

In a shocking admission, former Mossad director Yossi Cohen has openly boasted that Israel has deployed a global sabotage and espionage network which uses “booby-trapped and spy-manipulated equipment”. The method, denounced as terrorism by ex-CIA chief Leon Panetta, was used to target Hezbollah and now, according to Cohen, is embedded in “all the countries you can imagine.” In a video that’s now circulating on social media, Cohen is seen speaking on The Brink podcast hosted by Jake Wallis Simons, editor of The Jewish Chronicle. The former Mossad director, who led a blackmail campaign against ICJ judges, detailed the covert program Israel has planted across the globe. **#Mossad #Sabotage**



Source: [Middle East Monitor](#)     

### Scada over radio: vulnerabilities in RF links

The article highlights the overlooked vulnerabilities of Supervisory Control and Data Acquisition (SCADA) systems that operate over radiofrequency (RF) links rather than traditional wired networks. While RF-based SCADA enables flexibility and remote control for critical infrastructure, it also exposes systems to interception and manipulation through low-cost software-defined radios (SDRs) and tools such as Universal Radio Hacker. Major attack vectors are outlined (replay attacks, eavesdropping, protocol weaknesses and RF jamming), showing how unencrypted and unauthenticated protocols leave industrial systems open to disruption or sabotage. **#SCADA #RF**

Source: [Investigator515](#)     

# TRAINING & EDUCATION

## LAND

### Indian Army's Northern Command conducts multi-domain warfare exercise Vidyut Vidhhwans

The Indian Army's Northern Command conducted a large-scale multi-domain and multi-agency exercise called Vidyut Vidhhwans (13–16 October) to simulate futuristic warfare scenarios involving cyber, space, electromagnetic, and cognitive threats. The exercise included the Indian Army, Air Force, and Navy, as well as Central Armed Police Forces, government agencies, and private industry players, promoting a whole-of-nation approach to national defense. Troops practiced countering cyber intrusions, spectrum saturation, jamming, spoofing, and cognitive attacks. Army Commander Lt Gen Pratik Sharma emphasized the need to integrate niche technologies and maintain innovation to ensure readiness across all domains, especially amid continuing tensions along the borders with China and Pakistan. **#IndianArmy #Exercise**



Source: [New Indian Express](#)     

## SPACE

### Unverified COTS hardware enables persistent attacks in small satellites via SpyChain

The paper “SpyChain: Multi-Vector Supply Chain Attacks on Small Satellite Systems” introduces SpyChain, a framework for studying supply chain threats in small satellite systems. Unlike prior work focused on direct software attacks, SpyChain examines risks from third-party COTS hardware that often lacks strong verification but has deep system access. Using NASA’s NOS3 simulator, it demonstrates the first practical, persistent, multi-component supply chain attack on small satellites. **#SpyChain #COTS**



Sources: [Security Affairs](#), [Cornell University](#)     

### The frequency war: towards the commodification of spectrum/orbit resources?

This French study of the IRSEM explores the growing competition for access to the electromagnetic spectrum and orbital positions, strategic resources that are limited and have become commodities due to the proliferation of low-Earth orbit satellite constellation projects. **#IRSEM #Paper**



Source: [IRSEM](#)     



# TRAINING & EDUCATION

## CYBER

### Cyberspace: a new strategic and diplomatic battlefield

On the occasion of Cyber Month and United Nations Day on October 24, ACADEM explores the intersection between cyberspace and international governance. How has this intangible domain become a new arena of power, confrontation, and diplomacy? #TrainingFrequency #Directive



Source: [Académie de défense de l'Ecole militaire](#) EW UV ISR AI QT

*CyberInflight is a Market Intelligence company dedicated to the topic of Space Cybersecurity & Defense. The company provides strategic market and research reports, bespoke consulting, market watch & OSINT researches and cybersecurity awareness training.*

Contact us at: [research@cyberinflight.com](mailto:research@cyberinflight.com)