



CYBER DEFENSE MONTHLY WATCH

November 2025

Number of articles identified: 83

- # Geopolitics:** 23
- # Technology:** 13
- # Market:** 14
- # Regulation:** 5
- # Threat intelligence:** 17
- # Training & Education:** 11

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 month, defense developments have underscored the increasing integration of multi-domain capabilities, technological innovation, and operational resilience. In **India, the U.S., and Malaysia are embedding cyber, space, and electronic warfare into conventional operations.** Lt Gen Raj Shukla stressed India's need to fuse manned aircraft with unmanned platforms and advanced EW, cyber, and space systems. At the same time, the U.S. Army launched the 1st Theater Information Advantage Detachment in Hawaii to counter malign influence in the Indo-Pacific. **Malaysia's upcoming Cyber and Electronic Defense Command will centralize AI-enabled cyber and electromagnetic operations,** reflecting a global shift toward information-centric force design.

Market activity mirrors these strategic priorities. **CACI secured a \$79 million task order to support DEVCOM's C5ISR Center,** enhancing Army EW and intelligence capabilities. In space, the **UAE's NSSTC has partnered with Thales Alenia Space on LEO-based navigation solutions,** thereby strengthening sovereignty and international collaboration. Meanwhile, France is modernizing its naval fleet through the CNN MCO, Thales, and CS Group, upgrading amphibious helicopter carriers and other critical vessels to maintain operational readiness.

Technological innovation is driving new operational approaches. Northrop Grumman's TEEMS payload turns drones, robots, and unmanned vessels into mobile EW nodes. Deloitte's **Deloitte-1 satellite demonstrates space-based cyber defense,** detecting intrusions directly in orbit. In Europe, **Thales' MISTRAL post-quantum encryptor secures Restricted-level communications against emerging quantum threats,** highlighting the growing emphasis on resilient, autonomous, and integrated systems across domains.

Regulatory initiatives are adapting to these challenges. **Aerospace Corporation's SPARTEND integrates space-cyber threat intelligence with anomaly detection for autonomous satellite defense,** while Pakistan plans to establish a federal cybersecurity authority and amend the PECA to secure critical infrastructure and coordinate national cyber defense.

Threat intelligence reveals increasingly sophisticated cross-domain risks. CISA warned critical infrastructure operators to treat low-altitude airspace as an active attack surface due to rising drone threats. **Chinese simulations explored large-scale EW against Starlink over Taiwan,** requiring massive drone deployment to succeed. At the same time, **European leaders urged coordinated industry-military preparedness for high-intensity cyber threats,** illustrating the convergence of physical, electronic, and cyber domains.

Training and education reflect those preoccupations; the **U.S. Coast Guard mandated cybersecurity training for personnel with IT or OT access by January 2026.** Ukraine's EW and cyber units leverage electromagnetic capabilities against unmanned aerial threats. At the same time, Europe hosted its first **multi-satellite cybersecurity competition, CTRL+Space Capture-the-Flag,** enhancing hands-on expertise in defending space assets.

GEOPOLITICS

AIR

To coordinate strikes from space, U.S. needs space JTACs, experts argue

As space-based weapons move from concept to reality, experts argue that special operations forces will need Space Joint Terminal Attack Controllers (SJTACs) to coordinate orbital strikes much like JTACs direct airstrikes today. Embedding SJTACs with special operation forces (SOF) units would allow them to assess vulnerabilities, integrate space-based reconnaissance and cyber tools, and guide precision attacks using future capabilities such as lasers, EMP weapons, kinetic "Rods from God." Proponents contend that SJTACs must belong to U.S. Space Force to develop deep expertise, avoid redundancy across services, and ensure interoperability with NATO partners lacking their own space assets. #SJTACs #SOF

Source: [C4ISRNET](#)     



Need to develop and integrate space, electronic warfare and cyber capabilities with manned aircraft for air dominance: Indian Lt Gen Shukla

Stating that the quality of airpower will determine victory or defeat in any future fight, Former Indian General Officer Commanding-in-Chief, Army Training Command, Lt Gen Raj Shukla said that towards this end, it was imperative to integrate manned aircraft with unmanned platforms, space, cyber and electronic warfare capability. "In order to achieve air superiority, the adversary's kill chains that we have to defeat are very complex. And the instruments to defeat these enemy kill chains are EW, space, cyber, information, dominance, stealth and now AI," he said while speaking at the Military Literature Festival in Chandigarh. #Capability #IndianStrategy

Source: [The Tribune India](#)     



How U.S. Air Force prepares to fight inside a contested electromagnetic environment

The 74th Mission Generation Force Element at Moody Air Force Base is training under Mosaic Tiger 26-1 to sustain A-10 operations when communication with the Air Operations Center becomes unreliable. The exercise shows how mission command and longer planning cycles help units keep generating combat airpower inside a contested electromagnetic environment. Airmen describe the event as a deliberate test of decentralized execution, noting that a seventy-two-hour Air Tasking Order gives pilots enough approved targets, airspace blocks, and tanker windows to keep flying even when updates from the Air Operations Center arrive sporadically. #USAF #Exercise

Source: [Army Recognition](#)     



India, France ink pact to deepen collaboration in defense R&D

The Defence Research & Development Organisation (DRDO) of India and the Direction générale de l'Armement (DGA) of France signed a technical agreement to strengthen bilateral cooperation in defense research and development, establishing a formal framework for joint research, training programs, information exchange and technology transfers in areas such as aeronautical platforms, unmanned vehicles, advanced materials, cybersecurity, artificial intelligence, space, navigation, advanced propulsion, advanced sensors, quantum technologies and underwater systems. #R&D #Agreement

Sources: [The New Indian Express](#), [Forum Militaire](#)     



India increases efforts to collect GNSS spoofing data

India's aviation regulator, the Directorate General of Civil Aviation (DGCA), is collecting data on GPS interference and spoofing to have a better understanding of the situation, reports several news outlets in the country. The urge to collect data comes after the Delhi airport experienced issues at the beginning of the month. Following a circular issued by the Directorate General of Civil Aviation in 2023, instances of GPS interference/spoofing have been reported since November 2023. Recently, several airlines have faced GPS spoofing at the New Delhi airport, with at least eight such instances on Nov. 5, said an unnamed DGCA official. #DGCA #SpoofingData

Source: [GPS World](#)     



LAND

Marine Corps to pay \$15,000 bonuses to attract cyber, electronics recruits

As the Marine Corps gets increasingly technology-focused in calibrating for future battles, the service is, for the third year in a row, preparing to dole out substantial enlistment bonuses to recruits willing and able to do battle in the cyber realm. According to a Marine Corps Administrative Message published Nov. 3, bonuses worth up to \$15,000 are available for enlistees in the fields of electronic maintenance and cyber and crypto operations. #MarineCorps #Recruitment

Sources: [MilitaryTimes](#), [Marine Corps](#)     



New Army unit seeks to disrupt 'malign influence' in Indo-Pacific

The U.S. Army activated a new unit aimed at "disrupting malign influence" in the Indo-Pacific region, bringing information operations into the conventional battlespace. Headquartered on Fort Shafter, Hawaii, the 1st Theater Information Advantage Detachment, or 1st TIAD, was officially launched Nov. 7, the unit's public affairs officer said in a statement, adding that the unit is "a direct reporting unit" to the U.S. Army Pacific commander. The unusual 65-soldier formation combines military intelligence, psychological operations, electronic warfare, public affairs, civil affairs, information operations and cyber operations into a set of dedicated teams. #USArmy #NewUnit

Sources: [Army Times](#), [U.S. Army](#)     





GEOPOLITICS

LAND

Delhi: Electro Magnetic Board discusses jointness in electronic warfare

The annual meeting of the Joint Electro Magnetic Board (JEMB), held under the chairmanship of Air Marshal Rakesh Sinha in New Delhi, focused on synergy and integration for the three Services in the fields of Electronic Warfare, EMI/EMC, counter-UAS operations, emerging technologies, and spectrum management. The event featured a demonstration of an Electromagnetic Battlespace Management System for tactical battlefield use and the release of the Technical News Letter (TNL) 2025 outlining future warfare technologies. **#India #JEMB**

Source: [Social News XYZ](#) **EW UV ISR AI QT**



Indian CDS calls for incorporating lessons from Operation Sindoor into the theatre model

Post Operation Sindoor, there are some "more lessons" that the armed forces have learned and it needs to be incorporated into the model of the planned theaterisation, according to Indian Chief of the Defense Staff Gen Anil Chauhan. In his remarks, he also said that "we should have our ISR (intelligence, surveillance and reconnaissance) and kinetic operation capabilities across the length and breadth of Pakistan, that would be I think, new normal" post the decisive military operation conducted in May. He added that "we should be better prepared in our air defense, counter-UAS, and electronic warfare". **#OperationSindoor #Strategy**

Source: [Business Standard](#) **EW UV ISR AI QT**



SPACE

U.S. Space Force deploying ground-based jammers to counter Chinese, Russian surveillance

The U.S. Space Force is preparing to field 2 new ground-based systems designed to jam Chinese and Russian spy satellites, expanding the Pentagon's ability to disrupt enemy surveillance in space. Called Meadowlands and the Remote Modular Terminal (RMT), the systems will join the older Counter Communications System, which became operational in 2020 to "dominate the electromagnetic spectrum" during conflict. While still in early deployment phases, Space Force officials said the weapons are capable of being "operationally employed" now if needed. **#USSF #Jammers**

Sources: [The Defense Post](#), [The National Interest](#) **EW UV ISR AI QT**



UK commits £155m to protect critical positioning and timing signals

The UK government has pledged £155m (\$203m) to strengthen the country's Positioning, Navigation and Timing (PNT) infrastructure, aiming to protect everything from mobile networks to financial trading systems from disruption. The funding package, announced on 19th November by Science Minister Lord Vallance, is designed to boost national security and support the wider digital economy. **#UK #PNT**

Sources: [Gov UK](#), [Orbital Today](#) **EW UV ISR AI QT**



NATO, German BSI, and Israel's Rafael share strategies for securing space systems

As space becomes a domain of warfare, democracies across the globe will increasingly rely on commercial satellite operators and private sector space companies to wage it, Daniel Hilgert, a senior NATO official told at CyberSat conference. NATO is setting up a commercial integration cell at the alliance's new Space Operations Center (SOC) at Ramstein U.S. Air Force Base. The German government has put its shoulder behind the effort to secure its national space capabilities. According to Michael Bernat, cyberCTO of Israeli defense tech outfit Rafael Advanced Defense Systems, the cutting edge of space innovation might turn out to be a double-edged blade. **#NATO #SOC**

Source: [Satellite Today](#) **EW UV ISR AI QT**



Deputy Minister Danielė: Europe must strengthen the resilience of its satellite navigation system amid hybrid threats

According to the Deputy Minister of Transport and Communications of Lithuania, Akvilė Danielė, it is essential for the European Union to reach an agreement on a specific action plan that would enable a coordinated response to hybrid threats stemming from disruptions to satellite navigation systems (GNSS). She notes that the GNSS interference is expanding beyond airspace into other vital sectors and is becoming increasingly sophisticated. **#EU #Awareness**

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



NRO establishes Space Cyber Program after last month's Moonshine Guardian exercise

The National Reconnaissance Office (NRO) has launched a new Space Cyber Program to centralize space cybersecurity efforts across the agency. NRO officials stressed that today's evolving threat landscape requires integrating cybersecurity into space systems from the start. They noted that most vulnerabilities lie in the ground segment, where a compromised ground station can give adversaries full access to a satellite. The program underscores the need for onboard detection, response, and recovery capabilities, as essential protections such as intrusion detection or multi-factor authentication still are not consistently deployed across U.S. space systems. **#NRO #SpaceCyberProgram**

Source: [Via Satellite](#) **EW UV ISR AI QT**





GEO POLITICS

SPACE

The German Federal Government presents the first space safety and security strategy

Germany unveiled the country's first national space security strategy, with Defense Minister Boris Pistorius vowing to expand military and civilian capabilities in orbit. The strategy covers all areas relevant to Germany's security, from spaceflight projects to the expansion of satellite networks and promoting responsible state behavior in space. The objective is to become more capable of action also in space with partners in the EU, NATO and other partners around the world. The strategy comes weeks after Pistorius announced plans for the Armed Forces to spend €35bn (\$41bn) by 2030 on space defenses, citing growing threats posed by Russia and potentially China. **#SpaceSecurity #Strategy**

Sources: [Breaking Defense](#), [German Government](#)     



ESA raises more than €22bn at ministerial

At a press conference at the conclusion of the two-day ministerial conference, ESA Director General Josef Aschbacher announced that ESA member states had agreed to provide €22.1bn (\$25.58bn) for the agency's programs. The funding was a 32% increase from the €16.9bn ESA received at the previous ministerial in 2022. "I think this message of Europe needing to catch up and to step up and literally elevate the future of Europe through space has been taken by our ministers very seriously", he said. **#ESA #Budget**

Source: [Space News](#)     



CYBER

Malaysia's Cyber and Electronic Defence Command to launch with drones and AI integration

The Malaysian Armed Forces (ATM) Cyber and Electronic Defence Command is expected to be officially launched this December, said Deputy Defense Minister Adly Zahari. He said the country's defense transition towards a smart military is underway through a transformation that emphasizes artificial intelligence (AI), automated weapon systems and strengthened cyber warfare capabilities. "This cyber command will serve as the center of gravity for cyber and electromagnetic operations, while the Future Forces concept will shape doctrines, structures, and high-technology assets capable of operating in a digital battlespace," he said. **#ATM #CyberElectronicCommand**

Source: [Malaymail](#)     



European Cyber Week : « Only those who are fighting the battle in cyberspace today will be ready for tomorrow's clash. » (French Air Force Major General Emmanuel NAËGELEN, COMCYBER)

During European Cyber Week 2025 in Rennes, French Air Force Major General Emmanuel Naëgelen spoke for the first time since his appointment as commander of cyber defense about the challenges of cyberspace and the mission of the Cyber Defense Command. He spoke about how Cyber Defense Command is preparing for high-intensity conflict tomorrow, and what is the link between electromagnetic warfare and cyber defense. **#COMCYBER #Strategy**

Source: [MINARM](#)     



The NATO Electronic Warfare Advisory Committee (NEWAC) convenes in Istanbul

From 4 to 6 November 2025, the NATO Electromagnetic Warfare Advisory Committee (NEWAC) held its 118th plenary meeting at the Multinational Joint Warfare Centre in Istanbul. The widespread use of Electromagnetic Warfare (EW) in Ukraine and in the Middle East demonstrates that it has become a crucial domain in modern warfare. From attacks on radar systems, to jamming of communications and navigation systems, to electronic masking, probing, reconnaissance and intelligence gathering, EW can be applied in all operational domains – air, land, maritime, space and cyber. NATO's ability to counter the use of EW by adversaries is essential for security across the Alliance. **#NATO #NEWAC**

Source: [NATO](#)     



South Asia's evolving environment: Electronic warfare, cyber operations significantly alter strategic landscape: experts

Dr. Asma Khawaja, Executive Director of the Center for International Strategic Studies (CSIS), while describing South Asia's evolving environment as one of "tri-compression" of space, time, and domains, has said that electronic warfare and cyber operations have significantly altered the strategic landscape and stability between India and Pakistan "remains fragile" as emerging technologies had become central to strategic planning. She underscored the need to integrate cyber warfare considerations into modern military planning and called for dismantling "constructed narratives" that distort regional realities. **#CSIS #HybridWarfare**

Source: [UrduPoint](#)     



"Domain where borders don't exist...": Indian Air Marshal Ashutosh Dixit on possibilities in cyber, space and electronic warfare

Air Marshal Ashutosh Dixit, Chief of Integrated Defence Staff, noted that the possibilities in cyber warfare, space, and electronic warfare are limitless because there are no borders in these domains. He noted that a cyber agency and a defense space agency have been established in the country, and that efforts are being enhanced. Speaking at ANI's National Security Summit, he emphasized that the country is adopting a whole-of-nation approach in these areas. **#India #Strategy**

Sources: [ANI News](#), [Web India](#)     





GEOPOLITICS

CYBER

Electromagnetic warfare: NATO's blind spot could decide the next conflict

The war in Ukraine has exposed a critical front long neglected by Western militaries: electromagnetic warfare (EW). Control over this invisible battlespace, where communications are jammed, drones blinded, and precision weapons thrown off course, can decide the outcome of a conflict. Russia has understood this sooner than NATO, using EW to isolate Ukrainian units, disrupt command networks, and neutralize Western systems. Ukraine has adapted with ingenuity, but it is learning in combat what NATO should have learned in training. **#NATO #Opinion**

Source: [Rand](#)     



EDA urges stronger EU integration of cyber and electromagnetic capabilities in defense operations

The European Defence Agency (EDA) is calling for greater coordination between cyber and electromagnetic capabilities to keep pace with the rapid digital transformation of military systems and the growing reliance on the electromagnetic spectrum for operations. At its Cyber Electromagnetic Activities (CEMA) industry day, the EDA emphasized that uncoordinated efforts risk interference, while integration can significantly enhance operational effect. **#EDA #CEMA**

Source: [Defence Industry Europe](#)     



REGULATION

SPACE

Aerospace's SPARTEND integrates space-cyber threat knowledge with autonomous detection

Merging the strategic insights provided by SPARTA with the anomaly detection capabilities of DARS is critical to real onboard intrusion detection and mitigation capability. This is the purpose of SPARTEND, short for SPARTA Telemetry Encoder Neural Network to DARS. **#AerospaceCorporation #SPARTA**

Source: [Aerospace Corporation](#)     



European defense leaders call for a cohesive military SATCOM framework

The growing role of satellites in defense was one of the key themes of Global MilSatCom, with leaders from the German Federal Armed Forces, Swiss Armed Forces and the European Space Agency (ESA) sharing insights. According to Maj. Gen. Armin Fleischmann "You need one project, a unified, sustained European investment framework. You need to speak with one voice, one budget, and have shared objectives. You need common standards for safety and security. Every nation procures its own systems. We need to build one great project and have a common understanding. This is a very big issue for us," he said. **#SATCOM #Framework**

Source: [Via Satellite](#)     



New cybersecurity rules for Pentagon's commercial satellite vendors

The Pentagon recently issued new rules on cybersecurity measures that commercial satellite operators must employ if their products or services are used by U.S. intelligence agencies or military services. The rules, from the Pentagon-led interagency Committee on National Security Systems contain important new provisions, Brandon Bailey from Aerospace Corp., a federally funded research and development nonprofit, told the annual CyberSat conference. **#Pentagon #Rules**

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



CYBER

Trump FCC deregulates telecom cybersecurity, betting on self-policing amid China hack fallout

In a swift deregulatory move, the Federal Communications Commission under President Donald Trump's appointees has rescinded a Biden-era mandate requiring internet service providers to submit annual cybersecurity reports. The decision shifts oversight to voluntary self-certification by telecom giants, drawing sharp rebukes from privacy advocates and Democrats even as FCC leadership hails it as a path to more agile defenses. The rule change comes just months after Chinese hackers dubbed Salt Typhoon infiltrated major U.S. telecom. **#FCC #Deregulatory**

Source: [WPN](#)     



Pakistan to establish federal cybersecurity authority to combat cyber-threats

The federal government of Pakistan has announced plans to establish a dedicated cybersecurity authority aimed at strengthening national cyber defenses. The proposed authority will play a central role in implementing cybersecurity measures nationwide and will advise on strategies to protect "critical national infrastructure" from cyber-threats. The Ministry of Information Technology has circulated the draft Cybersecurity Act to stakeholders for consultation. In addition, the government is proposing amendments to the Prevention of Electronic Crimes Act (PECA) to support the new framework. **#Framework #CybersecurityAct**

Source: [Pakistan Observer](#)     





TECHNOLOGY

AIR

Ukraine's indigenous recon drones challenge China's DJI Mavic 3 across the battlefield

Forbes disclosed that Ukraine began fielding its first thousand domestically built "Mavic-class" quadcopters, marking a deliberate break from dependence on DJI and a shift toward a sovereign, war-hardened small-UAS ecosystem. Forged by two years of attrition and relentless electronic warfare, these pocketable scouts are engineered to keep flying through jamming, spoofing, and geofencing that often cripples consumer drones at the worst moment. Kyiv is prioritizing volume and survivability together, pairing local production lines with frontline feedback to trade showroom polish for hardened links, modular payloads, and visual navigation when GPS disappears. **#Ukraine #Sovereignty**

Sources: [Forbes](#), [Army Recognition](#)     



Northrop's 'card-sized' EW tech turns drones and robots into jamming machines



Northrop Grumman's latest electronic warfare (EW) solution helps platforms find and disrupt radio-frequency emitters, and it's reportedly smaller than a business card. Called Tactical Edge Electromagnetic Solutions (TEEMS), the compact EW payload can be mounted on robots, unmanned surface vessels, and even drones. Once mounted, the platforms turn into mobile EW systems that can both detect and deny hostile signals across the battlespace. TEEMS converts unmanned platforms into agile EW nodes, coordinating wideband jamming and emitter neutralization remotely via Tactical Assault Kit. **#NorthropGrumman #TEEMS**

Source: [NextGenDefense](#)     



Fokker Services to debut civil aircraft anti-jamming system in early 2026

Fokker Services is preparing to launch a full-spectrum anti-jamming and anti-spoofing system for civil aircraft from January 2026. The system is designed to actively defend navigation and avionics from satellite-signal interference, offering a modification kit that integrates seamlessly without additional pilot training and is especially relevant in regions with frequent GPS disruption such as the Middle East and Eastern Europe. The Dutch aerospace company noted that the technology will be available for Boeing 737s, including Max variants, as well as the 747-400 and 747-8 models. Further applications for other narrowbody and widebody aircraft are under consideration. **#Fokker #AntiJamming**

Sources: [Flight Global](#), [Airport Technology](#)     



U.S. firm's new weapon autonomously conducts precision strikes, offers electronic warfare power

A Texas-based defense giant has unveiled Damocles-launched effect, a modular, air or ground-delivered system that can conduct multiple types of missions. Textron Systems' Damocles launched effect allows the integration of various payloads to support different Concepts of Operations (CONOPS), such as electronic warfare effects. Equipped with advanced GEN2 Explosively Formed Penetrator (EFP), the new weapon system can penetrate and defeat a modern battle tank that has protection systems and reactive armor. **#CONOPS #Damocles**

Source: [Interesting Engineering](#)     



SDR signals intelligence for hackers: getting started with anti-drone warfare

The article promotes using software-defined radios (SDR) for signals intelligence and anti-drone operations, emphasizing techniques such as GPS/GNSS spoofing, electronic support measures (ESM) and jamming linked to UAV defence. It offers an introduction to how cyber-warfare practitioners can leverage SDR platforms for drone detection, tracking and neutralization. **#SDR #SIGINT**

Source: [Hackers Arise](#)     

MARITIME

EA-18G jets on USS Abraham Lincoln nuclear carrier signal new U.S. electronic warfare phase

New U.S. Navy photographs from the USS Abraham Lincoln (CVN 72) reveal EA-18G Growlers from VAQ-133 operating with a mixed loadout of legacy AN/ALQ-99 pods and the new AN/ALQ-249 Next Generation Jammer Mid-Band (NGJ-MB), signaling a tangible step in the U.S. Navy's transition to its next era of carrier-based electronic warfare. While officially described as standard Indo-Pacific activities, the deployment offers a direct look at how the Navy is integrating new airborne electronic attack capabilities into frontline units at a moment of heightened global competition and growing focus on contested electromagnetic environments. **#USNavy #EA-18G**

Source: [Army Recognition](#)



LAND

Both the Australian and New Zealand armies seem likely to acquire the Terrestrial Layer System backpack electronic warfare apparatus

The TLS backpack is equipping the U.S. Army. Three TLS capabilities are being developed: Stryker Brigade Combat Teams (BCT) will receive the TLS-BCT platform. TLS-BCT systems will be produced in two sub-variants: One will be restricted to Signals Intelligence (SIGINT) collection and processing. The other will also have cyber/electronic attack capabilities. TLS backpack systems destined for the Australian and New Zealand armies will likely equip the respective EW formations of these forces. **#Capability #TLSBackpack**

Source: [Armada International](#)     





TECHNOLOGY

LAND

Ukrainian specialists positively evaluate Ai-Petri EW complex for enhanced defense

Ukrainian specialists have provided a positive preliminary evaluation of the "Ai-Petri" electronic warfare (EW) complex, noting its potential to enhance defensive capabilities. This assessment highlights the system's features and its intended role in countering reconnaissance efforts and protecting critical infrastructure from aerial threats. The "Ai-Petri" system is designed to disrupt enemy reconnaissance operations and defend vital assets against attack drones, such as those of the Shahed type, by jamming their navigation systems in proximate areas. The initial review underscores its strategic importance in modern conflict zones, particularly in mitigating threats from unmanned aerial vehicles. According to Serhiy Beskrestnov, an expert in radio electronics and communication systems, the "Ai-Petri" system features "broadband antennas, wide-range interference modules, substantial output power, and remote-control capabilities."

#Ai-Petri #AntiDrone

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



SPACE

The race to defend satellites from cyberattacks

A small satellite named Deloitte-1 is hunting for hackers in orbit. Launched in March, it's the first of nine spacecraft the consulting firm Deloitte expects to be operating over the next 18 months to demonstrate a technology to detect cyber intrusions targeted at satellites in space. The company is building these satellites to prove that defending space networks from cyberattack requires putting defenses in orbit and not just on the ground. Deloitte's move comes amid a broader rethink of how to protect space infrastructure from cyber-threats. #Deloitte #SilentShield

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



Scientists reveal it is possible to beam up quantum signals

Quantum satellites currently beam entangled particles of light from space down to different ground stations for ultra-secure communications. New research shows it is also possible to send these signals upward, from Earth to a satellite; something once thought unfeasible. This breakthrough overcomes significant barriers to current quantum satellite communications. Ground station transmitters can access more power, are easier to maintain and could generate far stronger signals, enabling future quantum computer networks using satellite relays. #Quantum #Study

Sources: [Scientific Inquirer](#), [Scienmag](#) EW UV ISR AI QT



DHS wants satellite volunteers to test new cyber tools

The Department of Homeland Security (DHS) and Aerospace Corp. want satellite operators to volunteer to test out new tools they're building to detect cyberattacks on spacecraft, officials said at CyberSat conference. As part of its mission to protect critical infrastructure, DHS is working to develop cyber resilience tools for satellites that provide vital resources including position, navigation and timing (PNT) services like GPS, as well as communication channels like phone and internet. #DHS #CyberTools

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



SandboxAQ, Defense Innovation Unit advance quantum navigation for GPS-denied operations

SandboxAQ has entered an agreement with the Defense Department's Defense Innovation Unit (DIU) to join its Transition of Quantum Sensing (TQS) program, focusing on developing and testing advanced magnetic anomaly navigation technologies for the U.S. military's autonomous systems. The program accelerates the adoption of commercial quantum sensing technologies to ensure PNT resilience in environments where GNSS signals are unreliable or denied.

#TQSProgram #Agreement

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



CYBER

Thales launches its post-quantum MISTRAL encryptor, ready to secure sensitive communications across Europe

At the European Cyber Week, held in Rennes (France), Thales announced the launch of the MISTRAL post-quantum encryptor, a cutting-edge security solution designed to protect communications classified as Restricted against the emerging threats posed by quantum computing. The MISTRAL encryptor is intended for public administrations, operators of vital importance, and companies within the defense technological and industrial base. Fully aligned with ANSSI recommendations and certified to Common Criteria EAL4+, MISTRAL offers a certified and qualified level of security for Restricted-level communications. It is ready for deployment in European projects requiring a high degree of data protection between industrial partners and high-technology stakeholders. #MISTRAL #Quantum

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





MARKET & COMPETITION

AIR

Maximus to enhance Air Force cybersecurity capabilities under \$86m contract

Maximus has secured an \$86m Joint Cyber Command and Control Readiness contract from the U.S. Air Force Life Cycle Management Center's Cryptologic and Cyber Systems Division for advanced capabilities and support services. The company said it will lead engineering analysis, software modification, maintenance, enhancement and maturation of existing architecture and infrastructure. The JCC2 Readiness program enables rapid capability development and operational readiness by applying industry best practices and through the use of innovative technologies. The initiative aims to ensure that the Joint Cyber Command and Control system meets operational requirements while efficiently maturing existing government-owned software. **#JCC2 #Contract**

Source: [Executive Biz](#)     



L3Harris exec says Greece close to decision for electronic warfare package on F-16 upgrade



A senior L3Harris executive has said that Greece will soon decide on a new electronic warfare (EW) suite to equip a fleet of upgraded F-16 fourth-generation fighter jets. Athens requested "pricing" from industry related to the acquisition around 18 months ago, but "we think that decision [product selection] will come fairly quickly," David Nyikos, director of international EW programs for airborne combat systems at L3Harris, said that L3Harris sees Greece as the "next likely collaborator" of the company's Viper Shield AN/ALQ-254 solution, a dual package that combines a radar warning receiver and an electronic countermeasure designed for F-16 Block 70/72 or F-16V international customers. **#Greece #F-16**

Source: [Breaking Defense](#)     



L3Harris F-16 EW system cleared for low-rate production, company says


L3Harris' electronic warfare system for the F-16 fighter has been approved by the US Air Force to begin low-rate production, the company revealed, teeing up first deliveries of the system by the end of next year. Travis Ruhl, the company's lead for Viper Shield, told Breaking Defense on the sidelines of the Dubai Airshow that the EW suite recently cleared what's known as production readiness review, transitioning the program into low-rate production. Next the company plans to ramp up to full-rate production by the first quarter of next year. **#L3-Harris #F-16**

Source: [Breaking Defense](#)     



Frequency Electronics, Inc. announces contract increase for approximately \$5m

FEI-Zyfer, Inc., a wholly-owned subsidiary of Frequency Electronics, Inc. announced the receipt of two follow-on change orders with a combined value of approximately \$4.75m for on-going work on the development and manufacture of a customized version of our high-precision airborne time, synchronization, and frequency distribution systems, with deliveries scheduled through 2027. The system will support collaborative airborne operations and cooperative engagement scenarios for Joint Airborne SIGINT Architecture (JASA) Time, Frequency, Navigation and Geodesy (TFNG) and Airborne Overhead Cooperative Operations (AOCA) COMINT JICD requirements. **#FrequencyElectronics #Contract**

Source: [The Manila Times](#)     



MARITIME

Navy awards deal for holistic cyber supply chain monitoring of airborne systems

Naval Air Systems Command has given Fortress Government Solutions a \$95m contract to implement a new software platform able to provide continuous monitoring of the service's supply chain. Under the five-year indefinite delivery/indefinite quantity (IDIQ) contract, Fortress will deliver a suite of cyber supply chain risk management (C-SCRM) capabilities — including software, analytics, reporting tools and additional integration services. The platform will provide NAVAIR with detailed insights into its massive supplier base and alert program offices about potential risks, according to Don Archer, president of the company. **#C-SCRM #Contract**

Source: [Defensescoop](#)     



Strategic partnership between CNN MCO, Thales and CS Group to modernize three amphibious helicopter carriers of the French Navy

The French Navy's Fleet Support Service (SSF) is leading this initiative to upgrade navigation systems on the PHA-type amphibious helicopter carriers and has tasked CNN MCO as its fleet support contract holder with completing the work. Awarded in 2022 for a period of eight years, CNN MCO's contract covers all onboard systems on the three PHA vessels: Mistral, Tonnerre, and Dixmude. It also includes in-service support of the Somme BCR-type command and underway replenishment vessel. The objective is to ensure the availability at sea and full operational capability of these platforms in an increasingly demanding strategic environment. To address the progressive obsolescence of certain critical systems, the contract includes more than 40 modernization studies. **#FrenchNavy #Partnership**

Sources: [EDR](#), [Zone Militaire](#)     





MARKET & COMPETITION

LAND

FleetRF secures Indian Army tender for indigenous anti-jamming drone communication system

FleetRF, a Delhi-based defense technology start-up, has achieved a major milestone by securing a significant tender from the Indian Army to supply an entirely indigenous drone communication system. The system has been engineered to provide uninterrupted connectivity for unmanned aerial vehicles, even in contested Electronic Warfare (EW) environments where adversaries attempt to jam or spoof signals. Developed over six years of intensive research and development, the communication suite represents a fully in-house innovation. Every layer—from hardware design to embedded software—was conceived, built, and refined by FleetRF's engineering team in India. **#IndianArmy #Tender**

Source: [Indian Defence News](#) (EW) (UV) (ISR) (AI) (QT)



★ CACI secures \$79m U.S. Army task order for electronic warfare support

CACI International Inc announced that it has been awarded a three-year task order valued at up to \$79m to continue its work ensuring decision dominance for the U.S. Army Combat Capabilities Development Command (DEVCOM) Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance and Reconnaissance (C5ISR) Center.

#DEVCOM #Contract

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



China's investment spree in UK gave it access to military-grade technology

China has financed tens of billions of pounds' worth of investment in UK businesses and projects this century, some of which gave it access to military-grade technology, BBC Panorama has learned. The spending spree - worth £45bn (\$59bn) at 2023 prices - was at its height following a 2015 Chinese state directive, aimed at making the country a global leader in high-tech industries. The UK has been the top destination among G7 nations for these investments, relative to the size of its population and economy, according to US-based research group AidData. BBC Panorama has investigated how this led to cutting-edge technology and skills being transferred to China. The UK was "far too free in allowing access to strategically important industries", according to a former head of GCHQ. **#China #Investments**

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



SPACE

DIPS in space: cybersecurity for satellites

The DIPS in Space project, led by FORCE Technology with partners including DTU, the Alexandra Institute and commercial sat-provider GomSpace, will integrate an onboard intrusion-detection and prevention system in GomSpace's platform. Using datasets from the satellite, the project aims to train edge-AI models to identify cyber-anomalies, validate threat models and protect the satellite's service operation in orbit. **#DIPS #Project**

Source: [Digital Research Center Denmark](#) (EW) (UV) (ISR) (AI) (QT)



★ UAE Space Center, Thales Alenia Space partner on LEO-PNT navigation system

The National Space Science and Technology Center (NSSTC) and Thales Alenia Space are cooperating to explore opportunities in low-Earth orbit (LEO) space navigation systems. The collaboration reflects a vision to explore pathways that can enhance the robustness and sovereignty of future navigation services while deepening international cooperation and knowledge exchange between the United Arab Emirates and Europe in the field of space technology.

#UAESpaceCenter #Cooperation

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



Cracking the code for resilient, secure space-based communications

L3Harris has achieved NSA Cybersecurity Directorate certification for its KSV-650 space hub end cryptographic unit, ensuring secure, adaptable communications for military operations. Certification is required in order for operation of the unit's on-orbit reprogrammability, which protects against emerging cyber-threats, providing resilient and reliable SATCOM services to the warfighter that safeguard national security and ensure secure connectivity for mission-critical operations.

#L3Harris #NSACybersecurity

Source: [L3Harris](#) (EW) (UV) (ISR) (AI) (QT)



ICEYE sees role as Europe's defense space-intelligence linchpin

Finland's ICEYE has a "very big role to play" in giving Europe sovereign access to satellite intelligence, without having to rely on the United States, the company's Vice President for Missions Joost Elstak said. European interest in ICEYE rose after Russia invaded Ukraine in 2022. But it was the U.S. halting intelligence sharing with Ukraine in March 2025 that really underscored the need for sovereign access to space-based intel, Elstak told Defense News. Space-based intelligence, surveillance and reconnaissance, or ISR, was seen as the toughest area for Europe to achieve self-sufficiency, according to a Defense News survey in February. Most of the surveyed defense experts estimated Europe would need five to 10 years to build sufficient capacity to no longer rely on U.S. space intel. **#ICEYE #Sovereignty**

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





MARKET & COMPETITION

CYBER

Port San Antonio offers to build Air Force cyber campus for \$1bn less

Port San Antonio CEO Jim Perschbach says the port can build an Air Force consolidated cyber and electronic-warfare campus in four to six years for more than \$1bn less than the U.S. government could under normal circumstances. Speaking Nov. 18 at the Texas Association of Business Summit, Perschbach proposed a single new campus to bring together critical Air Force missions scattered across aging facilities. He said only the port's public-yet-commercial model can beat the normal 15-year, \$2bn-plus federal timeline, delivering the same project in four to six years for more than \$1bn less. Port San Antonio currently generates \$20bn in annual economic output. **#USAF #PortSanAntonio**



Source: [Biz Journals](#)     

THREAT INTELLIGENCE

AIR

Radars, satellites, GPS... Understanding the new electronic warfare

They are poetically called "wave trackers," even though their mission is anything but lyrical and instead fundamentally strategic. These service members specialize in intercepting and analyzing electromagnetic signals and are on the front line of what is known as electronic warfare, or "warfare in the electromagnetic domain" (EMD). Dominance of the electromagnetic spectrum (radio, radar, satellites, communications, GPS) on a battlefield where all systems are interconnected has become a decisive factor in achieving superiority on the ground. **#EMD #ContestedSpectrum**

Source: [Le Point](#)     

CISA tells critical infrastructure to 'be air aware' as drone threats surge

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has issued new guidance warning critical infrastructure operators to brace for rising drone threats and urging them to treat low-altitude airspace as an active attack surface. CISA's message is clear: UAS threats are no longer hypothetical. The agency describes drone activity as a growing component of the physical-security landscape for critical infrastructure sectors, including military bases, which it says are "subject and frequent, and often unidentified, UAS incursions." The agency emphasizes that its new guidance is intended to help operators "be air aware" by building a continuous posture of situational awareness around facility airspace, rather than treating drones as an occasional or peripheral concern. **#CISA #DroneThreats**



Sources: [Resilience Media](#), [CISA](#)     

Ukraine is jamming Russia's 'superweapon' with a song

The Ukrainian Army is knocking a once-hyped Russian superweapon out of the sky by jamming it with a song and tricking it into thinking it's in Lima, Peru. The Kremlin once called its Kh-47M2 Kinzhal ballistic missiles "invincible." Joe Biden said the missile was "almost impossible to stop." Now Ukrainian electronic warfare experts say they can counter the Kinzhal with some music and a re-direction order. As winter begins in Ukraine, Russia has ramped up attacks on power and water infrastructure using the hypersonic Kinzhal missile. Russia has come to rely on massive long-range barrages that include drones and missiles. An overnight attack in early October included 496 drones and 53 missiles, including the Kinzhal. Another attack at the end of October involved more than 700 mixed missiles and drones, according to the Ukrainian Air Force. **#UkrainianAirForce #Jamming**



Source: [404 Media](#)     

Indian government confirms cyberattack on Indian airports involving GPS spoofing

The central government has officially confirmed that seven major airports across India were targeted by cyber attacks involving GPS spoofing, raising concerns about vulnerabilities in the country's aviation infrastructure. Union Civil Aviation Minister Ram Mohan Naidu Kinjarapu informed Parliament that flights approaching Indira Gandhi International (IGI) Airport in Delhi reported GPS spoofing while using satellite-based landing procedures at Runway 10. Similar incidents were noted at other key airports, including Mumbai, Kolkata, Hyderabad, and Bengaluru. **#India #Spoofing**



Source: [Newsfirst Prime](#)     

MARITIME

China's military denies electronic jamming caused US Navy air crashes

China's military denied accusations that it used electronic jamming to cause two recent U.S. Navy air crashes in the South China Sea, calling the claims "conspiracy theories." State broadcaster CCTV reported that the People's Liberation Army (PLA) rejected any involvement in the October 26 incidents, when a U.S. Navy MH-60R Seahawk helicopter and an F/A-18F Super Hornet crashed within 30 minutes of each other near the USS Nimitz. **#PLA #Jamming**



Source: [Tipp insights](#)     



THREAT INTELLIGENCE

MARITIME

Maritime cybersecurity: vulnerabilities in naval systems, AIS spoofing, and GPS spoofing

The digitalization of the maritime sector has created a troubling paradox: while modern vessels navigate with millimetric precision thanks to GPS, ECDIS, and satellite communications, this very interconnection has made them vulnerable to threats that system designers twenty years ago could not have imagined. The maritime industry carries more than 80 percent of global trade, yet its digital infrastructure exhibits systemic vulnerabilities that challenge traditional cybersecurity paradigms. Maritime cybersecurity is no longer a theoretical topic for academic conferences but an operational reality that intersects international law, national security, and the continuity of global trade. **#GlobalTrade #AIS**

Source: [ICT Security](#)     

Russian spy ship jams Royal Navy GPS in North of Scotland

A Russian spy ship operating in waters north of Scotland has attempted to jam the GPS systems of a Royal Navy frigate while simultaneously targeting RAF pilots with military-grade lasers, Defense Secretary John Healey has revealed. The research vessel Yantar, operated by Russia's secretive deep-sea research unit GUGI, has been spotted lurking on the edge of British waters for several weeks. This marks the second time this year that the Yantar has deployed to UK waters, raising serious concerns about Russian intentions. **#SpyShip #Jamming**

Source: [Brit Brief](#)     



LAND

Russian hackers and EW forces can disable Ukraine's communication systems

Russian cybersecurity and electronic warfare specialists are capable of disabling modern communication systems used by the Ukrainian army, said retired Colonel Mikhail Timoshenko in an interview with NEWS.ru. He noted that if such cyber and EW operations succeed, Ukrainian forces could be forced to revert to outdated technologies. According to him, in that case the enemy would have to rely on wired field phones, the same type used since the First World War. He explained that Ukraine still possesses stocks of these devices left from Soviet times, and they are occasionally used even today. Russian troops, he added, also carry them as a safeguard against powerful enemy electronic interference, since such equipment cannot be jammed. **#Jamming #SecureCommunications**

Source: [Military Affairs](#)     



SPACE

Germany detects an increase in Russian attempts to intercept signals from satellites

Germany's military intelligence has confirmed a surge in hostile Russian activity in orbit, including satellite jamming, close-approach maneuvers, and attempts to monitor Ukrainian troops training on German soil, according to a joint investigation by WDR, NDR, Süddeutsche Zeitung, and Tagesschau on November 18. "We are under threat. Russia has the capability to seriously disrupt us in space," said Maj. Gen. Michael Traut, head of Germany's Space Command. **#Germany #Awareness**

Sources: [Tagesschau](#), [United42 Media](#)     



Securing Europe's defense future through the European protected waveform and multi-orbit networks

According to Koen Willems, vice president of EU Programs and Government Relations at ST Engineering iDirect Europe, secure satellite communications form the invisible backbone of modern defense operations. Yet these systems are facing mounting challenges. From cyberattacks and jamming to eavesdropping and the complexities of hybrid warfare, the threats are growing more sophisticated and persistent. **#SATCOM #Awareness**

Source: [Via Satellite](#)     



Space, the new cyber frontier of all dangers: exposing the vulnerability of satellite communications

French defense journalist and analyst Murielle Delaporte highlights how space has become the new front line in cyber conflict. Satellite communications—representing only 1–3% of global volume—have emerged as critical yet highly vulnerable infrastructure. Their strategic importance for defense, security, and remote regions makes them prime targets amid the rise of hybrid threats and information warfare. As with submarine cables in the past, satellites now stand at the core of digital sovereignty challenges. **#DataLeaks #CriticalInfra**

Sources: [Operationnels](#), [Murielle Delaporte](#)     





THREAT INTELLIGENCE

SPACE



China simulates jamming Starlink over Taiwan, mission to require over 1,000 drones

Instead of focusing on whether Starlink can be jammed in theory, Chinese military planners are increasingly concerned with how such a feat could be attempted in a real conflict over Taiwan. The challenge is staggering: Taiwan and its allies could rely on a constellation of more than 10,000 satellites that hop frequencies, reroute traffic and resist interference in real time. However, a recent simulation study by Chinese researchers delivers the most detailed public attempt yet to model a potential countermeasure. It concludes that disrupting Starlink across an area comparable to Taiwan is technically achievable – but only with a massive electronic warfare (EW) force. **#Starlink #Jamming**



Sources: [Interesting Engineering](#), [South China Morning Post](#) **EW** **UV** **ISR** **AI** **QT**

Multi-orbit networks expand the attack surface while basic cyber-threats persist

Software-defined satellites and multi-orbit architecture open up an expanded attack surface for hackers, but those vulnerabilities remain largely theoretical for now, satellite cyber and engineering experts said during CyberSat. The real and present dangers lie in more low-hanging fruit, they said. Five years ago, a presentation by James Pavur at the Black Hat cybersecurity conference sent shockwaves through the satellite industry. “Five years later, we’re doing the exact same thing, not encrypting the downlink,” added Brandon Bailey, a cybersecurity expert. **#Awareness #Vulnerabilities**



Source: [Via Satellite](#) **EW** **UV** **ISR** **AI** **QT**

Slingshot spots uncataloged Russian sat in MEO

A Russian sat spent five weeks in MEO without the U.S. public SDA database knowing its whereabouts. Slingshot Aerospace found it after just a few hours of looking. The achievement highlights how adept SDA companies have become at finding uncataloged things in orbit. **#SDA #MEO**



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

CYBER

Is the UK's defense ready for rising electronic warfare threats?

The U.K. is falling behind leading nations in electronic warfare, according to new POST research, which highlights growing dependence on the electromagnetic spectrum and rising threats demonstrated in Ukraine, where EW has driven major drone losses and rapid counter-innovation. UK critical infrastructure remains vulnerable, while national EW efforts suffer from fragmented structures, STEM skills shortages, procurement rigidity, and restrictive spectrum-testing rules. The 2025 Strategic Defence Review plans a new CyberEM Command, but implementation and capability gaps persist. **#UK #Opinion**



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



Cyber defense: companies urged to mobilize against high-intensity threats

To prepare for a potential conflict, large-scale readiness depends on strengthened collaboration with innovative companies, stated Air Division General Emmanuel Naëgelen, Commander of Cyber Defense, during the European Cyber Week (ECW) in Rennes. Moreover, the key stakeholders involved in cybersecurity, cyber defense, and defense AI reiterated the importance of a nationally driven cyber effort with a strong European dimension. **#Readiness #Awareness**



Source: [La Tribune](#) **EW** **UV** **ISR** **AI** **QT**

NVISO analyzes VShell post-exploitation tool

VShell, a Chinese-language intrusion tool, has increasingly been sighted over the last year, primarily used for long-term espionage activities has actively been tracking VShell infrastructure for months and notified affected victims worldwide with outstanding support from Team Cymru. Its report exposes how VShell works, which actors use it, and why it poses a cyber threat. With this, NVISO highlights the importance of proactive defensive measures against VShell, urging organizations to deploy network and endpoint detection strategies, strengthen vulnerability management, and enhance threat intelligence-informed detection capabilities. **#VShell #Report**



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

TRAINING & EDUCATION

AIR

Safety meets security: building cyber-resilient systems for aerospace and defense

Patrick Miller from Lynx, has spent his career at the intersection of safety, security, and performance, working across aerospace, defense, enterprise cloud, and embedded systems. In this Q&A, he shares how architecture, separation, and long-term thinking can help engineers and product teams design resilient weapons systems. **#Resilience #Podcast**



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





TRAINING & EDUCATION

AIR

India and network-centric warfare: The importance of cyber, electronic warfare and space technologies

This book analyses India's Network-Centric Warfare (NCW) capabilities and how well they are integrated into the Indian armed forces, especially the Indian Army. It explores primarily the technological and to a more limited extent the doctrinal and organizational issues that are related to NCW. It assesses how three technologies that are central to NCW – cyber, electronic warfare, and space – are being developed and integrated by the Indian armed services. In addition, it also analyses partially how the Indian armed services acquire and integrate Artificial Intelligence and Quantum Technology in specific areas and also explores the need for the Indian armed services to acquire Kinetic Energy Weapons (KEWs) and Directed Energy Weapons (DEWs), especially microwave and laser weapons. **#IndianArmy #Book**

Source: [Routledge](#)     



MARITIME

U.S. Coast Guard mandates cybersecurity training for personnel with IT, OT access by January 2026

The U.S. Coast Guard issued a policy letter outlining new cybersecurity training requirements for personnel with access to IT or OT (operational technology) systems. Aligned with recent regulations, the policy is part of broader efforts to enhance cybersecurity within the Marine Transportation System. It also mandates that personnel on U.S.-flagged vessels, facilities, and Outer Continental Shelf (OCS) facilities subject to the Maritime Transportation Security Act (MTSA) of 2002 complete the required cybersecurity training by Jan. 12, 2026. **#USCoastGuard #Training**

Source: [Industrial Cyber](#)     



LAND

Chief of the EW Directorate of the Armed Forces of Ukraine Ivan Pavlenko: "The more we interfere with a Shahed, the more we interfere with your phones"

In this interview, Colonel Ivan Pavlenko, Chief of the Electronic Warfare and Cyber Warfare Directorate of the Armed Forces of Ukraine, explains that Ukrainian EW units, research institutions and domestic manufacturers are fighting an uneven technological battle against DJI's large anti-jamming industry. He notes that EW effects are invisible but widespread, influencing both frontline soldiers and civilians during air-raid alerts, and stresses that EW is not a cure-all but one of the tools that help improve survivability. He also emphasizes that Ukrainian EW capabilities currently surpass those of several Western partners and outlines the growing role of the electromagnetic spectrum and cyberspace as strike drones have become more common than traditional infantry or mechanized assaults. **#Doctrine #Interview**

Source: [Novynarnia](#)     



U.S. 2nd BCT 1st Cavalry Division completes first heavy-force training with drones and electronic warfare systems.

According to information published on the X account of the U.S. Army's 1st Cavalry Division on November 24, its 2nd Brigade Combat Team completed the first heavy force training event guided by the Transforming in Contact framework at the National Training Center in Fort Irwin, California. The division stated that the brigade used advanced aerial drones, electronic warfare systems, and restructured formations to accelerate maneuver and increase lethality against a near-peer enemy force inside a live combat simulation. **#USArmy #Exercise**

Source: [Army Recognition](#)     



SPACE

Low-altitude UAV friendly-jamming for satellite-maritime communications via generative AI-enabled deep reinforcement learning

This research presents a system in which low-altitude unmanned aerial vehicles (UAVs) provide "friendly" jamming to secure satellite-maritime communications by improving physical-layer secrecy. The authors formulate a multi-objective optimization problem balancing secrecy rate and UAV energy consumption, convert it into a Markov decision process, and propose a transformer-enhanced soft actor-critic (TransSAC) algorithm to solve it. Simulation results indicate TransSAC outperforms comparative methods, achieving higher secrecy rates and lower energy consumption in maritime satellite links. **#AI #Paper**

Source: [Cornell University](#)     



Brno reaches for space: local innovators showcase Czech space excellence

The Brno region has become one of Europe's most dynamic tech hubs, uniting leading players across the local ecosystem. This collaborative platform is now taking Czech space excellence to the international stage at Space Tech Expo Europe in Bremen. TRL Space, Zaitra, and Groundcom will, for example, unveil new products. **#Brno #SpaceTechExpo**

Source: [The AI Journal](#)     





TRAINING & EDUCATION

SPACE



Europe hosts first-ever multi-satellite cybersecurity challenge

Europe has completed its first in-orbit cybersecurity competition, marking a new step in space defense collaboration. The CTRL+Space Capture-the-Flag (CTF) challenge, held in the Netherlands, was also the world's first live event involving multiple satellites. Organized by D-Orbit and ethical hacking group mhackeroni, with backing from the ESA Security Cyber Centre of Excellence and ESA Security Office, the event aimed to strengthen Europe's ability to protect spacecraft from cyber threats. D-Orbit confirmed the competition's completion on 6 November. CyberInflight was represented at this conference by its CEO, Florent Rizzo. **#CTF #3SConference**

Sources: [Orbital Today](#), [Via Satellite](#), [CyberInflight](#)     



CYBER

Pentagon releases 'revised' plan to boost cyber talent, 'domain mastery'

The Defense Department has released a highly anticipated plan to attract and retain cyber talent by better integrating U.S. Cyber Command with other military departments for recruitment and training, and establishing three new organizations to improve the military's hacking and defensive prowess. **#CompassCall #Tool**

Source: [Breaking Defense](#), [Military Embedded Systems](#)     



Golden Gate Chapter brings EW expertise to CMU Silicon Valley

On November 12, AOC Golden Gate Chapter Ragan Wilkinson, along with long-time member Bob Simmen, delivered an engaging presentation at Carnegie Mellon University Silicon Valley. The comprehensive session explored the history and future of electromagnetic warfare. The presentation examined current EW applications in contemporary conflicts, including operations in Ukraine, Iran, and Gaza. Looking ahead, Wilkinson and Simmen outlined emerging trends shaping the future of EW, with particular emphasis on the integration of artificial intelligence, space-based systems, and cyber warfare capabilities. **#EmergingTrends #Conference**

Source: [The Journal of Electromagnetic Dominance](#)     



Podcast: the vulnerable state of global navigation satellite systems

In this episode, PolicyTracker journalist Camilla Mina discusses the critical role of global navigation satellite systems (GNSS) with expert Logan Scott. They explore the importance of timing in navigation and the threat posed by the increase in spoofing and jamming in recent years. **#GNSS #Podcast**

Source: [Policy Tracker](#)     



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