CLAWS Newsletter



Cyber Index | Volume II | Issue 21

by Govind Nelika

@govindnelika
govind-nelika-4217969b

https://claws.co.in/category/newsletter/

* CLAWS Cyber Index Newsletter is a concise Bi-Monthly brief delivering Strategic Insights on Global Cyber Threats, Policy Shifts, and Geopolitical Technology Developments.

About us

The Centre for Land Warfare Studies (CLAWS) is an independent think tank based in New Delhi, India, dedicated to strategic studies and land warfare in the Indian context. Established in 2004 and registered under the Societies Registration Act, 1860, CLAWS operates as a membership-based organization governed by a Board of Governors and an Executive Council, under the Aegis of the Indian Army.

With a futuristic outlook and a policy-oriented approach, CLAWS focuses on national security issues, conventional military operations, and sub-conventional warfare. The Centre closely monitors regional conflicts and military developments within India's strategic frontiers, particularly in South Asia.

Committed to fostering strategic culture and informed policymaking, CLAWS disseminates its research to armed forces personnel, policymakers, members of the strategic community, and interested civilians. By facilitating in-depth studies and discussions, CLAWS contributes to shaping India's defense policies and military preparedness.

The CLAWS Newsletters is a fortnightly series under the leadership of Dr. Tara Kartha, Director Research & Academics. The newsletter features insightful content curated by CLAWS researchers, each specializing in their respective verticals. This initiative aims to provide in-depth analysis, strategic insights, and updates on key issues.

Contents

Internal……. I – III

External…… III – V

United States of America (USA)…….…… 01

United Kingdom of Great Britain and Northern Ireland …… 02

Japan | Nippon-koku / Nihon-koku ……..…… 02 – 03

People's Republic of China (PRC) | China ……..……... 03 – 04

Republic of China (ROC) | Taiwan …….……..... 04 – 05

Democratic People's Republic of Korea …….…..... 05

Российская Федерация, Rossiyskaya Federatsiya | Russian Federation 05 – 06

Ukraine | Ukrayina (Україна) …….....…….....…… 06 – 07

The Republic of Poland | Rzeczpospolita Polska …….....……07

The French Republic | République française …….....….....07 – 08

European Union ……..…… 08 – 09

Middle East | West Asia …… 09

Malware & Vulnerabilities ……..…… 09 – 11

Internal

ATAGS gets bulk production clearance for the Indian Army

Private defence manufacturers Bharat Forge and Tata Advanced Systems Limited (TASL) have secured bulk production clearance to transition India's indigenous 155mm/52-calibre Advanced Towed Artillery Gun System (ATAGS) into serial manufacturing for the Indian Army, advancing a ₹6,900 crore ($805 million) contract signed with the Ministry of Defence in March 2025. As modern land warfare increasingly relies on high-mobility precision fires, electronic integration, and resilient domestic supply chains amid contested border environments and global defence supply-chain strain, scaling indigenous heavy artillery is central to India's force modernization and defence-industrial autonomy. Developed by the Defence Research and Development Organisation's Armament Research and Development Establishment with private partners, ATAGS features an all-electric drive, automated ammunition handling, digital fire-control computing, auto-alignment, and a firing range reaching roughly 48 kilometres with extended-range ammunition.

Under the 60:40 production split, Bharat Forge will manufacture 184 units and TASL 123 units out of the initial 307 howitzers, supported by specialized 6x6 high-mobility towing vehicles, with serial output ramping up in FY2027, initial deliveries slated for early FY2028, and phased induction spanning roughly four years against a wider Army requirement of 1,400 to 1,500 towed guns. Because the gun's automation and armour push its weight to nearly 18 tonnes exceeding legacy towing ecosystems built around sub-15-tonne pieces fielding requires parallel logistics, mobility, and training adjustments. While no cyber incidents, firmware vulnerabilities, or exploit details were reported, embedding electric drives and computerized fire-control systems across distributed private-sector assembly lines elevates cyber-physical risk management priorities: securing industrial operational technology, protecting embedded software and supply-chain integrity, and enforcing fleet readiness as India expands domestic defence manufacturing.

Read more: https://defence.economictimes.indiatimes.com/news/manufacturing/atags-gets-bulk-production-clearance-for-the-indian-army/135672551

India Activates DPDP Consent Manager Registration Framework

India's registration framework for Consent Managers under the Digital Personal Data Protection (DPDP) Act, 2023 came into effect on November 13, 2026, marking the transition from initial regulatory guidance toward active supervision and technical compliance. Operationalized ahead of the May 13, 2027 full-compliance deadline, the framework establishes a minimum net-worth threshold of ₹2 crore for India-incorporated entities seeking registration to act as interoperable intermediaries between Data Principals and Data Fiduciaries. Consent Managers are mandated to capture consent, manage its lifecycle, maintain auditable records, and ensure platform interoperability so individuals can grant, modify, or withdraw consent across multiple organizations without vendor lock-in.

For enterprise security teams and Data Fiduciaries, the activation requires immediate API-level integration capable of receiving and acting upon real-time consent signals and withdrawals through authenticated channels across data controllers, processors, and sub-contractors. Because consent logs and audit trails stored or processed outside India must maintain equivalent protection and lawful accessibility for Indian regulators, non-compliant architectures risk suspension, cancellation, or cumulative penalty exposure once full enforcement begins in May 2027. From a national cyber-governance perspective, operationalizing the Consent Manager layer institutionalizes standardized, auditable data-governance pipelines across India's digital economy.

Read more: https://www.pib.gov.in/PressReleaseDetail.aspx?PRID=2336151

Escalation of AI-Driven Attacks on BFSI Entities by Threat Actor "CRAFTY FALCON"

The Indian Computer Emergency Response Team (CERT-In) and its financial sector arm, CSIRT-Fin, issued advisory CICA-2026-3651 (updating CIAD-2026-0058 and CIAD-2026-0046) on November 4, 2026, warning

of an escalating, AI-driven campaign by threat actor CRAFTY FALCON against banking, financial services, and insurance (BFSI) entities. As financial institutions increasingly rely on automated payment, disbursement, and settlement APIs alongside cloud-native architectures, autonomous offensive AI tooling is compressing intrusion timelines and exploiting gaps between staging and production environments during low-staffing windows. CRAFTY FALCON targets non-banking financial companies, digital lending platforms, fintechs, payment aggregators, payment service providers, and cryptocurrency or virtual digital asset exchanges including re-attacking organizations that performed incomplete remediation after earlier restricted alerts. Technically, operations leverage publicly available AI-driven offensive frameworks including the ARTEX LLM family, PentAGI, Cairn, and CyberStrikeAI to execute end-to-end attack chains at machine speed, iteratively generate and mutate custom scripts, and rotate infrastructure IPs within hours to days.

Initial access frequently abuses internet-exposed UAT, staging, or test environments linked to production via shared credentials, tokens, or network paths, as well as rapid exploitation of newly disclosed file-upload and deserialization flaws to drop web shells in PHP and Node.js applications. Adversaries also reverse-engineer client packages for unauthorized API calls, bypass IP allow-lists via third-party URL-fetcher pools, abuse cloud management and serverless services such as AWS Systems Manager and Lambda, steal wallet keys from crypto entities, and validate unauthorized fund flows with micro-value test transfers (such as Rs. 1) before draining funds through disbursement or merchant settlement APIs. For risk management and cyber resilience, organizations must enforce strict environment isolation, server-side transaction validation, ephemeral credentials, API anomaly and micro-transfer monitoring, and continuous weekend or holiday coverage, reflecting a broader threat trend in which AI-automated reconnaissance and exploit iteration turn conventional engineering oversights into rapid financial loss.

Read more: https://www.cert-in.org.in/s2cMainServlet?pageid=PUBADV01&CACODE=CICA-2026-3651

Surprise, technological edge and jointness key to India's military preparedness: Rajnath Singh

Indian Defence Minister Rajnath Singh called on India's armed forces including the Indian Air Force (IAF), Indian Army, and Indian Navy to prioritize the element of surprise, technological superiority, and tri-service jointness during the Air Force Commanders' Conference in New Delhi on November 12, 2026. Framed around the conference theme "The Year of Empowerment: Maximising Efficiency Through Decentralisation" and informed by lessons from the Russia-Ukraine and Israel-Hamas conflicts alongside India's own Operation Sindoor, the remarks arrive as modern warfare expands rapidly across unmanned aerial systems, electronic warfare, cyber operations, and space. Speaking alongside IAF Chief Air Chief Marshal Ashutosh Dixit and Defence Secretary Rajesh Kumar Singh, Singh stressed that surprise can be achieved in both conventional and electronic dimensions while urging stronger intelligence, surveillance, and counter-drone capabilities against threats such as kamikaze drones.

He called for dedicated doctrines and operational frameworks tailored to electronic, cyber, and space warfare, greater platform integration across the three services, and fuller use of younger personnel's technical expertise. Concurrently, Singh launched a suite of artificial intelligence applications built in-house by the IAF's AI Centre of Excellence under the Unit for Digitisation, Automation, Artificial Intelligence and Application Networking (UDAAN), deployed on the IAF's secure network to accelerate operational, administrative, and aerospace safety workflows. Although no specific network vulnerabilities, malware indicators, or exploit details were disclosed, embedding AI tooling inside a restricted military network while demanding dedicated cyber and electronic doctrines carries clear implications for defense risk management: defenders must enforce strict model governance, data integrity, and network segmentation across multi-domain command-and-control environments, reflecting a broader shift in which algorithmic speed, tri-service interoperability, and sovereign tech resilience define strategic deterrence.

Read more: https://ddnews.gov.in/en/surprise-technological-edge-and-jointness-key-to-indias-military-preparedness-rajnath-singh/

Indian Army moves to harden drone fleet with new cyber labs

The Indian Army is moving to significantly harden its unmanned aerial systems (UAS) and battlefield electronic infrastructure against deep-seated digital supply chain compromises, establishing a specialized network of six cyber laboratories under a strategic initiative known as AASHVAST (Assessment and Analysis of Electronic Systems Hardware for Vulnerabilities and Security Threats). This development unfolds against a backdrop of escalating geopolitical friction along contested borders, where modern military operations increasingly rely on connected hardware, making the integrity of embedded software and foreign-sourced components a critical national security vector. With the inaugural facility already operational in New Delhi and five additional regional centres scheduled to open, the initiative introduces mandatory, rigorous pre-deployment checks to intercept concealed vulnerabilities. Operating under the purview of the Directorate General of Electronics and Mechanical Engineers, the laboratories leverage a custom-built software stack titled the Firmware Analysis and Validation Suite developed by QuickPay Pvt Ltd to probe systems far beyond standard visual or hardware-only inspections.

The facilities are engineered to uncover a diverse array of hidden risks, including concealed malicious code, unauthorized backdoors, hardcoded administrative passwords, hardcoded cryptographic keys, and covert remote-access tools embedded within drone firmware, communication links, and navigation modules. By shifting the defence acquisition lifecycle from simple functional procurement to mandatory digital verification, the framework directly addresses the threat of compromised foreign microchips and embedded subcomponents particularly originating from adversarial tech ecosystems that could otherwise be exploited to disrupt missions, hijack payloads, or leak sensitive telemetry data under electronic warfare conditions. Ultimately, this initiative underscores a broader structural paradigm shift in military cyber resilience: as battlefield hardware transitions into software-defined infrastructure, state defence apparatuses are institutionalizing rigorous software bill of materials (SBOM) and firmware validation protocols as non-negotiable baselines to safeguard national sovereignty and strategic readiness.

Read more: https://defence.economictimes.indiatimes.com/news/advanced-technologies/indian-army-moves-to-harden-drone-fleet-with-new-cyber-labs/134414690

External

Global Focus Brief

Star mathematician Ma Xiao leaves the US for China – and a career pivot to AI

Chinese mathematician Ma Xiao, 28, has departed his postdoctoral position at the University of Michigan to return to the University of Science and Technology of China (USTC) in Hefei as a professor and doctoral supervisor, signaling a high-profile career pivot from pure mathematics into artificial intelligence. Announced by USTC in late October 2026 and reported in early November, the move unfolds amid intensifying U.S.-China technological competition, tightening export controls, and a broader reverse migration of elite STEM talent from American universities to China's premier research institutions. A graduate of USTC's School of the Gifted Young and Hua Luogeng Talent Program who earned his doctorate from Princeton University in 2023, Ma gained international acclaim after collaborating with Zaher Hani and 2026 Fields Medalist Yu Deng beginning in late 2022 on a landmark breakthrough toward Hilbert's sixth problem.

Their work rigorously derived the Boltzmann equation from hard-sphere particle dynamics over extended time scales, mathematically bridging microscopic particle physics and macroscopic fluid equations. Over the past year, however, Ma has redirected his focus toward AI agents and automated scientific research, contending that while frontier models increasingly excel at literature synthesis and complex problem-solving, pairing machine scale with human intuition remains decisive for tackling unsolved technical frontiers. His return to USTC an elite C9 League institution anchoring China's national laboratories in quantum computing, secure communications, and foundational sciences carries tangible implications for strategic risk management, cyber

resilience, and national security. As top theoretical mathematicians transition into agentic AI and autonomous research pipelines, the convergence of advanced mathematical rigor with sovereign AI infrastructure threatens to accelerate breakthroughs across cryptography, algorithmic optimization, and dual-use modelling, narrowing Western technical leads and complicating long-term threat forecasting for defence and cybersecurity decisionmakers.

Read more: https://www.scmp.com/news/china/science/article/3373211/star-mathematician-ma-xiao-leaves-us-china-and-career-pivot-ai

Justice Department and FBI Seize Platforms Operated and Used by China State-Sponsored Hackers to Target U.S. Critical Infrastructure

The U.S. Department of Justice and the FBI seized domains to disrupt QScan and QTRouter, two platforms operated and used by China state-sponsored hackers including activity linked to QTFY to target U.S. critical infrastructure and federal institutions. For security teams and policy leaders, the action underscores how state-aligned threat actors rely on distributed proxy networks and operational relay infrastructure to mask attribution while probing high-value energy, telecommunications, healthcare, and government networks across strategic competition with Beijing. Announced on August 26, 2026, by the Justice Department's National Security Division, the U.S. Attorney's Office for the Southern District of California, and the FBI's Cyber Division and San Diego Field Office, the court-authorized seizures rendered QScan and QTRouter inoperable.

According to federal authorities, QTFY had targeted government agencies, power companies, telecom providers, and hospitals for nearly a decade with alleged victims including NASA, the Federal Reserve, the Department of Energy, the Department of Justice, and the U.S. Senate while routing malicious traffic through compromised everyday devices across more than 130 countries. Alongside the domain takedowns, the FBI, National Security Agency, and Cyber National Mission Force issued a joint advisory detailing QTFY's distributed systems to assist defenders with detection and mitigation, building on prior disruptions such as the Flax Typhoon botnet. While detailed exploit chains and specific indicator lists are governed by the seizure affidavit and joint advisory, the operation highlights broader implications for national security and risk management: because edge devices worldwide serve as anonymizing relays for state-backed reconnaissance and intrusion campaigns, organizations must pair perimeter hardening and threat hunting with continuous edge-device telemetry and cross-sector resilience, fitting a wider pattern of law-enforcement and intelligence disruptions designed to impose operational friction on persistent state adversaries.

Read more: https://www.justice.gov/opa/pr/justice-department-and-fbi-seize-platforms-operated-and-used-china-state-sponsored-hackers

US approves $2.1 billion Patriot missile deal for Ukraine; Zelenskyy welcomes approval

The U.S. State Department has authorized a critical $2.1 billion Foreign Military Sale of 500 Patriot Advanced Capability-3 Missile Segment Enhancement (PAC-3 MSE) interceptors to Ukraine, highlighting a pressing geopolitical imperative to fortify national critical infrastructure against sustained kinetic bombardment by Russian state forces. Amid escalating winter campaigns deliberately targeting civilian power grids and logistics networks, this authorization underscores the acute operational necessity for advanced defensive architectures in high-intensity threat environments. The procurement, supported by prime contractor Lockheed Martin, is notably decoupled from direct U.S. financing; instead, it is entirely underwritten by a coalition of allied nations including Canada, Germany, and Norway leveraging the U.S. JUMPSTART program and European Union credit facilities to expedite the acquisition.

Operationally, the PAC-3 MSE interceptors deploy sophisticated hit-to-kill technology, providing the enhanced altitude and extended range performance required to neutralize complex, fast-moving ballistic and cruise missile threats before they breach defensive perimeters. Ukrainian President Volodymyr Zelenskyy welcomed the diplomatic clearance, which follows a reported month-long administrative delay, while urgently advocating for accelerated delivery timelines to sustain the operational readiness of Ukraine's existing Patriot and NASAMS defence grids. Beyond the immediate eastern European theatre, this multilateral transaction reflects broader

systemic vulnerabilities within the global defence-industrial base, as military contractors face intense demands to scale production output to meet overlapping international assistance and domestic stockpile requirements. For strategic planners and national security stakeholders, this allied-funded procurement model demonstrates a deliberate shift toward distributed financial burden-sharing in international risk management. Ultimately, the integration of these advanced interceptors serves as a foundational layer of defence-in-depth, functioning as a vital component in Ukraine's overarching resilience strategy to mitigate catastrophic disruptions to sovereign infrastructure and stabilize a highly volatile geopolitical landscape.

Read more: https://newsonair.gov.in/us-approves-2-1-billion-patriot-missile-deal-for-ukraine-zelenskyy-welcomes-approval/

United States of America (USA)

Pentagon tells Europeans to cool their rhetoric on Russia, sources say

Pentagon officials including Under Secretary of Defence for Policy Elbridge Colby have privately urged several European NATO allies, notably Lithuania, Latvia, and Estonia, to tone down public rhetoric warning of threats from Russia. For defenders and policy stakeholders tracking hybrid warfare, these diplomatic shifts arrive as European critical infrastructure faces sustained sabotage and espionage linked to Moscow, while Washington pivots defence priorities toward East Asia, the Middle East, and Latin America, conducts a review of U.S. troop deployments in Europe, and revives negotiations to end the fifth year of the war in Ukraine. In private engagements reported in late October 2026, U.S. officials cautioned against "poking" Russia or using inflammatory framing such as describing Moscow as cornered and asked an Estonian delegation to adopt more measured public messaging, even as European leaders have linked Russian sabotage operations across the continent to strain from the Ukraine conflict and debate whether candid threat signalling rallies defence readiness or amplifies Kremlin psychological operations.

The Pentagon declined to comment on private allied discussions, and no specific technical vulnerabilities, malware families, or indicators of compromise were disclosed. Still, the divergence underscores a critical strategic tension for cyber resilience and risk management: as Washington presses Europeans to shoulder greater defence responsibility and explores diplomatic off-ramps that could touch on sanctions relief, frontline states must balance deterrence, attribution transparency, and public risk communication against hybrid coercion and shifting alliance posture a dynamic consistent with broader state-backed grey-zone campaigns where information warfare, sabotage, and geopolitical leverage intersect.

Read more: https://www.reuters.com/business/finance/pentagon-tells-europeans-cool-their-rhetoric-russia-sources-say-2026-10-30/

Syrian Man Sentenced for Wide-Ranging Hacking Conspiracy Conducted on Behalf of the Bashar Al Assad Regime

A federal district court in the Eastern District of Virginia sentenced Syrian national Ahmad Umar Agha (also known online as "Th3Pr0") to 42 months in prison for his central role in an expansive, decade-long hacking conspiracy conducted on behalf of the former Bashar al-Assad regime. Operating from August 2011 through January 2024, Agha and co-conspirators belonging to the state-backed Syrian Electronic Army (SEA) systematically targeted Western media outlets, non-governmental organizations, businesses, and government entities to suppress reporting on regime atrocities, disseminate state propaganda, and intimidate opponents. This development highlights the persistent threat of state-sponsored information warfare, demonstrating how auxiliary cyber units weaponize social media and digital infrastructure to manipulate public sentiment and cause real-world economic disruption. Court findings revealed that Agha utilized spear-phishing, social engineering, and credential compromise techniques to infiltrate at least 47 high-profile organizations.

Among the conspirators' most disruptive operations was the takeover of a major news agency's official Twitter account in April 2013, through which they posted false reports of explosions at the White House injuring then-President Barack Obama a disinformation stunt that triggered a sudden market flash crash and a temporary $136 billion loss in the Dow Jones Industrial Average. Other notable incidents included hijacking the U.S. Marine Corps' recruitment website to redirect visitors toward pro-regime propaganda and attempting to trick White House staff into surrendering social media credentials. Although Agha spent more than a decade as an international fugitive following his federal indictment (Case No. 1:18-cr-221), his sentencing underscores the long arm of transnational law enforcement and the Department of Justice's ongoing commitment to holding state-backed cybercriminals accountable. Ultimately, the case exemplifies the evolving intersection of cyber operations and geopolitical influence campaigns, reinforcing the critical need for robust enterprise credential hygiene, multi-factor authentication resilience, and proactive threat intelligence sharing to defend public institutions and financial markets against state-directed disinformation warfare.

Read more: https://www.justice.gov/opa/pr/syrian-man-sentenced-wide-ranging-hacking-conspiracy-conducted-behalf-bashar-al-assad-regime

United Kingdom of Great Britain and Northern Ireland

Defence contracts to prioritise British jobs and skills

The United Kingdom Ministry of Defence (MOD) and HM Treasury have introduced a mandatory Defence Offset Policy targeting overseas defence contracts valued at £50 million or more, signalling a major strategic push toward sovereign supply chain security and domestic industrial resilience. Announced on October 30, 2026, by Chancellor John Healey and Defence Secretary Wes Streeting at BAE Systems' Scotstoun shipyard in Glasgow, the initiative forms part of the government's broader "Back British" Budget framework and supports the Defence Investment Plan and Defence Industrial Strategy. The move arrives amid heightened geopolitical instability and escalating global threats to critical defence supply chains pressures that have led London to set a 3% GDP defence spending target by 2030 on the path toward a 3.5% NATO commitment by 2035. Although roughly 85% of MOD expenditure (£34.1 billion, supporting 274,000 jobs) already flows to UK-based firms, the new rules compel foreign prime contractors winning qualifying awards to reinvest equivalent value back into Britain's industrial base.

Effective for select procurements beginning in April 2027, contractors can fulfil these obligations through five mechanisms: creating UK jobs and apprenticeships, opening or expanding domestic factories, investing in British suppliers, sourcing UK-made components, and executing formal technology and know-how transfers to local firms. A newly established central Offset Authority will negotiate, value, and audit compliance across the full lifecycle of each Offset Agreement. For cybersecurity practitioners, defence risk managers, and policy stakeholders, this policy carries dual operational implications: while onshoring component manufacturing and domesticating supply chains mitigates exposure to opaque foreign sub-tier vendors and geopolitical chokepoints, formal technology transfers and expanded SME supplier networks simultaneously widen the domestic attack surface. Organizations integrating into these offset ecosystems will face intensified scrutiny to protect transferred intellectual property, harden operational technology environments, and enforce strict third-party cyber resilience against state-sponsored espionage.

Read more: https://www.gov.uk/government/news/defence-contracts-to-prioritise-british-jobs-and-skills

Japan | Nippon-koku / Nihon-koku (日本国)

Information leak affecting Fugaku and RIKYU users following unauthorized access to the supercomputer Fugaku

Japan's national research institute RIKEN disclosed on November 17, 2026, that an unidentified external threat actor breached the internal operational network of its flagship Fugaku supercomputer, forcing an emergency shutdown and exposing personal data and credentials belonging to up to 4,597 users across Fugaku and the AI for Science supercomputer RIKYU [1.1.1, 1.2.3]. Operated by the RIKEN Center for Computational Science (R-CCS), Fugaku represents a cornerstone of Japan's strategic computing and scientific infrastructure, making the intrusion a stark reminder of how adversaries increasingly target high-performance computing (HPC) environments to harvest federated credentials and pivot across interconnected research networks. Forensic findings indicate the intruder operated inside the operational network between November 10 and November 13, gaining initial access via a publicly accessible operational-status web dashboard whose maintenance was outsourced to an external service provider, though the exact exploitation mechanism remains under investigation.

Once inside, the adversary tampered with multiple internal servers, deployed malicious programs, and accessed both the user authentication system compromising names, email addresses, and user IDs for up to 4,224 Fugaku users and up to 375 RIKYU users and user home directories containing stored SSH private keys and access keys for external systems. While RIKEN found no evidence that research data was exfiltrated, investigators confirmed the intruder actively attempted to use stolen credentials to access external platforms. Following suspicious traffic alerts on November 12, RIKEN confirmed the breach on November 13, isolated affected systems, suspended Fugaku operations and external connectivity on November 14, rotated administrative keys, revoked all user login public keys, halted queued jobs, and notified the Ministry of Education, Culture, Sports, Science and Technology (MEXT), High-Performance Computing Infrastructure (HPCI) partners, and

the Personal Information Protection Commission. Beyond immediate recovery which includes server rebuilds and network reconfiguration the incident underscores critical resilience imperatives for national research infrastructure: strictly isolating public telemetry interfaces from operational control planes, tightening outsourced vendor governance, and eliminating static SSH key storage to prevent single-site compromises from cascading across global scientific ecosystems.

Read more: https://www.riken.jp/en/news_pubs/news/2026/20261116_2/index.html

U.S. and Japan Accelerate Missile Co-Production and Joint Cyber Defence Under "Operation Supercharge"

Japanese Defence Minister Shinjiro Koizumi and U.S. Secretary of War Pete Hegseth convened on October 28, 2026, in the Philippines on the sidelines of the ASEAN Defence Ministers' Meeting Plus (ADMM-Plus) to accelerate bilateral deterrence, defence-industrial integration, and joint cyber defence across the Indo-Pacific. Marking one year since their inaugural ministerial dialogue, the talks unfold amid rapid regional nuclear and missile buildups, coercive challenges to the Indo-Pacific status quo, Japan's accelerated revision of its three national security documents, and a surge in malicious cyber operations including large-scale personal information breaches targeting both nations. Aligning Tokyo's strategy with the U.S. National Defence Strategy, both leaders committed to building robust "denial defence" capabilities and strengthening Integrated Air and Missile Defence (IAMD) for peacetime and crisis contingencies. Building on the record-scale bilateral deployments executed during October's Keen Sword 27 exercise, Washington and Tokyo confirmed plans for more realistic live-fire drills, flexible air dispersal, expanded joint access to Self-Defence Forces and U.S. facilities, and a reinforced military presence across Japan's southwestern islands.

On the industrial front, the ministers advanced "Operation Supercharge" by agreeing to share technical data to scale up SM-3 Block IIA interceptor production, establish an Advanced Medium-Range Air-to-Air Missile (AMRAAM) Final Assembly and Check-Out (FACO) facility in Japan, and explore naval vessel cooperation, while also addressing U.S. Forces Japan realignment in Okinawa and incident-prevention measures following a recent robbery-murder case. Critically, both governments pledged deeper bilateral coordination to prevent hostile cyber activity from disrupting civilian life, economic systems, and national security. For cybersecurity practitioners and defence stakeholders, this convergence of kinetic deterrence and industrial co-production carries clear operational stakes: transferring sensitive missile specifications, manufacturing blueprints, and command-and-control links across allied networks significantly widens the defence-industrial attack surface, making synchronized threat intelligence, hardened supply chains, and proactive cyber resilience foundational to sustaining regional stability.

Read more: https://www.mod.go.jp

People's Republic of China (PRC) | China

Chinese university bought Nvidia H200 chips despite US blacklist

Procurement and corporate records expose that Northwestern Polytechnical University a Chinese institution tied to the People's Liberation Army and listed on the U.S. Commerce Department's Entity List acquired restricted Nvidia H200 artificial intelligence processors through a domestic intermediary despite U.S. export controls. As AI compute becomes central to military modernization, cyber operations, and strategic autonomy, Washington's efforts to curb dual-use semiconductor proliferation face growing pressure from gray-market sourcing and compute-rental workarounds. An October 21 procurement disclosure showed Northwestern Polytechnical, part of China's "Seven Sons of National Defense" and blacklisted since 2001 with tightened license denials in 2019 over missile and military research, bought two H200 GPUs for 874,700 yuan ($123,000) for its management school from Shaanxi Bosuan Network Technology rather than directly from Nvidia.

The institution also entered five contracts in 2026 with Chinese firms to rent compute capacity powered by H200 and other restricted Nvidia chips, including two January agreements for its cybersecurity school covering eight H200 processors over seven months. Across 26 reviewed 2026 procurement and corporate records, other defense-linked and academic bodies including Beihang University, the University of Chinese Academy of Sciences, and Wuhan University of Technology similarly procured or rented restricted H100, H800, A100, and A800 hardware via domestic vendors. Although the records do not reveal

hardware provenance, server locations, or specific technical vulnerabilities, even limited case-by-case H200 export allowances for non-blacklisted Chinese entities complicate enforcement against diversion, third-country brokering, and cloud-rental loopholes. For security leaders and policymakers, the findings underscore how hardware export controls alone struggle to contain military AI development when domestic aggregators and rented clusters obscure end-use lineage, reinforcing a broader pattern of state-backed technology circumvention that demands tighter supply-chain auditing, compute-access governance, and cross-border enforcement.

Read more: https://www.reuters.com/world/pla-linked-chinese-university-bought-nvidia-h200-chips-despite-us-blacklist-2026-11-11/

China formally launches project to build aircraft carrier-sized 'science island'

The People's Republic of China, via state-affiliated academic and defence contractors, has formally initiated the construction phase of the "Deep-Sea All-Weather Resident Floating Research Facility," an aircraft carrier-sized semi-submersible platform scheduled for completion by 2030. Spearheaded by Shanghai Jiao Tong University in collaboration with the China State Shipbuilding Corporation (CSSC), the $405 million project represents a significant escalation in dual-use maritime infrastructure. Amid intensifying geopolitical friction in the Indo-Pacific, this mobile "science island" sits at the nexus of civilian oceanographic research and strategic grey-zone posturing, providing Beijing with a persistent, sovereign operating base capable of extending its technological and intelligence-gathering reach well beyond the First Island Chain.

The 74,000-tonne displacement platform integrates robust engineering, featuring a twin-hull design that is highly resistant to typhoons and fortified with metamaterial sandwich panels designed to withstand nuclear shockwaves. Capable of cruising at 11 knots, the self-sustaining facility will support over 200 personnel and house six distinct shipborne laboratories, alongside a large moon pool capable of deploying 300-ton equipment to depths of 6,000 meters. While officially designated for deep-sea resource extraction and ecosystem observation, the platform's onboard sensor suites encompassing advanced sonar, underwater robotics, and deep-sea communication arrays offer formidable intelligence capabilities. This infrastructure enables the continuous collection of acoustic signatures, bathymetric data, and seabed mapping vital for tracking allied submarine paths and enhancing maritime domain awareness. For strategic analysts and defence planners, deploying this highly resilient, mobile logistics hub to contested corridors such as the South China Sea or the Indian Ocean introduces complex risk vectors. By embedding advanced surveillance architectures within ostensibly civilian research platforms, China effectively bypasses traditional legal constraints and normalizes its administrative presence, thereby complicating allied deterrence networks and the broader security architecture of critical maritime choke points.

Read more: https://www.scmp.com/news/china/science/article/3372330/china-formally-launches-project-build-aircraft-carrier-sized-science-island

Republic of China (ROC) | Taiwan

Ex-US commander urges arms sales to Taiwan

Retired U.S. Admiral Philip Davidson, former commander of U.S. Indo-Pacific Command, has urged Washington to expedite $14 billion in pending arms deliveries to Taiwan while warning that China's escalating information warfare poses a rapidly worsening threat to democratic stability across the Indo-Pacific and the United States. Speaking on November 13, 2026, on the podcast Why Should We Care About the Indo-Pacific?, Davidson revisited his March 2021 "Davidson window" assessment which warned that Beijing could develop the military capability to threaten Taiwan by 2027, a timeline later linked to Chinese President Xi Jinping's readiness directive to the People's Liberation Army. He noted that allied deterrence has improved through U.S. troop and missile deployments along the First Island Chain and the Philippines, Japan's 2022 shift toward 2% GDP defence spending and expanded cyber and space capabilities, and deeper Keen-series exercises with Australia and Japan. Simultaneously, Taiwan has extended compulsory military service to one year and pursued asymmetric capabilities including drones, uncrewed surface vessels, mobile precision weapons, and naval mines under its Overall Defence Concept.

However, Davidson flagged critical bottlenecks in U.S. arms production strained by the Middle East war, Ukraine aid, and surging global interceptor demand, calling for urgent delivery of Patriot

Advanced Capability-3 (PAC-3) and NASAMS air defence missiles within the next year. Beyond kinetic readiness, he highlighted a severely degraded digital information environment in which Beijing alongside Russia, Iran, and other state actors exploits social media to erode trust in Taiwanese and U.S. political, military, and business leadership. By weaponizing localized accidents and personal hardships through coordinated narrative flooding, bots and propaganda operators may account for up to 70% of activity in certain discussion threads. For cybersecurity defenders, threat analysts, and policymakers, the warning underscores that conventional deterrence alone is insufficient: countering gray-zone cognitive operations requires dedicated investment in defensive information warfare, platform resilience, and cross-sector threat intelligence before adversaries fracture institutional trust ahead of any kinetic crisis.

Read more: https://www.taipeitimes.com/News/front/archives/2026/11/17/2003867864

Democratic People's Republic of Korea

North Korea Responsible for $6 Billion+ Binance Attack

The Federal Bureau of Investigation (FBI), in coordination with the U.S. Secret Service (USSS) and Internal Revenue Service Criminal Investigation (IRS-CI), has formally attributed the historic $6.36 billion cryptocurrency heist against Binance to North Korea's state-sponsored TraderTraitor cyber unit, a subset of the Lazarus Group. Issued on October 31, 2026, the joint cyber alert underscores Pyongyang's escalating reliance on large-scale virtual asset theft to bypass international sanctions and finance its weapons programs shattering the previous record set by the $1.5 billion Bybit breach in February 2025. The intrusion unfolded on October 29, 2026, when attackers drained funds from Binance wallets across ten blockchains, moving the bulk of the assets within a 20-minute window starting at 20:05 UTC. According to post-incident disclosures and on-chain analysis, the months-long operation began with targeted social engineering including fake job interviews delivering a malicious coding assignment before operators pivoted through an internal AI tool to compromise wallet engineers and abuse container deployment permissions.

On Ethereum, the actors exploited EIP-7702 account delegation using 50 pre-signed authorizations to convert a Binance hot wallet into an attacker-controlled sweeper, while executing ordinary signed transfers across nine other chains. Although stablecoin issuers including Tether, Circle, and Ripple alongside Arbitrum's Security Council rapidly froze roughly $2.7 billion to $3 billion, TraderTraitor raced the freezes by converting stolen funds primarily into Ether (ETH), leveraging Aave and market makers, and dispersing assets via peel chains. Law enforcement has published associated attacker wallet addresses and urged THORNode operators, RPC node operators, DeFi protocols, instant exchanges, and virtual asset service providers to block all linked transactions. For defenders and policymakers, the incident exposes acute risks at the intersection of developer-targeted social engineering, over-privileged internal AI tooling, and cross-chain signing infrastructure, demonstrating that without strict chain-level isolation and real-time ecosystem-wide transaction blocking, state-backed adversaries can convert corporate security gaps into strategic national-security windfalls within minutes.

Read more: https://www.fbi.gov/investigate/cyber/alerts/2026/north-korea-responsible-for-6-billion-binance-attack

Russian Federation | Российская Федерация, Rossiyskaya Federatsiya

Russia using own version of Starlink for military comms over Ukraine, Kyiv says

Russia's armed forces have begun deploying the domestic Rassvet low-Earth orbit (LEO) satellite constellation coordinated by the state-backed aerospace firm Bureau 1440 for military communications over Ukraine, according to a November 6, 2026 assessment by Ukraine's Main Intelligence Directorate (GUR). The operational milestone arrives amid an intensifying race for sovereign battlefield connectivity, accelerated after SpaceX implemented terminal whitelisting in February 2026 to sever Russian access to unauthorized gray-market Starlink units. While SpaceX's network operates more than 10,000 active satellites, Moscow has placed 32 Rassvet satellites into orbit across two launches in March and July 2026, with additional deployments scheduled before year-end and long-term plans targeting over 900 satellites by 2035. Although GUR notes that the nascent constellation currently provides only intermittent coverage over Ukrainian territory as spacecraft pass overhead, even periodic satellite links carry significant tactical

consequences: by relaying telemetry through LEO assets, Russian strike drones can exchange data in real time, adjust flight paths mid-mission, improve targeting accuracy, and resist ground-based electronic warfare (EW) jamming.

On the supply-chain and policy front, Denys Sienik, Ukraine's chargé d'affaires in Washington, reported that Russia is developing the Starlink analogue using Chinese components and urged the United States to impose sanctions on entities supporting Rassvet, including Bureau 1440 a push on which the U.S. Treasury Department declined to comment. For cybersecurity defenders, military planners, and policy stakeholders, Rassvet's early battlefield integration highlights the rapid proliferation of resilient, state-controlled space communications in modern hybrid warfare. As adversaries reduce their dependence on easily jammed radio-frequency links and Western commercial constellations, safeguarding military operations and critical infrastructure will increasingly require integrated counter-space cyber capabilities, adaptive EW countermeasures, and tighter multilateral export controls targeting dual-use satellite hardware supply chains.

Read more: https://www.reuters.com/science/russia-using-own-version-starlink-military-comms-over-ukraine-kyiv-says-2026-11-06/

Russian hosting provider Beget has been hit by a new, large-scale attack.

Major Russian web hosting provider and domain registrar Beget Russia's third-largest registrar across the .ru and .рф zones has been hit by a massive, sustained distributed denial-of-service (DDoS) attack in mid-November 2026, compounding its recovery from a devastating data-wiping intrusion earlier in the month. For defenders and infrastructure operators, the consecutive assaults underscore the heightened vulnerability of foundational cloud and registrar infrastructure amid ongoing geopolitical conflict, where state-aligned hacktivists and cyber adversaries increasingly combine destructive wipers with volumetric disruption to prolong operational downtime.

Reported around November 15 as Beget had restored over 215,000 websites from backups following the November 1–2 control-plane breach which had zeroed data across virtual private servers, S3 storage, and Kubernetes clusters and affected an estimated 335,000 to 500,000 online resources the new high-intensity DDoS campaign caused intermittent access disruptions extending beyond Beget-hosted properties to major Russian digital platforms including Ozon, Wildberries, and Sberbank. Although Beget and Russian authorities have not formally attributed either wave to a specific threat group or released technical indicators of compromise, the provider had previously drawn European Union sanctions for hosting digital services for Russian-installed authorities in occupied Ukrainian regions. While detailed vector telemetry remains undisclosed, the dual-phase impact first wiping core cloud orchestration layers and then saturating network edge capacity during restoration illustrates how layered attacks amplify recovery friction. For risk management and cyber resilience, the incident reinforces the necessity of architectural decoupling: organizations should maintain immutable off-site backups, separate DNS and domain registration from primary hosting providers, and deploy multi-provider edge mitigation to prevent single-point-of-failure outages across interconnected national digital ecosystems.

Read more: https://expert.ru/news/rossiyskiy-khosting-provayder-beget-podvergsya-novoy-masshtabnoy-atake

Ukraine | Ukrayina (Україна)

Ukraine's air raid alert system hacked, Russian system targeted hours later

Ukraine's widely used Air Alert public warning application alongside municipal sirens in areas such as Zakarpattia Oblast was compromised late on November 1, 2026, triggering fabricated nuclear, radiation, chemical attack, street-fighting, and Oreshnik missile notifications across the country, including in Kyiv. For defenders and crisis managers, the incident highlights how civilian alert infrastructure has become a prime battleground for psychological disruption and information warfare during prolonged conflict, as attackers seek to induce panic and erode trust in official channels when seconds matter.

Following the breach which Ukrainian officials including the Air Force and the Center for Strategic Communications (SPRAVDI) attributed to Russian interference developers temporarily suspended the app, disabled push notifications, and later reported that adversaries had gained unauthorized access to the system's operator interface rather than the mobile client itself, while regional officials warned against

potential phishing links in fraudulent messages. Ukrainian Air Force spokesperson Yuriy Ihnat noted that military operations were unaffected because Air Alert is a supplementary civilian tool rather than an Air Force-operated system, while Kyiv Digital, outdoor sirens, and official Air Force and government channels remained active to verify actual threats and clear the false alarms within roughly an hour. Hours later, Russia's Emergencies Ministry reported a cyberattack on its own alert app that pushed false nuclear strike warnings. Broader implications for risk management and cyber resilience center on securing administrative control planes, enforcing multi-channel verification, and maintaining out-of-band communication redundancies so high-impact false alerts cannot trigger mass panic or operational confusion a pattern consistent with tit-for-tat state information operations across the Russia-Ukraine conflict.

Read more: https://kyivindependent.com/ukraines-air-raid-alert-system-hacked-air-force-says-as-false-nuclear-chemical-warnings-sound/

The Republic of Poland | Rzeczpospolita Polska

Poland shuts down government services platform ePUAP following cyberattack

Polish authorities temporarily shut down ePUAP, the nation's centralized electronic public administration platform, after detecting and halting a cyberattack on November 10, 2026, prompting an investigation by the Internal Security Agency (ABW). The disruption underscores the escalating operational exposure of national digital public infrastructure across NATO's eastern flank, where Poland has remained a persistent target for hostile cyber operations amid heightened regional geopolitical tensions. Maintained by Poland's Central Information Technology Center (COI), ePUAP serves as the primary portal enabling citizens, businesses, and public institutions to exchange official documents, submit administrative filings, and authenticate digital transactions. Deputy Prime Minister and Digital Affairs Minister Krzysztof Gawkowski confirmed that security teams intercepted the attack before core COI infrastructure was compromised, while ministry spokesperson Marek Gieorgica emphasized that the overnight suspension into November 11 was executed strictly as a precautionary containment measure rather than due to system damage.

Although authorities have not publicly disclosed the initial attack vector, technical indicators, or formal attribution and reported no confirmed data exfiltration the precautionary outage rendered ePUAP electronic mailboxes unavailable and risked temporary disruptions to the Trusted Profile digital identity and electronic signature system, with no immediate restoration timeline announced. Subsequent official assessments on November 12 indicated the activity originated from abroad, with forensic logs suggesting preparations for a broader operation designed to paralyze Polish public administration in December. The incident extends a sustained wave of high-impact intrusions across Poland's digital ecosystem, following October's data breach at online invoicing provider Fakturownia and September's compromises of healthcare software vendor Qbusoft and medical technology firm MyDr the latter potentially affecting 19 million individuals and 12,000 healthcare organizations. For public-sector defenders and policymakers, the episode illustrates how even thwarted intrusions against shared identity and e-governance backbones can force disruptive preventive downtime, reinforcing the need for architectural decoupling, resilient offline fallback channels, and continuous threat hunting to safeguard essential state services.

Read more: https://therecord.media/poland-shuts-down-government-services-platform-cyberattack

The French Republic | République française

Airbus and Thales will share a contract worth more than 1.5 billion euros: France has chosen the two groups for its next generation of military observation satellites.

France's defence procurement agency (DGA) and Ministry of the Armed Forces have awarded a contract worth more than €1.5 billion ($1.7 billion) to Airbus Defence and Space and Thales Alenia Space to build IRIS (Instruments de Renseignement et d'Imagerie Spatiale), the next generation of French military Earth-observation satellites.

As orbital reconnaissance, space domain awareness, and sovereign defense resilience grow vital amid heightened geopolitical tensions, anti-satellite threats, and multi-domain operations, securing long-term imaging and space-surveillance capacity has become a strategic priority for European security and cyber-physical defense. Notified in early November 2026 and announced on November 9, 2026, the multi-decade agreement runs through

the end of the 2030s and covers detailed design, manufacturing, testing, command-and-user ground segments, orbital operations, and maintenance for two satellites succeeding the current three-satellite CSO constellation under the multinational MUSIS framework. Airbus serves as lead contractor delivering both satellite platforms, much of the first satellite's payload, and ground infrastructure while Thales Alenia Space provides the first satellite's imaging payload, develops a next-generation optical instrument for the second, engineers data-protection and intelligence-security systems, and works with French supply-chain partners including Lynred, Pyxalis, Sodern, Reosc, ALAT, and Thales SESO. Designed for day-and-night visible and infrared very-high-resolution imagery, faster delivery, and on-orbit object imaging to detect orbital threats, the program will remain open to allied participation while no launch dates or specific vulnerability disclosures were released. For defenders, analysts, and policymakers, the award highlights critical risk-management imperatives across space and ground segments: protecting high-value telemetry, command-and-control links, ground stations, and AI-enabled imagery pipelines against cyber intrusion, signal interference, and supply-chain compromise a trend that reflects growing European investment in sovereign space intelligence and resilient multi-domain deterrence.

Read more: https://www.bfmtv.com/economie/entreprises/defense/airbus-et-thales-se-partageront-un-contrat-de-plus-de-1-5-milliard-d-euros-la-france-a-choisi-les-deux-groupes-pour-sa-prochaine-generation-de-satellites-militaires-d-observation_AD-202611090783.html

European Union

CERT-EU Warns of Widespread Threat-Actor Abuse of ARTEX AI Framework

The Cybersecurity Service for the European Union institutions, bodies, offices, and agencies (CERT-EU) warned on November 5, 2026, that threat actors worldwide and highly likely adversaries targeting EU institutions are actively weaponizing ARTEX, an open-source, large language model (LLM)-driven autonomous penetration testing framework. This development marks a pivotal inflection point in the global threat landscape, materializing April 2026 warnings that autonomous offensive AI would reshape the economics of vulnerability discovery by compressing intrusion timelines and lowering technical barriers to sophisticated exploitation. Designed to translate natural-language security objectives into multi-stage operations, ARTEX dispatches autonomous agent workers to execute real reconnaissance and exploitation tooling under an operator dashboard while integrating with external, user-supplied LLMs. Although the original developer removed the public repository in October 2026 following widespread misuse reports, independent community forks continue proliferating globally, fueling campaigns observed since August 2026 across government, financial, and supply-chain sectors including operations tied to China-aligned actors such as Storm-0940.

Because ARTEX lacks hard technical guardrails to enforce operational scope, malicious operators readily leverage it across MITRE ATT&CK techniques including Active Scanning (T1595), Obtain Capabilities: Tool (T1588.002), and Exploit Public-Facing Application (T1190). Unlike human testers constrained by time and fatigue, the platform probes internet-facing infrastructure at machine speed, crafting tailored payloads and chaining seemingly minor misconfigurations alongside traditional software vulnerabilities into high-impact attack paths. For enterprise defenders and policy stakeholders, the rise of agentic offensive tooling demands an urgent shift in cyber resilience: organizations must isolate internet-exposed management panels, prioritize emergency patching, enforce multi-factor authentication, closely monitor privileged accounts, deploy web application firewalls and endpoint detection and response controls, hunt for automated scanning artifacts, and retain even low-severity findings in continuous remediation cycles before autonomous adversaries chain them at scale.

Read more: https://cert.europa.eu/blog/from-penetration-testing-to-cyber-threat-beware-of-artex

Coordinated Cyberattacks Disrupt Refrigeration Systems Across More Than 115 European Supermarkets

A wave of cyberattacks struck commercial refrigeration and freezer control systems across more than 115 supermarkets and food retail outlets in Europe on November 2, 2026, forcing retailers to remove chilled and frozen inventory as a precaution. Affected locations spanned Belgium (including

Carrefour, Intermarché, SPAR, and Ahold Delhaize outlets), Sweden (over 20 ICA stores and 7 Coop locations), the Netherlands (at least 17 local food shops), Ireland (13 SuperValu stores), Portugal (7 Intermarché stores), Italy (4 Coop stores in Sicily), Germany (Edeka and CAP Markets), Finland (Kesko outlets), Estonia (Selver), Romania, Luxembourg, Poland, and food production facilities in the United Kingdom.

Following a larger October 11 disruption in France that forced refrigeration units into continuous defrost cycles reaching 50°C to 80°C, Swedish retailer ICA indicated that compromised Danfoss industrial controllers were likely leveraged in the November 2 wave, while an Estonian supplier confirmed attackers remotely elevated a store's refrigeration temperature to 50°C. Although no formal state attribution has been issued, European authorities and security researchers noted that exposed operational technology (OT) management interfaces and weak remote-access controls allowed attackers to inflict physical food-supply disruption without deploying sophisticated malware, prompting urgent advisories to isolate industrial controllers behind VPNs and multi-factor authentication.

Read more: https://www.theguardian.com/world/2026/nov/02/supermarket-freezers-across-europe-hit-by-second-suspected-cyber-attack

Middle East | West Asia

Turkey and Qatar sign mutual defence agreement

On November 13, 2026, Turkey and Qatar signed a bilateral mutual defence agreement in Istanbul, formalizing an upgraded security partnership between Turkish President Recep Tayyip Erdoğan and Qatari Emir Sheikh Tamim bin Hamad Al Thani during the 12th Turkey-Qatar Supreme Strategic Committee at Dolmabahçe Palace. Executed alongside four accords covering trade, education, consumer protection, and diplomacy, the pact emerges amid acute Middle Eastern instability following the U.S.-Israeli war with Iran, repeated Iranian disruptions in the Strait of Hormuz, and diminishing Gulf confidence in traditional U.S. security umbrellas. According to the joint communiqué, Ankara and Doha committed to safeguarding each other's sovereignty and presenting a "unified stance in confronting any external armed attack targeting either party or both of them," while expanding joint exercises, intelligence and operational coordination, military training, and defence-industrial co-production.

The agreement builds on more than a decade of bilateral military integration including Turkey's garrison established in Qatar during the 2017 Gulf blockade, Turkish F-16 deployments at Dukhan Air Base, and Doha's acquisition of Bayraktar TB2 unmanned aerial vehicles and complements Ankara's broader regional defence network, notably the August 2026 Makkah Pact with Saudi Arabia and Pakistan and October's four-nation "Badr" defence memorandum with Qatar, Pakistan, and Indonesia. Crucially, the full operational text remains undisclosed; unlike the Makkah agreement's explicit collective-defence clause, the publicly released terms leave ambiguity over binding combat obligations, and Qatar's non-NATO status precludes automatic alliance intervention. For defence analysts, cyber defenders, and critical infrastructure operators, the pact signals a structural shift toward multi-layered, non-Western security architectures in the Gulf. While enhanced deterrence aims to insulate Qatari energy assets and defence supply chains, deeper bilateral intelligence sharing, joint command networks, and co-developed military technologies inevitably expand cross-border digital attack surfaces, elevating the risk of state-sponsored cyber espionage, hybrid disruption, and defence-industrial targeting by rival regional actors.

Read more: https://www.middleeasteye.net/news/turkey-and-qatar-sign-mutual-defence-agreement

Malware & Vulnerabilities

Critical APT Package Manager Flaw (CVE-2026-109518) Exposes Debian and Ubuntu Systems to Root Code Execution

Security maintainers disclosed a high-severity time-of-check time-of-use (TOCTOU) vulnerability in the APT package manager, tracked as CVE-2026-109518, on November 4, 2026, affecting default configurations of Debian 12 (Bookworm), Ubuntu 22.04 LTS, and newer releases. The flaw requires a non-zero Acquire::Retries setting—enabled by default with a value of 3 in affected distributions—and allows an on-path attacker or malicious package mirror to abuse HTTP download retries to bypass archive signature verification. Because .deb installation scripts execute with root privileges, successful exploitation enables arbitrary remote code execution as root.

Canonical, Debian, and cloud providers including AWS (Bulletin 2026-172-AWS) issued immediate security updates and advised administrators to patch APT using -o Acquire::Retries=0 while migrating repository sources from HTTP to HTTPS. Organizations operating Linux fleets across cloud instances and container images were instructed to rebuild and redeploy affected images with updated APT packages. The vulnerability underscores the systemic supply-chain risk posed by cleartext package-retrieval defaults in foundational open-source infrastructure.

Read more: https://ubuntu.com/blog/apt-vulnerability-fixes-available

SlippyNunchucks hijacks Sogou Input Method's brand promotion mechanism to distribute malware

ESET Research has uncovered a DNS hijacking campaign by the China-aligned advanced persistent threat group SlippyNunchucks, which abused Tencent's widely used Sogou Input Method for Windows to deploy the modular DarkVigil espionage implant across Asia. Disclosed on November 4, 2026, the operation underscores how state-aligned actors increasingly weaponize trusted consumer software and legacy network protocols rather than costly zero-days to conduct transnational surveillance aligned with Beijing's crackdown on overseas online gambling and fraud networks. Active since at least September 2023 and assessed by ESET as distinct from Mustang Panda, SlippyNunchucks pivoted to Sogou on July 1, 2026, three days after a clean release ended its prior QuickFox supply-chain compromise. Exploiting an unencrypted HTTP weakness tracked as CVE-2026-120422 (CVSS 8.9), the group hijacked DNS resolution for the official backend config.pinyin.sogou[.]com through an undetermined router or ISP-level vector redirecting traffic to staging servers at 47.239.250[.]102 and 47.237.122[.]175 (sogou-cdn[.]com).

When the legitimate dispatcher SGTool.exe queried /api/brandScd/getBrandScd.php to fetch branded dictionary icons, attackers returned a spoofed AES-256-CBC configuration containing modified MD5 checksums and crafted file paths. This instructed the utility to drop a signed Adobe helper renamed biz_helper.exe alongside a malicious libcef.dll for DLL side-loading via SogouComMgr.exe or BizCenterCom. Execution launched DarkVigil (also known as FDMTP), a .NET framework supporting over 20 plugins and encrypted Duplex Message Transport Protocol (DMTP) command-and-control communications, targeting Chinese-speaking individuals and organizations including a multinational betting operator in Hong Kong, Thailand, Japan, Vietnam, Oman, and Sri Lanka. Following ESET's September 11 disclosure, Tencent released version 16.10 in late October to enforce HTTPS and TLS validation. For defenders and risk managers, the campaign illustrates how a single cleartext auxiliary endpoint can transform ubiquitous desktop software into a covert espionage conduit, reinforcing the imperative for universal TLS enforcement, strict egress controls, and continuous auditing of third-party applications.

Read more: https://www.welivesecurity.com/en/eset-research/slippynunchucks-hijacks-sogou-input-methods-brand-promotion-mechanism-to-distribute-malware/

Trojanized Claude Code Extension Plants an SSH Backdoor

An unidentified threat actor compromised the Cursor VS Code Extension Marketplace to distribute trojanized builds of Anthropic's official Claude Code extension (anthropic.claude-code versions 2.1.312 and 2.1.313), planting a cross-platform, persistent SSH backdoor on up to 5,000 developer workstations. Discovered by researchers at OpenSourceMalware alongside industry security teams, the campaign underscores an escalating supply-chain risk landscape in which adversaries bypass traditional perimeter defenses by weaponizing trusted AI coding assistants and auto-updating IDE ecosystems to gain privileged access to corporate environments. Rather than breaching Anthropic's internal infrastructure or Microsoft's official Visual Studio Marketplace, the attackers targeted Cursor's third-party extension registry between 09:27 and 20:35 UTC on October 29, 2026. Upon initialization, the injected multi-stage loader silently harvests host metadata including public IP addresses via ifconfig.me or api.ipify.org, OS architecture, global Git email configurations, and the names (though not values) of up to 40 sensitive environment variables matching strings like AWS, GCP, TOKEN, or SECRET and beacons this reconnaissance payload via HTTP POST to 134.209.82.225:8099/beacon to help operators prioritize high-value targets.

To establish interactive remote access, the malware appends an attacker-controlled Ed25519 public key (svc-telemetry) to ~/.ssh/authorized_keys, attempts to enable the local SSH daemon across Linux (systemctl), macOS (systemsetup), and Windows (OpenSSH.Server), and drops a hidden identity key to initiate a silent reverse SSH tunnel (ssh -N -R *:0:localhost:22) back to tunnel@134.209.82.225 every 60 seconds using autossh, ssh, or PowerShell loops. Cross-reboot persistence is maintained via a hidden ~/.config/.smt script paired with a spoofed com.apple.sysmond.plist LaunchAgent on macOS, an @reboot cron job on Linux, and a SysMon scheduled task or sysmon.cmd Startup script on Windows. Because replacing the extension with the clean 2.1.314 build or taking down marketplace infrastructure does not purge local artifacts, this incident highlights the urgent need for defenders to govern IDE extension supply chains, monitor living-off-the-land tunneling behaviors, and manually eradicate unauthorized SSH keys, persistence mechanisms, and exposed cloud credentials across developer endpoints.

Read more: https://opensourcemalware.com/blog/trojanized-claude-code-extension-plants-persistent-ssh-backdoor

AI-Powered Espionage Campaign Targets Government Linux Infrastructure

Palo Alto Networks Unit 42 has uncovered an AI-assisted cyberespionage campaign, tracked as CL-UNK-1211, that targeted government entities and state-affiliated Linux infrastructure between October 2025 and April 2026. Disclosed on October 15, 2026, the unattributed operation illustrates a pivotal shift in the threat landscape: rather than relying on exotic zero-days, adversaries are leveraging generative AI to rapidly produce, customize, and iterate disposable intrusion tooling at minimal development cost. Exploiting compromised web-facing servers for initial access, operators established durable persistence by altering global PHP auto_prepend_file directives under /etc/php/ and /opt/plesk/php/ to load /usr/lib/php/plesk_sys_driver.php, supplemented by web shells, SSH backdoors, SUID-enabled binaries, GsNetcat tunneling, and CVE-2021-4034 privilege escalation. Credential harvesting was multi-layered, combining poisoned. bashrc files featuring a spoofed sudo alias that logged passwords to a decoy file named Solarwinds.StatusLog.txt with no compromise of SolarWinds itself alongside modified PHP login pages and cleartext scraping of command histories and configuration files.

For persistent remote access, CL-UNK-1211 deployed SysGoRAT, a custom cross-platform Go-based remote access Trojan masquerading as legitimate utilities such as sys-control-client, pip2.7, and semanage, which communicated over WebSockets with a hardcoded command-and-control endpoint (104.194.158[.]65:443) to support arbitrary command execution, directory enumeration, interactive shells, and TCP proxying. Multiple scripts contained verbose, plain-English comments and occasional syntax errors such as a broken mailbox-compression script (zip_mails.sh) indicating LLM-assisted generation, paired with traditional anti-forensics including log erasure, file timestomping, blocked pgrep/pkill attempts against Cortex XDR, and false-flag red-team lures (RedTeamOps2025 and password pentest123). For defenders and decisionmakers, the campaign demonstrates that AI-accelerated payload churn rapidly erodes static indicator-based defences on mission-critical Linux servers, making behavioural detection, integrity monitoring of PHP and shell initialization files, off-host log forwarding, and strict red-team deconfliction essential for cyber resilience.

Read more: https://unit42.paloaltonetworks.com/ai-campaign-targets-linux-infrastructure/

About the Author

Govind Nelika is a Researcher, Web Manager, and Outreach Coordinator at the Centre for Land Warfare Studies (CLAWS), working on national security issues at the intersection of technology, cybersecurity, and geopolitics. His research focuses on hybrid warfare, digital influence operations, semiconductor geopolitics, AI-enabled conflict, and cyber governance, with publications covering topics such as U.S.–China tech rivalry, the Quad's cyber dynamics, and emerging risks in AI and supply chains.

He previously worked at Pondicherry University under the UGC-SAP (DRS II) programme in the Department of Politics & International Studies, progressing from Project Fellow to Project Associate. He holds a degree in Political Science and a Data Science certification from IBM. Earlier in his career, he gained research and digital management experience with the Regional Centre of Expertise, Trivandrum (affiliated with the United Nations University), and the Bureau of Police Research & Development (BPRD), Ministry of Home Affairs where he conducted research on cybercrime trends in India. He was awarded the Chief of Army Staff (COAS) Commendation Card on Army Day 2025 for his contributions to CLAWS

© All Rights Reserved 2026 Centre for Land Warfare Studies (CLAWS)

No part of this publication may be reproduced, copied, archived, retained or transmitted through print, speech or electronic media without prior written approval from C L A W S.

The views expressed and suggestions made are solely of the author in his personal capacity and do not have any official endorsement. Attributability of the contents lies purely with author.