



# DEFENSE MONTHLY WATCH

September 1 – 30, 2025

**Number of articles identified:** 90

- # in **Geopolitics**: 16
- # in **Technology**: 19
- # in **Market**: 24
- # in **Regulation**: 9
- # in **Threat intelligence**: 15
- # in **Training & Education**: 7

**Tags and themes**

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

Recent developments across the global defense landscape reveal an intensifying drive toward technological innovation and strategic resilience. In the geopolitical arena, the **U.S. has signaled a doctrinal shift with Defense Secretary Pete Hegseth's speech**, renaming the Department of Defense as the Department of War and emphasizing heightened readiness. **NATO continues to strengthen its operational capabilities through exercises like Dynamic Guard**, which tested electronic warfare and missile defense under degraded communications. **Meanwhile, Germany's €35 bn investment in space defense** reflects the increasing strategic importance of securing orbital assets amid competition with Russia and China.

The defense market is experiencing significant modernization and procurement activity. The **U.S. Army has accelerated investments** in radar, counter-UAS, and electronic warfare systems through contracts with Raytheon and Parsons Corporation, complemented by the upcoming RAPTER initiative for next-generation EW solutions. **India is expanding its domestic defense industrial base** with a \$7.5 billion Tejas Mk1A fighter contract and the development of portable drone jammers, while U.S. Navy contracts to Raytheon and L3Harris Technologies reinforce shipborne weapons and advanced communications capabilities. In the space sector, Viasat has been selected to deliver a next-generation cryptographic solution for the U.S. Space Force's Space Systems Command, strengthening satellite security and data protection against evolving cyber threats.

Regulatory frameworks are evolving, **Germany plans to authorize its military to neutralize hostile drones**, addressing a spectrum of hybrid threats ranging from small commercial UAVs to coordinated swarms. In the U.S., **NASA has been reclassified as an intelligence and security agency**, reflecting a fusion of space exploration and national security priorities. Simultaneously, the Department of War has implemented the **Cybersecurity Risk Management Construct (CSRMC)**, a five-phase framework designed to deliver real-time cyber defense across air, land, sea, space, and cyberspace, institutionalizing resilience as a core operational principle.

Regarding technological news, **Thales unveiled its DCM5 cryptographic platform**, which delivers sovereign, quantum-ready security for multinational coalitions, ensuring secure communications while maintaining backward compatibility with legacy systems. The Pentagon is investing in **non-space-based alternatives to GPS using quantum-based positioning systems** to counter signal jamming. In France, the **SERVAL armored vehicle now integrates tactical SIGINT systems**, expanding battlefield intelligence and operational flexibility.

Regarding the threat intel front, the **Netherlands has deployed cyber operators to frontline positions through the 101 CEMA Battalion**, while Russia's GPS jamming increasingly affects European aircraft and navigation systems. In space, **U.S., French, and German officials warn of aggressive activities by China and Russia**, including satellite jamming, laser dazzling, and cyber intrusions. Concurrently, Chinese state-aligned APT groups have intensified cyber operations targeting Taiwan's semiconductor industry, Philippine military networks, and U.S. defense contractors, exploiting advanced malware and zero-day vulnerabilities.

# GEOPOLITICS

## AIR

### China's military parades into the cognitive era, showing how it's arming for future wars

During its 17th National Military Parade, China showcased a new generation of AI-driven drones, electronic warfare platforms, and counter-UAS systems, reflecting its ambition to dominate the electromagnetic spectrum. The event also marked the debut of the Information Operations Group (IOG), a dedicated unit integrating cyber, EW, and cognitive warfare under a unified command structure. **#Parade #CognitiveWarfare**

**Sources:** [Forbes](#), [Business Insider](#), [Orbital Today](#)     



### The United States must prepare for war: the full speech of Pete Hegseth to the American generals


In a historic speech on September 30, Defense Secretary Pete Hegseth declared the end of the "Department of Defense" era, renaming it the Department of War and signaling a radical change in U.S. military doctrine. The unprecedented gathering of hundreds of generals in Virginia raised both symbolic and security concerns. **#Doctrine #Speech**

**Source:** [Le Grand Continent](#)     



### VOLFA 2025 - L'Armée de l'Air et de l'Espace à l'épreuve de la haute intensité (Trad.: VOLFA 2025 - The French Air and Space Force put to the test of high-intensity warfare)

From September 22 to October 10, the French Air and Space Force is conducting VOLFA 2025, its annual high-intensity air combat training exercise. Presented at a press briefing by Colonel Jean-Christophe, head of the operational training division at CDAOA, the exercise brings together more than 1,000 airmen, around 50 aircraft, and several allied nations to strengthen interoperability and force responsiveness. **#VOLFA2025 #Exercise**

**Source:** [Ministère des Armées](#)     



## MARITIME



### NATO electronic warfare and missile defense skills tested

Standing NATO Maritime Group Two (SNMG2) has concluded Exercise Dynamic Guard off the coast of Turkey, with training centred on electronic warfare (EW) and anti-ship missile defense, NATO stated. The objective was to give Allied forces realistic training in a contested electronic environment, including scenarios where communications and sensors were degraded or denied. The NATO Joint Electronic Warfare Core Staff (JEWCS) supported the exercise with advanced systems and specialist expertise, providing up-to-date simulations of adversary threats. **#DynamicGuard #Exercise**

**Source:** [UK Defence Journal](#)     



### China's A2/AD electronic warfare challenge and the US Navy's NGJ response

China's Indo-Pacific strategy relies heavily on Anti-Access/Area Denial (A2/AD), combining missiles, naval and air power with advanced EW, cyber operations, and space denial capabilities to disrupt U.S. communications, GPS, and intelligence networks. This layered system of weapons and doctrines aims to keep adversaries out of contested zones. In response, the U.S. Navy is fielding the Next Generation Jammer (NGJ) on its EA-18G Growler aircraft, a major upgrade over the legacy AN/ALQ-99 pods. The NGJ provides advanced jamming, deception, and suppression of enemy air defenses (SEAD) to counter agile radars and integrated defense systems at the heart of China's A2/AD approach. **#A2/AD #Doctrine**

**Sources:** [The National Interest](#), [The National Interest](#)     



## LAND

### India-U.S. joint military drill 'Yudh Abhyas 2025' begins in Alaska

Military contingents from India and the U.S. engaged in a spectrum of tactical drills, including the integrated use of artillery, aviation and electronic warfare systems, as part of a bilateral exercise in Alaska, beginning September 1, officials said. **#YudhAbhyas2025 #Exercise**

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



### Trump nominee for Joint Chiefs vice chairman vows to tackle electronic warfare challenges

In his recent confirmation hearing, Gen. Chris Mahoney, the nominee for vice chairman of the US Joint Chiefs of Staff, set electronic warfare as one of his top priorities. Ensuring U.S. military systems are resilient to electromagnetic attack is critical for joint force lethality and survivability, Mahoney told lawmakers, noting the need for continued investment and innovation in this area. **#Priorities #Strategy**

**Source:** [Defensescoop](#)     



### India strengthens drone warfare capabilities through large-scale joint exercises

The Indian Armed Forces are intensifying efforts to integrate indigenous drone systems and electronic warfare tactics through major exercises. The Army recently conducted "Vayu Samanvay" to validate homegrown UAS performance in contested EW environments, while the upcoming "Cold Start" exercise will unite Army, Navy, and Air Force units to test drones and counter-drone systems on an unprecedented scale. **#CounterDrones #Exercises**

**Sources:** [Social News XYZ](#), [Dawn](#)     





# GEOPOLITICS

## SPACE

### EU deploys LEO satellites to counter GPS jamming and Russia threats, NATO says it's also working on it after interference with European Commission President's plane

EU Defense Commissioner Andrius Kubilius announced plans to deploy additional satellites in low Earth orbit (LEO) to enhance resilience against interferences. The announcement directly responds to an incident that targeted European Commission President Ursula von der Leyen, who was en route to Bulgaria. Meanwhile, NATO is working "day and night" to counter Russian GPS jamming, Secretary-General Mark Rutte confirmed two days after the incident. **#LEO #Jamming**

Sources: [WPN](#), [Reuters](#), [Time](#)     



### U.S. Space Force to establish electromagnetic warfare operations center and considers doctrinal evolution

U.S. Space Force leaders announced the upcoming establishment of an electromagnetic warfare tactical operations center within the next months. Officials also stressed that partnerships with allied, space-capable nations are vital to sustaining U.S. space dominance. Moreover, the service is weighing a doctrinal shift with a proposal to rename Space Operations Command as Combat Forces Command. **#TacticalOperationsCenter #Doctrine**

Sources: [National Defense Magazine](#), [Dnyuz](#), [Task & Purpose](#)     



### Israel offers space cybersecurity cooperation to South Korea's NIS






The Israeli government recently conveyed to the South Korean National Intelligence Service (NIS) its willingness to cooperate, saying it can share its satellite security know-how with Korea. A security industry official said "as Israel also has issues in preparation in the field of space cybersecurity, it delivered a message that it would like to discuss cooperation with Korea". **#SpaceSecurity #Cooperation**

Source: [Chosun Biz](#)     



### ESA Director General's opening remarks at the General Assembly on Defense, Space & Cybersecurity

Josef Aschbacher made an urgent call to strengthen Europe's space defense capabilities during his opening speech at the General Assembly on Defense, Space and Cybersecurity event held at Esrin, the ESA's Earth Observation Center. Faced with the growing threat from international actors and recent incidents in space, he warned: "Europe is not just lagging behind; we are not even playing the same game". Numerous European echoed his concerns. **#ESA #Resilience**

Sources: [ESA](#), [Via Satellite](#), [Decode 39](#)     



### U.S., France step up joint military satellite moves to counter China in space

France and the U.S. are planning a second joint mission of coordinated satellite maneuvers in orbit, part of a growing push to sharpen allied spying capabilities as China expands its own military footprint in space, a senior U.S. general told Reuters. The operation would be the Pentagon's third known mission conducted in space with an ally following its first-ever joint maneuver with two spacecraft in orbit late last year, also involving France. **#Exercise #Cooperation**

Source: [Reuters](#)     



### Germany pledges €35bn for space defense against Russia, China

Germany's Defense Minister Boris Pistorius warned of escalating space threats, accusing Russia of using satellites to shadow those vital to German military operations, signaling potential orbital conflicts. Amid rising tensions, Germany plans a €35bn (\$41bn) investment in space defenses by 2030 to deter attacks and bolster security. This reflects a broader shift toward contested space domains. **#Germany #Strategy**

Source: [WPN](#)     



## CYBER

### U.S. military branches align on new cyber strategies to strengthen national defense

Across the U.S. armed forces, cybersecurity is increasingly placed at the center of transformation strategies. The U.S. Air Force is developing a new defensive cyber campaign plan to better coordinate its defenders and protect critical infrastructure. In parallel, the Navy Reserve is integrating cyber warfare specialists into the operational level of war, linking strategic capabilities with tactical objectives. The Army also places cyber at the core of its transformation strategy, stressing resilience, AI applications, and closer collaboration with the private sector. Moreover, the head of the National Geospatial-Intelligence Agency added that cyber defenders need AI tools to fend off a new generation of AI-powered attacks. **#USMilitary #CyberStrategy**

Sources: [Breaking Defense](#), [U.S. Navy](#), [Soldier Systems](#), [Defense One](#)     



### CAF CYBERCOM leads the charge in regional cyber defense with Sarajevo training

From September 15 to 19, the Canadian Armed Forces Cyber Command (CAF CYBERCOM) delivered the Military Cyber Security Operations Course (MCSOC) in Sarajevo, Bosnia, and Herzegovina, arming the next generation of cyber defenders with the tools to protect nations and critical infrastructure. The course welcomed participants from eight countries: Bosnia and Herzegovina, Georgia, Kazakhstan, Kosovo, Jordan, Moldova, Tunisia, and Ukraine. **#MCSOC #Courses**

Source: [Government of Canada](#)     



# REGULATION

## AIR

### Germany plans to let military shoot down drones domestically

German Interior Minister Alexander Dobrindt announced plans to overhaul the country's aviation security law to give the armed forces a formal role in drone defense, including the authority to shoot down hostile aircraft. He described the spike in recent drone incursions over Germany and neighboring countries as part of a "constant hybrid threat" ranging from small commercial quadcopters to coordinated swarms. **#DroneIncursions #Law**

Source: [Politico](#)     



## MARITIME

### Industry giants sign MoU at Gastech to address U.S. maritime cyber regulations

Hanwha Systems, Hanwha Ocean and Hanwha Power Systems announced a joint research collaboration with the American Bureau of Shipping (ABS) to address U.S. maritime cybersecurity regulations, including requirements set by the U.S. Coast Guard (USCG) and for U.S.-flagged vessels. **#MoU #Cyber**

Source: [Safety4Sea](#)     



## LAND

### Army Secretary in 'holy war' with Congress over budget flexibility

Army Secretary Daniel Driscoll says he is locked in a "holy war" on Capitol Hill as he works to convince lawmakers to grant the service more flexible funding authority for electronic warfare, unmanned aerial systems and counter-drone efforts. The resistance Driscoll has encountered in his first eight months in the job is part of a longstanding tension between the Pentagon and Congress over the trust and oversight of taxpayer dollars. **#USBudget #Capabilities**

Source: [Defense News](#)     



## SPACE

### New executive order reclassifies NASA as an intelligence and security agency

An Executive Order issued by the Trump Administration declares that NASA and several other U.S. government agencies will now operate primarily as intelligence and security agencies. The Order states that NASA will now "have as a primary function intelligence, counterintelligence, investigative, or national security work." **#Intelligence #ExecutiveOrder**

Source: [The Debrief](#)     



### BSI TR-03184-2 Information Security for Space Systems, Part 2: Ground Segment

The Federal Office for Information Security (BSI) has published the next document for Space Security. The Technical Guideline "BSI TR-03184-2 Information Security for Space Systems, Part 2: Ground Segment" is available in English.

**#BSI #Guideline**

Source: [BSI](#)     



## CYBER

### The EU Commission is working to simplify the EU's cybersecurity rulebook

Executive Vice-President Henna Virkkunen hosted an Implementation Dialogue focused on cybersecurity. The event feeds into the preparation of the Digital Omnibus and the Cybersecurity Act revision – two upcoming legislative initiatives that address cybersecurity issues. **#EU #Rulebook**

Source: [European Commission](#)     



### The cybersecurity information sharing act faces expiration

The Cybersecurity Information Sharing Act (CISA) is designed to provide encouragement and protection for and while sharing threat information. A sunset clause built into the Cybersecurity Information Sharing Act 2015 (PDF) means it will expire at the end of September 2025 unless reauthorized by the US Congress. At the time of writing, it has not been reauthorized. **#InformationSharing #CISA**

Source: [Security Week](#)     



### France strengthens digital risk governance across state information systems

With the publication of a new decree specifying exceptions, the French government completes its regulatory framework launched in 2019. All ministries must now systematically accredit their IT systems' security, with results tracked by indicators and overseen at the highest level of government. **#IT #Framework**

Sources: [ANSSI](#), [Legifrance](#)     



# REGULATION

## CYBER



### U.S. Department of War rolls out CSRMC to deliver real-time cyber defense

The U.S. Department of War (DoW) announced the implementation of a Cybersecurity Risk Management Construct (CSRMC), a transformative framework to deliver real-time cyber defense at operational speed. This five-phase construct ensures that U.S. warfighters maintain technological superiority against rapidly evolving and emerging cyber-threats. By institutionalizing this construct across the Department, the DoW is ensuring cyber survivability and mission assurance in every domain: air, land, sea, space, and cyberspace. **#CSRMC #Framework**

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



# TECHNOLOGY

## AIR

### China and the U.S. advance radar technologies to boost electronic warfare edge

Both China and the U.S. are accelerating radar innovation. In China, a recent test showcased what could be the world's first AI-powered radar for military aircraft, capable of dynamically adjusting frequencies and beam direction to resist jamming and maintain near-perfect target tracking. Meanwhile, the U.S. Air Force is advancing the modernization of its B-52 Stratofortress with the new AN/APQ-188 radar, a key upgrade providing greater precision and electronic warfare capabilities to keep the platform operational through mid-century. **#RadarSystem #SmartSensors**

Sources: [Interesting Engineering](#), [Army Recognition](#)     

### DSEI 2025: Danish RQ-35 Heidrun and Czech-Ukrainian MACE showcase frontline reconnaissance and EW-resilient strike capabilities

At DSEI 2025 exhibition in London, Sky-Watch presented the RQ-35 Heidrun, a fixed-wing unmanned aerial system designed for low-altitude surveillance and reconnaissance missions. It has been employed in combat since 2022 by the Armed Forces of Ukraine, confirming its resilience in contested electromagnetic environments. Meanwhile, the Czech-Ukrainian company UAC presented the MACE unmanned aerial strike system, a loitering munition designed for reconnaissance and precision strike roles. **#RQ-35 #MACE**

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



### L3Harris advances electronic warfare with Viper Shield pod and new C-UxS initiative






L3Harris has introduced a podded variant of its Viper Shield electronic warfare system, offering F-16 operators enhanced flexibility and reduced aircraft downtime compared to the internally integrated configuration. In parallel, the company unveiled a structured Counter-Unmanned Systems (C-UxS) initiative, combining AI and electronic warfare to counter increasingly complex swarms of drones and autonomous platform. **#L3Harris #C-UxS**

Sources: [FlightGlobal](#), [L3Harris](#), [Army Recognition](#)     



### U.S. Air Force accelerates electronic warfare modernization with new waveform and software developments






The U.S. Air Force is intensifying efforts to enhance its electronic warfare capabilities. The Spectrum Warfare Wing has accelerated its cycle for testing and deploying new waveforms, aiming to outpace adversaries in the ever-evolving electromagnetic battlespace. In parallel, Terma and the Georgia Tech Research Institute (GTRI) have successfully completed the Critical Design Review (CDR) of the Air Force's Modular Software program, a key milestone confirming the system's robust design and paving the way for full system integration. **#USAF #Developments**

Sources: [Breaking Defense](#), [Defence Industry Europe](#)     



### U.S. Lockheed Martin Skunk Works unveils Vectis stealth drone for future air combat






Lockheed Martin's Skunk Works® introduced Vectis, a Group 5 collaborative combat aircraft (CCA), at the Air, Space & Cyber Conference 2025 in Maryland. The stealthy drone is designed to integrate with U.S. and allied fighters for precision strike, electronic warfare, and ISR missions, with Lockheed pledging to build and flight-test it within two years, a move that repositions the company in the Air Force's competitive CCA race. **#Vectis #CCA**

Source: [Army Recognition](#)     



### At the Partner 2025 exhibition in Serbia, EDGE Group puts next-gen EW tech on show along with other Serbian electronic warfare advancements

The Partner Belgrade exhibition has brought together senior officials from NATO, the European Defense Agency, and other security organizations. The Emirati EDGE Group stepped onto the stage for the first time, unveiling a mix of drones, radars, and electronic warfare (EW) systems as it sharpens its sights on the Balkans and Central and Eastern Europe. Serbia presented the Komarac 3 FPV multirotor, a low-cost, EW-resistant strike option, and the Komarac 2A, a multirole UAS designed for reconnaissance and attack missions while resisting electronic countermeasures. **#Partner2025 #Exhibition**

Sources: [Defense Industry Europe](#), [Army Recognition](#), [Army Recognition](#)     





# TECHNOLOGY

## MARITIME

### Raytheon strengthens US Navy's radar and electronic warfare capabilities

Raytheon and the U.S. Navy have achieved two key milestones to enhance maritime defense. The AN/SPY-6(V)4 radar completed its first live test in Hawaii, proving advanced air and surface tracking performance, while the ADVEW prototype for F/A-18E/F Super Hornets passed a major review, confirming improved survivability and electromagnetic resilience. Together, these programs mark a decisive step in modernizing the Navy's detection and electronic warfare capabilities.

#Raytheon #USNavy








Sources: [Army Recognition](#), [Naval Today](#)     

## LAND

### US Army demonstrates Epirus Leonidas electromagnetic weapon to neutralize 49 drones simultaneously

A swarm of 49 quadcopter drones was brought down within seconds during a test organized by Epirus at the Indiana National Guard base. The Leonidas system used high-power electromagnetic waves to simultaneously disable the onboard electronics of all the aircraft. The exercise was conducted in front of U.S. military officials, foreign delegations, and journalists. The drones crashed into a nearby field after losing control systems, confirming the system's capacity to neutralize a multiple-drone threat. #Leonidas #Neutralization



Source: [Army Recognition](#)     

### Turkish Army receives İLTER J350 C-UAS jamming system

The İLTER J350, made by Boğaziçi Savunma, is a full defense against the rising threat of unmanned aerial systems on the modern battlefield. The device can find up to 30 drones at once using protocol-based technologies. It can find signals coming from different directions up to 10km away for analogue video transmissions, 2km away for digital video signals, and 5km away for command-and-control signals. #İLTERJ350 #CounterDrones



Source: [TurDef](#)     

### Ukraine and Russia advance counter-drone and EW tactics

Ukrainian company Piranha Tech unveiled the DF-M, a modular electronic warfare system designed to jam drones such as Mavic and FPV models. The system allows military units to select different jamming blocks tailored to frequency ranges most often used by enemy drones on the front line. In parallel Nebo (Sky), a company based in the Belarus Lipetsk Technology Park, presented an FPV drone capable of autonomously disengaging from EW zones, highlighting ongoing efforts to develop UAVs resilient to jamming. #FPVDrone #Jamming

Sources: [Defence Blog](#), [TASS Russian News Agency](#)     

### Next-gen combat vehicle with UAV, loitering weapons to replace Army's T-72s

A future-ready combat vehicle (FRCV) is set to replace the Indian Army's Russian-origin T-72 main battle tanks. The army's FRCV will integrate human-machine teaming, ISR systems, and cyber-hardened networks to operate in a fully digitized battlefield. #FRCV #Tank



Source: [Business Standard](#)     



### French Army gains tactical Intelligence with new SERVAL electronic warfare vehicle

The French Directorate General of Armaments (DGA) announced the qualification of the first tactical signals intelligence (SIGINT) system integrated into the light multi-role armored vehicle SERVAL. This step is important as it represents the first electronic warfare capability directly embedded on a SCORPION family platform. The integration of electromagnetic sensors into a vehicle designed for mobility and modularity considerably broadens the operational scope of the French Army. #SIGINT #SERVAL



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

### U.S. Army advances resilient navigation and electromagnetic support capabilities

The U.S. Army is deploying its next-generation Mounted Assured Positioning, Navigation, and Timing (MAPS GEN II) systems to improve accuracy and resilience in GPS-degraded environments. In parallel, soldiers from the 25th Infantry Division are experimenting with innovative electromagnetic support technologies under the X-Tech program to enhance situational awareness, reduce operational risks, and strengthen multi-domain effectiveness—particularly across the Pacific theater. #USArmy #Developments






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

## SPACE

### Pentagon doubling down on alternatives to GPS that aren't in space

The U.S. military is doubling down on non-space-based alternatives to GPS, the position, navigation, and timing service provided by the U.S. Space Force, with new funding for developing and testing operational prototypes of quantum-based devices that don't depend on easily jammable signals from satellites. #PNT #Alternative



Source: [Air and Space Forces](#)     



# TECHNOLOGY

## SPACE

### US Space Force advances operational resilience with new FORGE, CROO, and training initiatives

The U.S. Space Force has reached several milestones to boost the resilience and readiness of its space operations. Space Systems Command delivered the second operational acceptance of the FORGE ground system, expanding OPIR processing capabilities for missile threat detection. In parallel, engineers are developing the AI-powered Cyber Resilience On-Orbit (CROO) tool to detect and mitigate cyberattacks on satellites in real time. To enhance preparedness, the service also plans to deploy "aggressor satellites" to simulate adversary tactics, providing more realistic training environments for space and cyber warfare. **#USSF #Resilience**

**Sources:** [Space Systems Command](#), [Air & Space Forces](#), [Air & Space Forces Magazine](#)     



### China launches group of Yaogan-40 satellites to study electromagnetic field

China has successfully launched the third group of remote sensing satellites Yaogan-40 into orbit, according to the China Aerospace Science and Technology Corporation (CASC). The Yaogan-40 satellites will be used to study the electromagnetic environment and conduct experiments related to it. **#Yaogan-40 #China**

**Sources:** [Russian News Agency](#), [CGTN](#)     



### India plans 'bodyguard satellites' to shield its space assets from debris and rivals

India is considering the deployment of specialized 'bodyguard' satellites designed to shield critical orbital infrastructure from emerging threats. This strategic initiative, still under development, responds to increasing concerns over vulnerabilities in space. Equipped with cutting-edge sensors, these protective spacecraft aim to counter risks such as signal jamming, cyberattacks, or physical interference from adversarial satellites. **#BodyguardSatellites #Resilience**

**Sources:** [The Free Press Journal](#), [Deccan Canal](#)     



### Deloitte studying cyber defense with on-orbit testbed

Deloitte is using its first internally funded satellite to game out on-orbit cyberattacks with a new system that could bolster the resiliency of current and future spacecraft. Since the launch of Deloitte-1, a 10-kg cubesat, Deloitte's space team is using the satellite to test out 20 vignettes, or scenarios of varying levels of cyber-threat or attack, Ryan Roberts said at the Space and Cyber Conference. During the tests, Silent Shield is ingesting radio frequency (RF) data and then analyzing it for cyber anomalies. **#SilentShield #Deloitte-1**

**Source:** [Aviation Week](#)     



## CYBER

### Thales unveils DCM5: a sovereign cryptography solution to combat the quantum threat for global defense and government

Building on the trusted Datacryptor heritage, DCM5 is future-proofed for quantum readiness and offers seamless integration with existing systems. With full backward compatibility with Datacryptor 2000, it is designed for secure communications across multiple nations, including Five Eyes partners and multinational coalitions. Key features include sovereign control, global interoperability, quantum-ready and certified protection. **#DCM5 #Quantum**

**Source:** [Soldier Systems](#)     



# MARKET & COMPETITION

## AIR

### UAV Navigation, Septentrio to enhance anti-jamming capabilities for UAVs

UAV Navigation-Grupo Oesia has collaborated with Septentrio, a division of Hexagon, to enhance navigation resilience for unmanned aircraft systems. The partnership focuses on ensuring compatibility between UAV Navigation's guidance, navigation and control systems and Septentrio's GNSS receivers. **#AntiJamming #Partnership**

**Source:** [GPS World](#)     



### Lockheed Martin Skunk Works, BAE Systems, and BANC3 advance next-gen electronic warfare capabilities

Lockheed Martin's Skunk Works and BAE Systems' FalconWorks have teamed up to co-develop a family of autonomous uncrewed air systems, with the first platform focused on electronic attack for Suppression of Enemy Air Defense (SEAD) missions. In parallel, BANC3 secured a U.S. defense contract to deliver a wideband 16x12 non-blocking RF switch matrix designed to enhance electronic warfare, SIGINT, and spectrum surveillance. Together, these initiatives underscore the push to field cutting-edge EW solutions across domains. **#Contract #Partnership**

**Sources:** [Breaking Defense](#), [TWZ](#), [PR Newswire](#)     





# MARKET & COMPETITION

## AIR

### Leonardo aims to build NATO's electronic warfare backbone

At DSEI 2025 exhibition in London, Leonardo positioned itself as the company underpinning NATO's return to serious electronic warfare mass. The firm used the London exhibition to confirm BriteCloud's adoption under the US ALQ-260 designation, to highlight BriteStorm, and to present Typhoon's ECRS Mk2 radar and EuroDASS upgrades as the foundation of a future European electronic attack force. Leonardo wants its UK-built systems to be seen as the backbone of an integrated combat air architecture that allies can adopt at scale. **#Leonardo #NATO**

**Source:** [UK Defence Journal](#)     

### South Korea launches \$1.3bn EW aircraft program

South Korea has initiated the Block-I Electronic Warfare System Development Project, a KRW 1.775 trillion (\$1.3bn) plan to induct 4 airborne EW and stand-off jamming aircraft by 2034. KAI-Hanwha Systems and LIG Nex1-Korean Air are competing. DAPA is reviewing bids submitted in September and is expected to select a preferred bidder in early October. Reports suggest the LIG Nex1-Korean Air team is currently favored. **#DAPA #Consortium**

**Sources:** [Korea JoongAng Daily](#), [Alert5](#), [FlightGlobal](#), [The Avionist](#)     

### Maxar and AIDC advance Taiwan UAV sector with GPS-jamming resilience software

Maxar Intelligence has partnered with Taiwan's Aerospace Industrial Development Corporation (AIDC) to integrate its Raptor vision-based navigation software across the country's unmanned aerial vehicle (UAV) sector. The collaboration aims to strengthen the reliability of autonomous systems operating in environments where GPS and GNSS signals are denied or jammed. **#AIDC #Partnership**

**Source:** [Spacewar](#)     

### India strengthens defense capabilities with \$7.5bn Tejas Mk1A contract and upcoming order for portable drone jammers

India's Ministry of Defense has signed a \$7.5bn contract with Hindustan Aeronautics Limited (HAL) for 97 Tejas Mk1A light combat aircraft, equipped with advanced systems such as the UTTAM AESA radar and the Swayam Raksha Kavach electronic warfare suite. Meanwhile, the Indian Army is preparing to place its first order for portable drone jammers from Paras Defense and Space Technologies Ltd., valued at up to \$3m, to boost counter-drone capabilities. **#India #Contracts**

**Sources:** [Defence Industry Europe](#), [Indian Defense News](#)     

## MARITIME

### L3Harris Technologies and Raytheon secure Navy contracts

Raytheon has secured a \$205m contract to continue production and upgrades of the Phalanx CIWS, the Navy's radar-guided close-in weapon system deployed across all surface combatant classes. In parallel, L3Harris Technologies won a contract worth up to \$939m for advanced radio systems for the Navy and Air Force, with work extending through 2030. Together, these awards highlight sustained U.S. investment in shipborne defense and next-generation communications capabilities. **#USNavy #Contracts**

**Sources:** [Naval Today](#), [Guru Focus](#), [Investing](#), [DoW](#)     

### Thales and UK partner unveil drone-based EW solution

At DSEI 2025 exhibition in London, Thales and the British firm Autonomous Devices announced a new partnership to develop a drone-based electronic warfare system for naval and land forces. The collaboration will produce the EW-UAS1, a turnkey platform combining Thales' electronic warfare payloads with a next-generation drone designed by Autonomous Devices. The payload aims to deliver both electronic support, detecting and geolocating threats, and electronic attack, including jamming. **#EW-UAS1 #Partnership**

**Source:** [UK Defence Journal](#)     

### Military orders new stealthy boats with advanced electronics for infiltrating and extracting special forces

Officials of the U.S. Special Operations Command announced a \$22.1m contract option to produce the Combatant Craft Heavy V (CCH V) stealthy special operations boats, designed primarily for use by Naval Special Warfare teams. The CCH is known for being among the largest and most technologically advanced boats in the U.S. Special Operations Command. It offers low observability, modularity, and improved capability for high-risk and covert missions, and uses advanced stealth and electronic technologies to evade detection. **#CCHV #Contract**

**Source:** [Military Aerospace Electronics](#)     








# MARKET & COMPETITION

## MARITIME

### DIU asks industry for 'non-kinetic' tech to help Coast Guard, Navy disable small boats

The U.S. Defense Innovation Unit (DIU), a Pentagon research agency known for its connections to Silicon Valley, is asking industry for non-kinetic technologies capable of helping federal authorities disable small, high-speed watercraft encroaching into American waters. "This could be, but is not limited to, localized, non-kinetic energy (e.g., electromagnetic radiation), a novel Electronic Attack (EA) method, or other novel means," the notice continued. **#DIU #Industry**

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



## LAND

### ★ U.S. Army accelerates radar and electronic warfare modernization through major contracts and new RAPTER initiative

The U.S. Army is ramping up its investment in radar, counter-UAS, and electronic warfare capabilities. Raytheon secured more than \$5.7bn across 2 contracts to deliver KuRFS and LTAMDS radar systems as well as Coyote counter-UAS platforms for the U.S. and allied forces. Meanwhile, Parsons Corporation obtained an \$81m C5ISR contract to provide AI-driven radar engineering solutions for the Army's DEVCOM. In parallel, the Army is preparing to launch the RAPTER program (Rapid Advanced Prototyping, Threat Environments, and Representation) to acquire next-generation EW services and solutions. **#USArmy #Contracts**

**Source:** [Army Recognition](#), [Zacks](#), [Insider Monkey](#), [Washington Technology](#)     



### BAE Systems pushes modernization with anti-jamming tech and autonomous vehicles

BAE Systems has teamed up with Forterra to rapidly prototype an autonomous version of the U.S. Army's Armored Multi-Purpose Vehicle (AMPV). The program aims to keep ground platforms operationally relevant against emerging threats such as drones, electronic warfare, and autonomous adversaries. In parallel, BAE has signed a contract with Hanwha Aerospace to integrate next-generation anti-jamming GPS technology into Hanwha's Deep Strike Capability precision-guided weapon system, reinforcing resilience against EW disruptions. **#Partnership #Contract**

**Sources:** [GPS World](#), [Army Times](#)     



### Bharat Electronics secures additional orders worth \$130m across EW, communication and tank systems

Bharat Electronics Limited (BEL), the Navratna Defense Public Sector Undertaking, has announced the receipt of additional orders valued at Rs. 1,092 Crore (\$130m), since its last disclosure on 16th September 2025. This development underscores BEL's continued prominence in India's defense and strategic technology sector. **#BEL #Contract**

**Sources:** [Business Upturn](#), [NDTV](#)     



### Ukraine strengthens electronic warfare with new military deliveries and U.S.-backed innovation

Ukraine is advancing its electronic warfare capabilities on two fronts. Defense startup Falcons secured U.S. funding from Green Flag Ventures to scale its RF direction-finding system, ETER, designed to detect enemy devices in GPS-denied environments, while moving toward NATO certification. In parallel, the Ministry of Defense announced that the first EW equipment has been delivered to the armed forces under the Army of Drones Bonus program, with additional contracts signed with domestic suppliers such as Parasol and Contra-drone. **#Contract #Funding**

**Sources:** [Tech EU](#), [Mezha](#), [Global Security](#)     



## SPACE

### Hanwha Aerospace and BAE Systems to enhance Deep Strike Capability with anti-jamming GPS

Hanwha Aerospace has signed a contract with BAE Systems to integrate next-generation anti-jamming Global Positioning System (GPS) technology into its 'Deep Strike Capability' precision-guided weapon system. The agreement brings together the companies' expertise to counter sophisticated electronic warfare threats and ensure superior accuracy in contested environments. **#EW #Contract**

**Source:** [Defense Industry Europe](#)     



### ★ Viasat selected to deliver space crypto solution for U.S. Space Force Space Systems Command

Viasat, Inc. is developing a new, space-based encryption solution to support data security for U.S. Space Force (USSF) Space Systems Command (SSC). Under this multi-year development award, Viasat's encryption team within its Defense and Advanced Technologies segment will build a next-generation cryptography solution for satellite applications, allowing the government to better protect critical space assets from cybersecurity threats. **#Viasat #SSC**

**Sources:** [Satnews](#), [Satcom Digital](#)     





# MARKET & COMPETITION

## SPACE

### **IRIS<sup>2</sup> : Thales remporte un premier grand contrat pour le développement de la constellation spatiale (Trad.: IRIS<sup>2</sup>: Thales wins first major contract for the development of the space constellation)**

The SpaceRISE consortium, which will operate the IRIS<sup>2</sup> space constellation launched by the European Commission, has awarded Thales Alenia Space a risk mitigation contract worth over €400m for the development of onboard technologies.

**#SpaceRISE #Contract**

Source: [La Tribune](#)     



### **Safran + QinetiQ forge alliance to deliver advanced anti-jamming PNT capabilities for UK Armed Forces**

Safran Electronics & Defense and QinetiQ have entered into a strategic partnership to deliver sovereign and resilient Positioning, Navigation and Timing (PNT) solutions for the United Kingdom Ministry of Defence (MoD). This collaboration addresses today's urgent need for trusted PNT capabilities in increasingly challenging and GNSS-denied operational environments. **#MoD #Partnership**

Source: [Satnews](#)     



### **NATO investing \$728m in new space capabilities, including a new 'data lake'**

NATO's collectively funded space efforts are focused on space domain awareness and intelligence, surveillance and reconnaissance. Col. Jonathan Whitaker, who heads the NATO Combined Forces Space Component Command, told Breaking Defense. The space operations center falls under the CFSpCC, with both located at Ramstein AFB in Germany. The two organizations are funded by a coalition of 16 NATO members. **#NATO #OperationCenter**

Source: [Breaking Defense](#)     



### **SatNews, SpaceNews launch EU Space Defence Track at SmallSat Europe 2026**

SatNews and SpaceNews have partnered to launch the EU Space Defence Track at SmallSat Europe 2026 in Amsterdam, convening stakeholders to discuss small satellites' role in enhancing Europe's defense amid geopolitical tensions. Drawing from Ukraine lessons, it focuses on rapid procurement, dual-use innovations, and resilient systems. This initiative aims to boost Europe's space autonomy and counter threats like GPS jamming. **#EUSpaceDefenceTrack #Partnership**

Source: [WPN](#)     



## CYBER

### **Leonardo accelerates Nordic cybersecurity acquisitions to strengthen Europe's defenses**

Italy's Leonardo is on a shopping spree to beef up Europe's cyber-defense capability and is targeting Nordic firms to get the job done, CEO Roberto Cingolani has told Defense News. He laid out the Italian defense giant's strategy after announcing a series of new investments during the summer. **#Acquisitions #Resilience**

Sources: [Defense News](#), [CyberExperts](#)     



### **USF signs contract with US Army for up to \$85m to conduct research in cybersecurity and more**

The University of South Florida (USF) is continuing to expand its relationship with the U.S. Department of Defense. The institution announced it has signed a contract with the U.S. Army for up to \$85m to conduct research in cybersecurity, biotechnology, energy sciences and more. This is a five-year deal with the U.S. Army Combat Capabilities Development Command Army Research Laboratory — also known as DEVCOM ARL. **#Research #Contract**

Source: [Wusf](#)     



### **Industrial sector faces tougher cyber insurance landscape with escalating premiums, coverage gaps**

Filing cyber insurance claims has become a tough journey for many industrial organizations, especially because more policies now exclude coverage for attacks linked to nation-states or 'war-like' incidents. **#Insurance #Gaps**

Source: [Industrial Cyber](#)     

### **Lockheed boosts defense tech with key microelectronics partnerships**

Lockheed Martin has launched strategic partnerships with key players such as Intel, Honeywell, and GlobalFoundries to advance trusted microelectronics for defense systems. These collaborations aim to secure critical supply chains, integrate high-reliability components, and reduce exposure to untrusted suppliers. The initiative underscores the growing role of secure microelectronics in enabling cyber resilience, electronic warfare capabilities, and advanced defense architectures. **#Microelectronics #Partnerships**

Source: [Zacks](#)     





## MARKET & COMPETITION

### CYBER

#### Code meets combat: Architecting the future of electromagnetic spectrum superiority

The Canadian Department of National Defence (DND) and the Canadian Armed Forces (CAF) have launched a challenge under the IDEaS program, offering up to \$6.75m in phased funding to advance electromagnetic spectrum (EMS) superiority. The initiative seeks innovative solutions for precision planning of offensive electronic warfare (EW) operations while preventing EMS fratricide—accidental interference with friendly signals. **#EMS #Funding**

Source: [Government of Canada](#)     



## THREAT INTELLIGENCE

### AIR

#### European officials warn of escalating Russian GPS jamming while military aircraft with Spanish defense minister undergoes GPS attack over Kaliningrad

After the GPS on Ursula von der Leyen's plane was reportedly jammed over Bulgaria, Lithuania's Foreign Minister said that signal disruptions are a daily reality in countries neighboring Russia. A Swedish statement also highlighted the fact that interference with GPS signals over the Baltic Sea has sharply increased. Most recently, a Spanish military aircraft carrying Defense Minister Margarita Robles became the third high-profile European government plane this year to experience GPS interference. Moreover, the commander of the Latvian Armed Forces witnessed a "360-degree threat" that includes invasion of airspace, cyber attacks, disinformation and manipulation. **#GPSJamming #Russia**

Sources: [Politico](#), [Euromaidan Press](#), [Independent](#), [The New Voice of Ukraine](#), [Pravda](#)     



#### Operation Sindoor heralded new kind of warfare, says Indian Chief of defense Staff

Chief of Defense Staff Gen Anil Chauhan said Operation Sindoor heralded a new kind of warfare, ensuring that India beat Pakistan decisively in every escalation during the strike. Unlike traditional warfare, this was fought in land, air, sea, electromagnetic space and cyber domains, where the adversary was seen only through the help of satellite and electronic images or signal intelligence, he said. **#OperationSindoor #HybridWarfare**

Source: [Business Standard](#)     



#### North Korea jammed South's GPS for 329 straight days

North Korea conducted GPS jamming for 329 consecutive days, from Oct. 2, 2024, to Aug. 26 this year, disrupting thousands of flights and maritime voyages and even causing South Korean military drones to crash, according to newly disclosed government data. **#GPS #Jamming**

Source: [The Chosun](#)     



#### Ukrainian drones strike Foros in Crimea, evading Russia's electronic warfare systems

Explosions in Crimea send a signal to Russia's leadership, who may have come under attack by Ukrainian Armed Forces drones, according to the head of the Ukrainian military's Reserve Council. He added the strikes suggest Ukraine's munitions bypassed Russian electronic warfare systems, which he said are no fewer than those deployed around the Kremlin in Moscow. **#UkraineWar #Strikes**

Source: [UAWIRE](#)     



#### Industry groups push U.S. government for rapid action on GPS jamming, spoofing

A coalition of industry organizations led by the GPS Innovation Alliance urged the U.S. Defense and Transportation departments to launch a coordinated, "whole-of-government" effort targeting GPS jamming and spoofing threats. The letter calls on federal agencies to accelerate the deployment of anti-jamming and authenticated signals in new satellites and ground systems, streamline certification of resilient GPS technologies, and strengthen enforcement against illegal jamming device sales. **#Industry #Warning**

Sources: [Location Business News](#), [GPS World](#), [GPS Innovation Alliance](#)     



### LAND

#### Dutch army to deploy hackers to front lines to gain battlefield advantage

The Royal Netherlands Army is deploying hackers to the front lines as part of the newly formed 101 CEMA Battalion. According to De Telegraaf, the unit, officially established in Stroe, merges companies specialized in electronic warfare and cyber operations. **#DutchArmy #101CEMABattalion**

Sources: [NL times](#), [De Telegraaf](#)     





# THREAT INTELLIGENCE

## SPACE

### New space threat fact sheet – US Space Force

This new updated Space Threat Fact Sheet reminds that space is no longer a safe haven for critical assets. It lists China and Russia and the intentional threats they pose. It mostly focuses on threats to satellites. While China's ambitious space program is a source of national pride and key to the Chinese Communist Party (CCP) plans for a powerful and prosperous nation, Russia has one of the world's largest space programs and remains a capable space actor. **#RNT #Jamming**

**Sources:** [Space Force](#), [Resilient Navigation and Timing Foundation](#)     



### ★ U.S., French, and German officials warn of growing space threats from China and Russia

Lt. Gen. Douglas Schiess, commander of U.S. Space Forces-Space, warned that China has become the foremost orbital threat to U.S. interests, rapidly advancing its capabilities to rival American dominance. France's Space Command chief, Maj. Gen. Vincent Chusseau, highlighted Russia's intensifying hostile actions since 2022, including satellite jamming, laser dazzling, and cyberattacks. Echoing these concerns, German Defense Minister Boris Pistorius revealed that Russian spacecraft are actively stalking German military satellites, capable of jamming, manipulation, or even destruction. All three stressed that space has fully emerged as a contested warfighting domain. **#SpaceWarfare #Rivalry**

**Sources:** [WPN](#), [The Washington Times](#), [Reuters](#), [Ars Technica](#), [Reuters](#)     

### IAF fooled Pakistan as European satellite firm tasked to track airbases during operation Sindoor

During the May 2025 India-Pakistan conflict, Pakistan reportedly contracted a Berlin-based satellite imagery company to monitor Indian Air Force bases in real time. India's space monitoring agencies, led by ISRO, detected these satellites and deployed countermeasures, while the IAF used dummy aircraft movements and decoy tactics to mislead surveillance. This strategic deception enabled a decisive strike on 11 Pakistani airbases, underscoring how commercial satellites can be exploited for military intelligence. **#ISRO #Intelligence**

**Source:** [Indian Defence Research Wing](#)     



### DSEI Takeaways: Space and cyber and the invisible front line

The advance of space and cyber technologies is creating "an invisible front line" in the warfighting domain. Military leaders at the Defense and Security Equipment International (DSEI) event stressed the need for agility, favoring faster 80% solutions over lengthy, rigid programs. The piece also underscores closer industry-defense collaboration to accelerate innovation and strengthen capabilities against hybrid space-cyber threats. **#DSEI #FrontLine**

**Source:** [Via Satellite](#)     



## CYBER

### Ukraine highlights evolving cyber tactics and resilience after three years of conflict

Ukraine's cybersecurity chief noted that while critical Russian cyberattacks have decreased due to stronger defenses and rising operational costs, non-critical operations such as espionage and DDoS attacks have intensified. The government's H1 2025 cyber report underscores how three years of full-scale war have turned cyberspace into a core battleground, stressing institutional resilience, adaptation, and international cooperation as key lessons for future preparedness. **#UkraineWar #Tactics**

**Sources:** [The Record](#), [Government of Ukraine](#)     



### ★ Chinese APT groups escalate cyber operations against Taiwan's semiconductor sector, Philippine military systems and U.S. defense tech firms

Proofpoint research revealed that China-aligned cyber espionage group TA415 has intensified attacks on Taiwan's semiconductor supply chain. At the same time, another Chinese APT group has been linked to a cyberattack on a Philippine military contractor using EggStreme, a sophisticated fileless malware designed to evade detection by injecting malicious code directly into system memory. Moreover, the state-backed RedNovember group has broadened its espionage to strike U.S. defense, aerospace, and technology firms, exploiting vulnerabilities in internet-facing devices for stealthy access. **#China #APTGroups**

**Sources:** [Industrial Cyber](#), [Dedi Rock](#), [Security Online](#)     



### ENISA Threat Landscape 2025

Through a more threat-centric approach and further contextual analysis, this latest edition of the ENISA Threat Landscape analyses 4875 incidents over a period spanning from 1 July 2024 to 30 June 2025. At its core, this report provides an overview of the most prominent cybersecurity threats and trends the EU faces in the current cyber-threat ecosystem. **#ENISA #Report**

**Source:** [ENISA](#)     





# THREAT INTELLIGENCE

## CYBER

### Russia-linked cyber actors intensify campaigns targeting critical infrastructure, defense personnel, and Poland

The FBI has warned that Russian state-sponsored hackers from FSB Center 16 are targeting networking devices and critical infrastructure worldwide. In the UK, cybercriminals from Russia, Iran, and Belarus are using fake LinkedIn job ads to compromise Ministry of Defence staff with malware. Meanwhile, Poland reports facing 20–50 cyberattacks daily against its critical infrastructure, prompting Warsaw to boost its cybersecurity budget to a record €1bn in response to Moscow's sabotage attempts. **#FSB #Center16**

Sources: [FBI](#), [FBI](#), [The i Paper](#), [Industrial Cyber](#) EW UV ISR AI QT



### 电磁硝烟与数字暗战：俄乌冲突中的电子战与网络战全景解析 (Trad.: *electromagnetic smoke and digital dark war: a panorama of electronic warfare and cyberwar in the Russia-Ukraine conflict*)

The Russia-Ukraine conflict fully illustrates the strategic value of electronic warfare and cyberwar in a high-intensity confrontation. Based on open-source information and reports from specialized organizations, this article reviews typical cases of electronic warfare and cyber operations observed during the conflict, analyzes the tactical logic and strategic impacts underlying these technological applications, and reveals how the 'silicon-based confrontation' is redefining the traditional rules of modern armed conflict. **#UkraineWar #CyberWarfare**

Source: [Chinese Institute of Command and Control](#) EW UV ISR AI QT



# TRAINING & EDUCATION

## AIR

### Course on military aviation cyber & electro-magnetic activities resilience

From 18 to 20 November 2025, the European Defense Agency (EDA), in cooperation with the European Security and Defense College (ESDC), will organize a course on military aviation cyber & electro-magnetic activities (CEMA) resilience. Alongside strategic briefings, the program will include a table-top exercise, allowing participants to respond to simulated cyber and electromagnetic incidents affecting air operations. **#CEMA #Course**

Source: [European Defence Agency Information](#) EW UV ISR AI QT



### The scale of Russian sabotage operations against Europe's critical infrastructure

This IISS paper assesses Russia's unconventional war on Europe, focusing on sabotage of critical infrastructure, from military sites and energy grids to communications and undersea cables, testing the resilience of European governments and societies and challenging NATO/EU deterrence. **#Russia #Paper**

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



## SPACE

### Cyberattacks on space information networks: vulnerabilities, threats, and countermeasures for satellite security

The growing reliance on satellite-based infrastructures has magnified the urgency of securing Space Information Networks (SINs) against cyber threats. This paper presents a comprehensive review of the vulnerabilities, threat vectors, and advanced countermeasures impacting SINs. Key vulnerabilities, including system complexity, use of Commercial Off-the-Shelf (COTS) components, lack of standardized security frameworks, and emerging quantum threats, are critically analyzed. **#SINs #Paper**

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



## CYBER

### France publishes educational guide on information warfare and new guides to strengthen cyber crisis management, and translates its annual cybercrime report in English

The French Ministry of Europe and Foreign Affairs has released a digital educational booklet designed to raise awareness of international information warfare, outlining strategic tools to counter disinformation and manipulation of information on the global stage. Meanwhile, the French National Cybersecurity Agency (ANSSI) has published a collection of 3 practical guides to support organizations in managing cyber crises. Moreover, The French Ministry of the Interior's Cyber Command (COMCYBER-MI) shared the 2025 annual cybercrime report, now translated into English. **#Guides #Report**

Sources: [MEAE](#), [ANSSI](#), [COMCYBER-MI](#) EW UV ISR AI QT



# TRAINING & EDUCATION

## CYBER

### Evaluating Russia's cyber strategy – CSIS report

The Center for Strategic and International Studies (CSIS) has released Part 2 of its Playbook for Winning the Cyber War. For over 15 years, Russia has refined its model of integrating cyber operations with military action—from Georgia in 2008, to Serbia in 2016–2017, and now the ongoing war in Ukraine. **#Russia #Strategy**



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

### Course on military aviation cyber & electro-magnetic activities resilience

From 18 to 20 November 2025, the European Defence Agency (EDA), in cooperation with the European Security and Defence College (ESDC), will organize a course on military aviation cyber & electro-magnetic activities (CEMA) resilience. Alongside strategic briefings, the program will include a table-top exercise, allowing participants to respond to simulated cyber and electromagnetic incidents affecting air operations. **#CEMA #Course**



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

### CLUSIF releases updated cybersecurity guide for industrial systems

CLUSIF has published an updated edition of its Cybersecurity Guide for Industrial Systems, freely available online. The guide offers practical benchmarks to strengthen the security of industrial environments, covering governance, asset mapping, cyber risk assessment, secure architectures, subcontractor management, and security maintenance.



**#CLUSIF #Guide**

Source: [CLUSIF](#) 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)