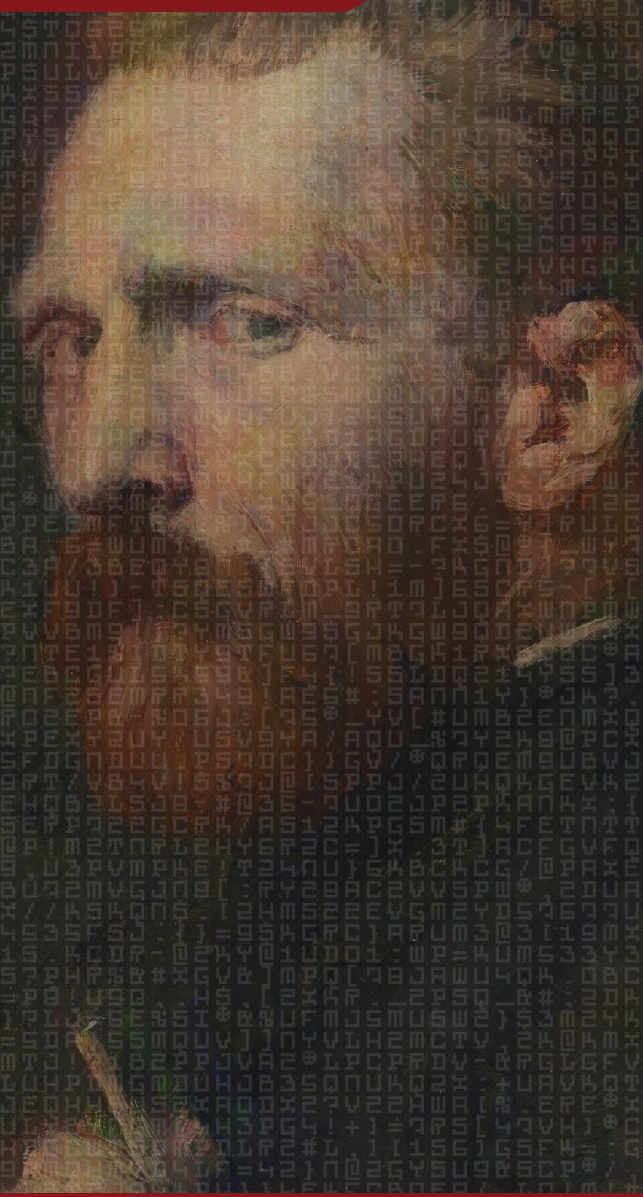


CLAWS Newsletter



Cyber Index | Volume II | Issue 16

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 Newsletter 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 – IV
External.....	IV – VI
United States of America (USA).....	01 – 02
The Commonwealth of Australia	02
European Union (EU)	02 – 03
People’s Republic of China (PRC) China	03 – 04
Republic of China (ROC) Taiwan	04 – 05
Российская Федерация, Rossiyskaya Federatsiya Russian Federation	05 – 06
Ukraine Ukrayina (Україна)	06
Malware & Vulnerabilities	07

Internal

Adani Defence signs 5-year deal with Indo-Russian JV IRRPL to supply ammunition for AK-203 rifles

In a critical move to harden supply chain sovereignty and reduce reliance on foreign defence ecosystems, Adani Defence and Aerospace has executed a strategic five-year agreement with Indo-Russian Rifles Private Limited (IRRPL) to supply indigenous 7.62x39 mm ammunition for India's AK-203 assault rifle program. Against the backdrop of volatile global supply chains and the strategic imperative to mitigate dependency on external notably Russian consumables amid ongoing geopolitical friction, this pact bridges a critical operational gap in India's defense-industrial base. Operationally, the agreement connects IRRPL's established rifle manufacturing hub in Korwa, Uttar Pradesh tasked with delivering over 600,000 AK-203 rifles under a December 2021 mandate with Adani's private-sector ammunition facility in Kanpur. This integration ensures a localized, disruption-proof pipeline of the specific small-caliber rounds required for the modernized Kalashnikov-pattern weapons, which feature a 700-round-per-minute rate of fire and an 800-meter effective range.

For military planners, supply chain security analysts, and risk management professionals, this consolidation represents a significant paradigm shift from state-monopolized hardware procurement to a decentralized, hybrid manufacturing model that heavily leverages private sector capacity. Until now, the program had achieved domestic rifle production but remained vulnerable to fragmented or externally sourced ammunition supply lines. By securing the end-to-end domestic lifecycle of these critical combat consumables, New Delhi is actively mitigating the risk of international embargoes, foreign exchange outflows, or logistical bottlenecks. Ultimately, this development substantially bolsters India's operational readiness and strategic autonomy, reflecting a broader global trend where nation-states are aggressively prioritizing closed-loop, localized defence ecosystems to insulate tactical military assets from international instability and systemic supply shocks.

Read more: <https://timesofindia.indiatimes.com/defence/news/adani-defence-signs-5-year-deal-with-indo-russian-jv-irrpl-to-supply-ammunition-for-ak-203-rifles/articleshow/133807487.cms>

DAC clears defence acquisition proposals worth ₹1.10 lakh crore

In a decisive move to fortify national defense infrastructure and mitigate supply chain vulnerabilities, India's Defence Acquisition Council (DAC) operating under the Ministry of Defence has authorized capital acquisition proposals totaling approximately ₹1.10 lakh crore for the Armed Forces. Situated against a backdrop of escalating regional tensions and the strategic imperative to achieve defense supply chain autonomy, this procurement unequivocally advances New Delhi's indigenization mandate, with 98% of the authorized platforms and systems designated for domestic sourcing. The approvals span a critical spectrum of multi-domain modernization efforts across the Army, Navy, and Air Force. Key land-based acquisitions include Chemical, Biological, Radiological, and Nuclear (CBRN) reconnaissance vehicles, high-mobility logistics transports, self-propelled mechanical mine layers, and the Sarvatra Bridge System, designed to enhance operational mobility and force protection in contested terrains.

For maritime operations, the Navy will integrate indigenous Arudhra radars to replace legacy Air Route Surveillance Radars, alongside the development of Marine Gas Turbines (MGTs) to decouple warship propulsion dependencies from foreign original equipment manufacturers. In the aerospace and electromagnetic domains, the Air Force will procure Advanced Light Helicopters (ALHs) and Ground-Based Multi-Purpose Jammers (GBMPJs) to degrade adversary radar capabilities, critically reinforcing the nation's electronic warfare (EW) posture. Furthermore, addressing physical and cyber-physical access risks, the military will roll out the Defence Forces Secure Access Card (DEFSAC) an interoperable, RFID-based identity architecture replacing antiquated paper-based credentialing. For defense contractors, risk managers, and geopolitical analysts, this sweeping capital injection signals a definitive maturation of India's indigenous defense-industrial base. By systematically decoupling from external suppliers while simultaneously upgrading its EW, CBRN, and access-control frameworks, India is aggressively hardening its multi-domain operational resilience. This comprehensive overhaul ultimately establishes a robust foundation to counter hybrid, symmetric, and asymmetric threat vectors in an increasingly volatile Indo-Pacific threat landscape.

Read more: <https://manufacturing.economictimes.indiatimes.com/news/aerospace-defence/dac-clears-defence-acquisition-proposals-worth-1-10-lakh-crore/133884848>

ISRO's 'privatisation' move: What India's space policy says

Under India's strategic push to radically expand its footprint in the global space economy, the Indian Space Research Organisation (ISRO) is executing a phased privatization of its core launch and operational processes, reallocating routine manufacturing to non-governmental entities (NGEs). This systemic transition, governed by the "Indian Space Policy 2023" and brokered through the Indian National Space Promotion and Authorisation Centre (IN-SPACe) and NewSpace India Limited (NSIL), aims to scale India's space economy from \$9 billion to upwards of \$40 billion over the next decade. Functionally, ISRO is divesting from the end-to-end manufacturing of operational launch vehicles including the workhorse Polar Satellite Launch Vehicle (PSLV), the Small Satellite Launch Vehicle (SSLV), and the heavy-lift LVM3 transferring these technologies to private consortiums such as Hindustan Aeronautics Limited (HAL) and Larsen & Toubro (L&T).

Additionally, IN-SPACe has initiated the handover of the upcoming Kulasekharapattinam spaceport in Tamil Nadu for private operation and management. While employee associations have raised concerns regarding workforce displacement, leadership maintains that ISRO is not being privatized; rather, the agency is pivoting its internal resources exclusively toward high-stakes, research-oriented missions. These include the Gaganyaan human spaceflight program, the Bharatiya Antariksh Station (India's planned modular space station), and complex lunar sample return missions like Chandrayaan 4 and 5. For geopolitical analysts and aerospace stakeholders, this policy execution signals a critical maturation in India's space doctrine. By offloading commercial cargo and low-earth orbit (LEO) logistics to a burgeoning private sector which saw investments surge to \$618.5 million in early 2026 India is fortifying its sovereign supply chain resilience while simultaneously freeing its premier space agency to compete directly in the high-end strategic domain of deep-space exploration and sustained orbital presence.

Read more: <https://indianexpress.com/article/explained/explained-sci-tech/isro-privatisation-private-sector-space-policy-10874018/>

Army sets up AASHVAST lab to detect Chinese components in military drones

In response to escalating supply chain vulnerabilities and the pervasive integration of commercial-off-the-shelf (COTS) technologies in military hardware, the Indian Army has established a specialized forensic facility named AASHVAST. Situated at the Directorate General of Electronics and Mechanical Engineers (DG EME) headquarters in New Delhi, the laboratory is specifically engineered to audit military unmanned aerial vehicles (UAVs) and defence electronics for unauthorized Chinese-origin components and malicious firmware. This strategic deployment arrives amid heightened geopolitical friction and a growing recognition that opaque global supply chains present severe espionage and sabotage risks, particularly where adversary-linked microprocessors or software logic are embedded within critical defence platforms. Operationally, the AASHVAST facility executes deep-level technical teardowns, employing advanced diagnostic software and hardware forensics to scrutinize drone electronics, firmware architectures, and communication protocols.

The primary objective is to systematically identify undocumented hardware anomalies, hidden backdoors, and embedded logic bombs that could enable data exfiltration, remote disruption, or signal hijacking by hostile threat actors. Technicians enforce stringent vetting protocols to guarantee that imported and domestically assembled drone systems are entirely sanitized of untrusted technologies before field deployment. For risk management professionals and defence analysts, the operationalization of AASHVAST represents a critical inflection point in supply chain security and cyber-physical resilience. It signals a definitive tactical shift from reactive perimeter defence to proactive, zero-trust hardware auditing at the nation-state level. Ultimately, this initiative underscores a broader international paradigm where securing the microelectronic supply chain is now viewed as functionally inseparable from maintaining sovereign operational integrity and neutralizing modern hybrid warfare threats.

Read more: <https://www.moneycontrol.com/news/india/army-sets-up-aashvast-lab-to-detect-chinese->

[components-in-military-drones-14024437.html](https://timesofindia.indiatimes.com/india/india-to-get-another-major-drdo-missile-testing-range-in-bengal/articleshow/134161810.cms)

India to get another major DRDO missile testing range in Bengal

In response to the escalating proliferation of asymmetric aerial threats and the tactical complexity of border security, India's Defence Research and Development Organisation (DRDO) is architecting a next-generation, technology-driven border surveillance and counter-unmanned aerial systems (C-UAS) network. As state and non-state actors increasingly leverage low-cost, modular drone technology for reconnaissance and payload delivery, traditional physical infrastructure is proving insufficient, driving a critical shift toward autonomous, multi-layered security architectures. The DRDO's strategic deployment integrates a dense array of advanced sensors, artificial intelligence, and directed-energy weapons into a unified operational shield. First-generation C-UAS frameworks are already active in high-risk zones, utilizing combined radar and electro-optical technologies for early detection and threat assessment. The platform operates on a dual-mitigation capability model: deploying soft-kill mechanisms for electronic interference and hard-kill solutions, specifically variable-power laser systems, for the physical neutralization of hostile drones.

To support comprehensive domain awareness, the overarching architecture incorporates fiber-optic intruder detection, hyperspectral and multispectral infrared imaging, and synthetic aperture radar (SAR). Crucially, these hardware components are orchestrated by newly developed AI and machine learning algorithms designed to accelerate threat classification and automate decision-making. A robust, next-generation communications infrastructure underpins the ecosystem, ensuring low-latency telemetry and threat data transmission across the decentralized network. Ultimately, this development significantly hardens India's defensive posture against hybrid warfare tactics and drone incursions. By prioritizing indigenous innovation in directed-energy interceptors and AI-driven domain awareness, the initiative enhances immediate cyber-physical resilience while reducing reliance on foreign supply chains. For global defense and risk management stakeholders, this signals a broader strategic pivot where the fusion of autonomous intelligence, electronic warfare, and modular sensor arrays has become the baseline requirement for maintaining sovereign integrity in a continuously evolving operational environment.

Read more: <https://timesofindia.indiatimes.com/india/india-to-get-another-major-drdo-missile-testing-range-in-bengal/articleshow/134161810.cms>

Armenia may be first buyer for India's longer-range guided Pinaka round

Amid escalating geopolitical friction and complex regional security pressures, Armenia is poised to significantly upgrade its kinetic strike capabilities by becoming the inaugural foreign operator of India's new 120-kilometer extended-range guided Pinaka rocket round. This development highlights a broader strategic trend in modern defence architectures: prioritizing modular, backward-compatible capability enhancements over costly, rip-and-replace hardware overhauls. As state actors look to maximize asymmetric advantages without ballooning procurement budgets, New Delhi and Yerevan are deepening a defence partnership that alters the tactical calculus in a volatile theatre. Developed by India's Defence Research and Development Organisation (DRDO), the guided Pinaka munition currently undergoing developmental trials with large-scale production slated for mid-2027 effectively extends Armenia's precision strike radius from 75 kilometres to 120 kilometres. Operationally, the critical advantage lies in seamless system interoperability.

Yerevan can deploy this extended-range ordnance using its existing Pinaka multi-barrel rocket launchers, command-and-control (C2) frameworks, and logistics chains. By significantly extending the stand-off distance, the system provides a critical tactical benefit: it allows artillery crews to execute precision strikes against high-value backend infrastructure such as adversary command posts, ammunition depots, and rear-echelon troop assemblies while remaining safely outside the immediate range of counter-battery fire. This scalable lethality upgrade bypasses the protracted procurement cycles typically associated with acquiring standalone tactical missile programs. For military planners and geopolitical analysts, this pending acquisition underscores a shift in how mid-sized state actors manage battlefield risk and operational resilience. By leveraging plug-and-play defence architectures, Armenia is hardening its defensive posture and enhancing its deep-strike deterrent capabilities. Simultaneously, the move cements India's evolving export playbook; by supplying continuously

upgradeable defence ecosystems alongside platforms like BrahMos and Akash, New Delhi is actively reshaping global arms supply chains and reinforcing strategic stability through localized deterrence.

Read more: <https://defence.economictimes.indiatimes.com/news/military-systems/armenia-may-be-first-buyer-for-indias-longer-range-guided-pinaka-round/134233803>

External

Global Focus Brief

US accuses Chinese AI firms of ‘malicious’ copying of AI technology

In a major escalation of the global artificial intelligence arms race, U.S. cybersecurity and intelligence agencies including the NSA, FBI, and CISA have formally accused six prominent Chinese technology firms of conducting “industrial-scale” and “systematic” theft of proprietary U.S. AI models via a technique known as knowledge distillation. Taking place against a backdrop of intensifying geopolitical friction ahead of a late-September summit between U.S. President Donald Trump and Chinese President Xi Jinping, this development underscores the massive economic and national security risks surrounding frontier AI systems. According to a joint federal advisory, Chinese companies including DeepSeek, Moonshot AI, Alibaba, and MiniMax extracted billions of tokens across millions of interactions from leading U.S. models such as Anthropic’s Claude and Fable, OpenAI’s GPT series, Google’s Gemini, and xAI’s Grok since at least late 2024.

Operating with likely state awareness, these actors exploited complex evasion tactics to bypass geographic restrictions and terms of service. They systematically leveraged fraudulent accounts, remote cloud providers, and a grey market of API proxies known as “transfer stations” to obfuscate metadata while extracting specialized reasoning, coding, and agentic capabilities. For example, Moonshot AI reportedly relied heavily on distilled data from Anthropic’s advanced Fable 5 model to train its Kimi K3 system, drastically undercutting traditional research and development costs. To mitigate this threat, U.S. agencies are urging AI developers to implement aggressive behavioural monitoring, quietly degrade outputs for suspected distillation requests, and enhance cross-industry threat intelligence sharing. Ultimately, this large-scale exploitation bridges the gap between corporate intellectual property theft and national security, as stolen capabilities could directly accelerate adversarial military and cyber-offensive operations. With U.S. officials warning of potential targeted sanctions, this campaign exposes a critical vulnerability in the AI ecosystem, demanding that defenders treat model API endpoints with the same rigorous defence-in-depth strategies historically reserved for critical infrastructure.

Read more: <https://www.reuters.com/technology/us-accuses-chinese-ai-firms-industrial-scale-theft-ai-technology-2026-09-08/>

Cao, Toti, Breckenridge Formally Nominated for Top Navy Jobs

In a decisive move to strengthen the strategic direction of the U.S. maritime defence posture, the White House has formally nominated three seasoned military and industry veterans Hung Cao, William Toti, and Richard Breckenridge to the highest civilian leadership roles within the Department of the Navy. This leadership transition occurs against a backdrop of escalating geopolitical tensions and a rapidly evolving technological risk landscape, where the Navy is aggressively overhauling its shipbuilding pipeline, industrial base, and cyber-physical infrastructure to counter near-peer adversaries. The primary development centres on the nomination of Hung Cao for Secretary of the Navy. Cao, who has served as the acting secretary since April 2026 and recently advanced the Navy’s data and artificial intelligence weaponization strategy, requires a congressional waiver for confirmation due to his 2021 retirement as a Navy captain, bypassing the statutory seven-year cooling-off period.

He is joined by William Toti, a retired Navy submarine commander and former defence sector executive nominated for Under Secretary, and retired Vice Admiral Richard Breckenridge, nominated for Assistant Secretary of the Navy for Research, Development, and Acquisition. Both Toti and Breckenridge have recently operated in advisory and acting capacities to shape the department’s modernization, pushing the “Golden

Fleet” initiative to streamline procurement, consolidate enterprise IT networks, and accelerate the fielding of advanced defence technologies. For defence practitioners, risk managers, and policy stakeholders, this leadership slate signals a critical operational pivot. By elevating officials with deep expertise in electronic warfare, AI integration, and systems acquisition, the Pentagon is moving to harden its defence supply chains and accelerate the deployment of next-generation combat capabilities. Ultimately, this structural realignment reflects a broader national security imperative to ensure cyber resilience and sustain tactical overmatch in an increasingly contested global threat environment.

Read more: <https://news.usni.org/2026/09/15/cao-toti-breckenridge-formally-nominated-for-top-navy-jobs>

Bengaluru-based Pranos unveils India’s 1st private compact nuclear fusion reactor

In a significant shift toward sovereign energy resilience and deep-tech autonomy, Bengaluru-based startup Pranos Fusion has activated “Pragya,” India’s first privately developed compact nuclear fusion reactor. This development occurs against a backdrop of intensifying global competition to secure high-density, zero-carbon energy sources, marking a structural pivot from massive, state-funded multinational projects like ITER to agile, privately capitalized ventures. For critical infrastructure defenders and strategic decision-makers, this transition is pivotal; localized mastery of advanced fusion architectures promises to ultimately decouple national power grids from volatile, geopolitically contested fossil fuel supply chains. Operationally, Pragya is a low-aspect-ratio tokamak engineered in approximately eight months. Rather than generating commercial electricity, the facility functions as a high-frequency experimental testbed designed to study and stabilize superheated plasma. Operating with a 0.40-meter major radius and a 0.1 Tesla toroidal magnetic field, the reactor is projected to execute roughly 3,000 experimental plasma shots annually over a 20-year lifecycle.

This rapid testing cadence will generate vast datasets to refine real-time plasma control algorithms, validate next-generation high-temperature superconducting (HTS) magnets, and optimize reactor diagnostics. Pragya represents the foundational phase of Pranos Fusion’s broader roadmap, which targets the deployment of operational HTS magnets by 2027 and the construction of a net-gain fusion reactor, designated PraniQ, by 2030. For national security planners and risk management professionals, the emergence of private-sector fusion hardware in India signals a critical maturation of domestic technological capabilities. By accelerating the development pipeline for compact fusion systems, initiatives like Pragya fortify long-term energy security and critical infrastructure resilience. Ultimately, the successful commercialization of these technologies will fundamentally alter the geopolitical risk landscape, neutralizing energy-based economic coercion and establishing a highly resilient, decentralized power infrastructure capable of sustaining next-generation strategic demands.

Read more: <https://www.indiatoday.in/science/story/bengaluru-based-pranos-unveils-indias-1st-private-compact-nuclear-fusion-reactor-pragya-2986249-2026-09-03>

Kalyani Strategic Systems signs strategic alliance agreement with Thales for 70-mm rocket systems

Amid escalating global ammunition shortages and the critical imperative to secure sovereign defence supply chains, French aerospace giant Thales and India’s Kalyani Strategic Systems Limited (KSSL) have executed a Strategic Alliance Agreement to localize the manufacturing of advanced 70-mm rocket systems. This technology transfer represents a strategic decentralization of kinetic production at a time when modern battlefields demand high volumes of precision munitions to neutralize asymmetric threats such as drone swarms. By onshoring manufacturing, military readiness is effectively insulated from international logistical chokepoints and geopolitical friction. Signed during a recent Belgian state visit to New Delhi, the pact facilitates the domestic assembly of both unguided and laser-guided variants of Thales’ combat-proven 2.75-inch (70-mm) rockets.

Leveraging intellectual property and launcher technology developed in Belgium, production will be anchored at KSSL’s upcoming energetics facility in Andhra Pradesh, with the first fully Indian-assembled rocket slated for rollout by early 2027. These munitions are already active within the Indian Armed Forces and are engineered for multi-domain integration, specifically arming rotary-wing assets like the HAL Rudra (ALH-WSI) and the

Prachand Light Combat Helicopter (LCH). Tactically, the 70-mm architecture provides scalable lethality, allowing operators to bridge the gap between economical unguided saturation and high-value precision strikes, with specialized variants increasingly positioned for kinetic counter-unmanned aerial systems (C-UAS) operations. For defence planners, risk managers, and supply chain analysts, this alliance significantly alters the strategic calculus. It hardens India's defence-industrial base, transitioning the nation from an importer of finished hardware to a sovereign systems integrator. Simultaneously, it provides European stakeholders with a critical secondary manufacturing node, building resilient global supply redundancy to counter surging operational demands and persistent geopolitical volatility across the international threat landscape.

Read more: https://www.business-standard.com/markets/capital-market-news/kalyani-strategic-systems-signs-strategic-alliance-agreement-with-thales-for-70-mm-rocket-systems-126090301441_1.html

Bharat Forge, Pratt & Whitney join hands for India's HALE programme: What it means for India's UAV push

In a strategic move to fortify indigenous aerospace capabilities and reduce supply chain dependencies, Bharat Forge and Pratt & Whitney Canada (an RTX business) have announced a collaboration to develop propulsion systems for India's High-Altitude, Long-Endurance (HALE) Unmanned Aerial Vehicle (UAV) program. Spearheaded by the Defence Research and Development Organisation (DRDO), this initiative unfolds against a backdrop of prolonged geopolitical friction along the Line of Actual Control and intensifying competition for maritime domain awareness in the Indian Ocean Region.

Historically reliant on foreign original equipment manufacturers for tactical drone powerplants, India is leveraging this partnership under its Aatmanirbhar Bharat (self-reliance) mandate to close a critical technology gap in advanced aerospace propulsion. Operationally, the joint effort will evaluate the integration of Pratt & Whitney's turboprop engines into the DRDO-designed HALE platform, targeting sustained, heavy-payload operations at altitudes exceeding 35,000 feet. Pratt & Whitney Canada will drive engine compatibility and performance assessments, while Bharat Forge will spearhead end-to-end engine-airframe integration, systems interfacing, and domestic manufacturing. By combining proven, high-reliability turboprop architectures with localized engineering expertise, the program aims to deliver a platform capable of persistent, high-resolution intelligence, surveillance, and reconnaissance (ISR) across volatile mountainous and maritime domains. For defence planners and supply chain risk analysts, this collaboration represents a significant milestone in India's pursuit of strategic autonomy. Developing a sovereign industrial base for complex unmanned systems directly mitigates the risks of international embargoes and prolonged procurement bottlenecks, transitioning the nation from an importer of finished aerospace assets into a robust systems integrator. Ultimately, securing a reliable, indigenously integrated propulsion pipeline for long-endurance drones enhances India's operational readiness, hardening its strategic deterrent posture and reinforcing operational resilience in an increasingly contested multi-domain threat landscape.

Read more: <https://www.livemint.com/news/india/bharat-forge-pratt-whitney-join-hands-for-india-s-hale-programme-what-it-means-for-india-s-uav-push-11789544117994.html>

Ethereal Exploration Guild takes aim at the one thing SpaceX hasn't yet achieved: full rocket reusability

In a significant disruption to the commercial aerospace sector, Indian space-tech startup EtherealX is engineering a fully reusable medium-lift launch vehicle, directly targeting a capability threshold the recovery of both booster and upper stages that remains unmastered by industry leaders like SpaceX. As the global space economy accelerates, the high cost of orbital transport and limited launch cadences remain critical bottlenecks for deploying resilient satellite constellations and maintaining sovereign aerospace capabilities amid intensifying geopolitical competition in low Earth orbit (LEO). To overcome these constraints, EtherealX is developing the Razor Crest MK-1 rocket, powered by its proprietary 80 kN Pegasus upper-stage engine. The architecture leverages a novel Full-flow Segregated Cooling Cycle (FSCC) running on RP-1 (kerosene) and liquid oxygen.

Departing from traditional designs that require heavy heat shields, the FSCC system captures aerothermal re-

entry heat through regenerative cooling channels to vaporize and pressurize the propellant before injection, bypassing the need for pre-burners while achieving a reported 99% combustion efficiency. The vehicle is engineered to deliver 24.8 tonnes to LEO in an expendable configuration or 8 tonnes when fully reused, aiming to drive launch costs down to a highly competitive \$500–\$1,000 per kilogram. Bolstered by a recent \$20.5 million Series A funding round, EtherealX plans hot-fire testing by 2027, with commercial missions slated for 2028. If validated, this capability will drastically lower the financial barrier for orbital access, enabling rapid replenishment of critical space-based communication, navigation, and observation assets. Ultimately, mastering full-stage reusability will decentralize the current launch monopoly, fortify national security supply chains, and redefine the strategic calculus of space domain awareness and operational resilience.

Read More: <https://www.moneycontrol.com/news/business/startup/etherealx-takes-aim-at-the-one-thing-spacex-hasn-t-yet-achieved-full-rocket-reusability-14022701.html>

Singapore unveils world-first biological data centre with 16 million living human neurons powering 20 computers in a landmark moment for AI

In a significant evolution of hybrid computing infrastructure, a consortium comprising the National University of Singapore (NUS), data center operator DayOne, and biological computing firm Cortical Labs has unveiled the world's first biological data center prototype. As the explosive growth of artificial intelligence severely strains global energy grids and silicon processor scaling nears its physical limits, the technology sector is increasingly pursuing unconventional computing architectures to mitigate looming resource constraints. The newly demonstrated prototype addresses this by integrating 20 CL1 biological computing units into a standard server rack, utilizing an estimated 16 million living human neurons grown from stem cells. These neuronal cultures are physically interfaced with silicon microelectrode arrays and managed by Cortical Labs' biological intelligence operating system (biOS). This architecture enables real-time, closed-loop interactions where electrical signals stimulate the biological network, actively translating cellular responses into actionable digital data.

Notably, the system incorporates a dedicated life-support mechanism capable of maintaining the neural cultures for up to six months, introducing a novel requirement for biological stewardship alongside traditional electronic maintenance. Building upon prior synthetic biological intelligence experiments like the "DishBrain" model, this installation transitions the technology from isolated laboratory environments to scalable, commercially oriented server deployments. While currently operating as a proof of concept rather than an immediate replacement for GPU-driven infrastructure, this development signals a potential long-term shift in digital resilience and security operations. Biological neural networks inherently adapt to dynamic conditions and can process information using a fraction of the power required by conventional digital systems. For cybersecurity practitioners and enterprise risk managers, this technology could eventually pioneer highly efficient, low-power computing platforms uniquely optimized for complex anomaly detection, behavioural fraud modelling, and rapid incident response, simultaneously reducing the environmental footprint and supply-chain vulnerabilities inherent in modern AI ecosystems.

Read more: <https://timesofindia.indiatimes.com/science/singapore-unveils-world-first-biological-data-centre-with-16-million-living-human-neurons-powering-20-computers-in-a-landmark-moment-for-ai/articleshow/133451573.cms>

United States of America (USA)

Army Announces Move to Production for Tactical Intelligence Targeting Access Node (TITAN)

In a pivotal advancement for military AI and battlefield intelligence infrastructure, the U.S. Army has officially transitioned the Tactical Intelligence Targeting Access Node (TITAN) program into its production phase. As defense strategies increasingly pivot toward Multi-Domain Operations (MDO) and algorithmic warfare, the need for resilient, edge-deployed data processing has become a critical operational mandate to outpace near-peer adversaries. On August 31, 2026, the Army awarded two delivery orders totaling \$192 million to defense technology contractors allocating \$127 million to Palantir Technologies to lead overall system production alongside partners like L3Harris and Sierra Nevada Corporation, and \$65 million to Anduril Industries for critical hardware and shelter integration. Over the next 18 months, this coalition will deliver eight initial production systems, split evenly between TITAN Advanced and Basic configurations, augmenting nine prototype units currently in active testing. Functionally, TITAN serves as an AI-enabled, expeditionary intelligence ground station designed to aggregate multi-sensor data, execute deep sensing processing, and fuse a common intelligence picture directly at the tactical edge.

By automating target recognition and geolocation, the platform drastically compresses sensor-to-shooter timelines a critical capability for executing Long-Range Precision Fires in highly contested, high-velocity operational domains. This milestone follows four years of iterative prototype fielding based on direct operator feedback, addressing the tactical demand for decentralized, high-speed data exploitation capable of functioning amid disrupted communications or electronic warfare environments. For national security stakeholders and defence technologists, the operationalization of TITAN represents a strategic leap in integrating artificial intelligence into kinetic kill chains. It underscores a broader trajectory where multi-domain data fusion, automated targeting, and expeditionary edge computing are no longer conceptual prototypes, but foundational prerequisites for sustaining tactical overmatch, accelerating decision advantage, and maintaining robust cyber-physical resilience in modern conflict.

Read more: <https://cpeisw.army.mil/2026/09/01/army-announces-move-to-production-for-titan/>

American Rheinmetall delivered the first of eight Lynx XM30 prototypes to the U.S. Army to replace M2 Bradley

In a significant milestone for U.S. ground force modernization amidst an increasingly contested geopolitical landscape, American Rheinmetall has delivered the first of eight Lynx XM30 combat vehicle prototypes to the U.S. Army. As near-peer adversaries accelerate the deployment of drones, precision-guided munitions, and electronic warfare (EW) capabilities, the imperative to replace the aging M2 Bradley Fighting Vehicle with a digitally integrated, highly survivable platform has become a central priority for national defense strategy. The delivery initiates rigorous government-led developmental and performance testing under a \$764 million Phase 3/4 Engineering and Manufacturing Development (EMD) contract. Operationally, the XM30 introduces critical technological leap-aheads, featuring a modular open systems architecture designed for rapid payload insertion and the platform's first-ever hybrid-electric powertrain to optimize battlefield mobility and onboard power generation.

The remaining seven prototypes, slated for delivery later this year, will bypass traditional protracted acquisition timelines to support the Army's Transformation in Contact (TiC) 2.0 initiative, transitioning directly into active field maneuvers and large-scale combat simulations. This expedited, parallel evaluation is sustained by a resilient, multi-state production pipeline spanning turret fabrication in Plymouth, Michigan, to final chassis integration in Slidell, Louisiana coordinated by an elite industrial consortium known as Team Lynx, which integrates specialized capabilities from Textron Systems, Raytheon, L3Harris Technologies, Allison Transmission, and Anduril Industries. For defense planners, risk managers, and national security stakeholders, this deployment signals a critical paradigm shift in military procurement and cyber-physical readiness. By demonstrating that the U.S. Defense Industrial Base can strip years off legacy development cycles and deliver software-defined, networked combat systems at the speed of operational relevance, the XM30 program hardens strategic resilience. It ensures that infantry formations will possess the adaptability, secure connectivity, and power required to maintain tactical overmatch in complex, multi-domain conflict environments.

Read more: <https://www.rheinmetall.com/en/media/news-watch/news/2026/09/2026-09-01-american-rheinmetall-delivers-first-lynx-xm30-combat-vehicle-prototype-to-us-army>

People's Republic of China (PRC) | China

China achieves 98% transmission efficiency in single quantum router breakthrough

Contemporary quantum computing development faces significant engineering bottlenecks, specifically concerning error accumulation and operational complexity during data transmission in quantum random access memory (QRAM). Addressing this limitation, Chinese researchers including Origin Quantum Computing Technology Co. have successfully tested a coherent quantum routing system for bucket-brigade QRAM on China's third-generation superconducting quantum computer, the Origin Wukong. This breakthrough occurs against the backdrop of escalating global competition for quantum supremacy, where mastering scalable QRAM is essential for advancing quantum search algorithms and quantum machine learning, capabilities that could ultimately disrupt cryptographic standards and accelerate AI development.

During testing, researchers deployed three independent quantum routers and a two-layer routing network directly onto the Origin Wukong hardware. Results demonstrated that a single quantum router achieved up to 98% information transmission efficiency with an average fidelity of 94.8% in random-access tests, while the two-layer network maintained a 93% overall transmission efficiency with 82.4% fidelity. Crucially, this system mitigates the scalability issues of conventional designs, which typically demand a prohibitive number of standard quantum gates that geometrically increase circuit depth and accumulated errors. By tapping into additional energy levels of superconducting qubits rather than simply adding more physical qubits, this architecture effectively shortens critical operation paths and optimizes individual node efficiency. For risk managers, national security analysts, and cryptographic defenders, this milestone signals that China's quantum program is pivoting from merely maximizing physical qubit counts to refining the architectural efficiency and real-world functionality of complex quantum systems. While significant hurdles in error correction, hardware stability, and cryogenic operating requirements persist

before large-scale QRAM commercialization, this advancement functionally compresses the timeline toward achieving cryptographically relevant quantum computing. This necessitates that organizations prioritize the adoption of quantum-resistant algorithms and robust post-quantum cryptographic (PQC) transition strategies to protect sensitive data infrastructures against future decryption threats.

Read more: <https://www.globaltimes.cn/page/202609/1369709.shtml>

China unveils world's first simulation and verification platform for lunar satellite navigation and positioning

As the geopolitical race to establish permanent lunar infrastructure accelerates, researchers from China's Guangdong University of Technology (GDUT), in coordination with state-backed aerospace entities including the Deep Space Exploration Laboratory and the China Academy of Space Technology, have unveiled the world's first high-precision simulation and verification platform for a lunar satellite navigation system. Against the backdrop of an impending shift toward large-scale, sustained lunar operations most notably China's ambition to construct the International Lunar Research Station (ILRS) by 2035 the ability to establish reliable positioning, navigation, and timing (PNT) services in a non-terrestrial environment has become a critical strategic capability. Because engineers cannot physically validate navigation technologies in a real-world lunar setting, this integrated virtual testing ground fills a vital gap. Operationally, the platform simulates lunar-orbit satellite trajectories and evaluates joint satellite-ground-station and surface base-station positioning architectures. It provides end-to-end verification, from scenario modelling and observation data generation to algorithm validation and real-time performance evaluation, utilizing 3D dynamic scene displays and statistical error analysis.

This development is technically pivotal for testing the complex architectures needed to coordinate continuous surface exploration, autonomous robotic swarms, and crewed missions across vast lunar operational zones. For the defence, space policy, and risk management communities, this milestone represents a significant leap in China's deep-space infrastructural maturity. By establishing foundational PNT testing capabilities, China is moving aggressively to dictate the technical standards and

operational cadences of future lunar activity. The creation of such a platform not only mitigates the inherent technological risks of deploying untested navigation constellations but also reinforces Beijing's broader strategic objective to achieve technological autonomy and assert dominance in the next frontier of international space competition and multi-domain operations.

Read more: <https://www.globaltimes.cn/page/202609/1370097.shtml>

Republic of Korea (ROK) | South Korea

SK Hynix Breaks Ground on Indiana Fab... “Annual Production of Hundreds of Thousands of HBM Units”

In a strategic manoeuvre reshaping the geopolitical and technological risk landscape, South Korean semiconductor giant SK Hynix has officially broken ground on a \$4 billion advanced packaging facility in West Lafayette, Indiana, marking a pivotal effort to secure the hardware supply chains underpinning next-generation artificial intelligence. As nation-states increasingly recognize critical technology dependencies as potential vectors for systemic disruption, establishing a trusted, domestic pipeline for AI infrastructure has become a paramount defensive priority for the United States. Backed by up to \$450 million in grants and \$500 million in loans via the CHIPS and Science Act, the Indiana fab represents the first U.S.-based production node for High Bandwidth Memory (HBM) a foundational component for advanced AI accelerators, including Nvidia's cutting-edge Vera Rubin architecture. The facility is designed to handle the critical post-processing and advanced packaging of DRAM wafers manufactured in Korea, projecting an annual output of hundreds of thousands of HBM units upon reaching mass production in the second half of 2029.

Operationally, the site will advance current architectures, such as the 12-stack 6th-generation HBM4, while co-driving research and development for 7th-generation (HBM4E) technologies alongside Purdue University to integrate leading engineering talent. For cybersecurity analysts, risk managers, and national policy stakeholders, this infrastructure expansion extends far beyond standard economic development; it directly mitigates severe hardware-level supply chain vulnerabilities linked to the geographic over-concentration of semiconductor manufacturing in East Asia. By onshoring the advanced packaging of memory modules indispensable to

high-performance computing, the U.S. significantly hardens its strategic technological base, insulating future AI-driven cyber defence, corporate operations, and national security capabilities from adversarial coercion or physical supply chain severance.

Read more: https://news.sbs.co.kr/english/article.do?news_id=N1008725857

Russian Federation | Российская Федерация, Rossiyskaya Federatsiya

Russian “Planshet-A” and “Prometey” systems caused a stir among visitors at the Egypt Airshow

Amid an accelerating global arms race centered on battlefield automation and compressed kill chains, Russian state-owned defense conglomerate Rostec specifically its High-Precision Systems holding and VNII Signal is aggressively marketing its combat-tested autonomous command-and-control (C2) and robotics platforms to international buyers. Showcased recently at the El Alamein International Airshow 2026 in Egypt, the export push of the “Planshet-A” automated fire control system and the “Prometey” remote-control architecture highlights a critical shift in the tactical technology landscape: the modular retrofitting of legacy kinetic assets into networked, semi-autonomous platforms. As modern conflicts increasingly rely on drone-integrated artillery and rapid counter-battery warfare, these software-defined enhancements offer state actors a cost-effective method to multiply lethality without procuring entirely new hardware fleets.

The portable “Planshet-A” system functions as a decentralized tactical node, directly interfacing with reconnaissance drones to automate targeting for multiple launch rocket systems (MLRS), howitzers, and mortars. By algorithmically optimizing firing solutions, it drastically reduces the time from target acquisition to payload delivery while minimizing ammunition expenditure. Concurrently, the “Prometey” software and hardware complex operates as a plug-and-play autonomous operating system capable of converting standard manned vehicles such as the MGR-4 “Shmel” demining unit and heavy logistics trucks into remote-controlled robotic assets. For defense planners, intelligence analysts, and electronic warfare (EW) practitioners, the global proliferation of these systems represents a significant escalation in asymmetric threat

capabilities. The integration of legacy military platforms with sophisticated, drone-linked C2 software severely compresses reaction windows for defenders and necessitates a strategic pivot toward robust electromagnetic spectrum operations. Defeating these systems will increasingly require disrupting the telemetry, C2 data links, and sensor-to-shooter networks that underpin architectures like Planshet-A and Prometey, making electronic warfare as critical as kinetic interception in neutralizing next-generation ground threats.

Read more: <https://www1.ru/en/news/2026/09/09/planset-a-i-prometey-vyzvali-interes.html>

Middle East | West Asia

Turkiye's ASELSAN TOLUN Munition Family Demonstrates Versatile Deep-Strike Capabilities

Amid an accelerating global shift toward sovereign precision-strike capabilities and resilient unmanned architectures, Turkish defense prime ASELSAN recently conducted a landmark live-fire demonstration of its TOLUN deep-strike munition family. Executed from a Bayraktar AKINCI unmanned combat aerial vehicle (UCAV) at the Konya Karapınar Firing Test Range before an international military delegation, the September 1, 2026 event underscored a critical evolution in asymmetric warfare: the democratization of advanced, hardened-target penetration and electronic warfare-resistant payloads. As state actors increasingly deploy GPS jamming and spoofing to degrade adversary targeting, the demand for compact, autonomous munitions capable of surviving contested electromagnetic environments has become paramount. During the operational trials, ASELSAN showcased three distinct variants integrated via its SADAK-4T Smart Quad Rack, which maximizes sortie lethality by allowing multiple independent engagements.

The TOLUN I, equipped with an impact fuze and fragmentation warhead, executed a direct hit on a container target. The TOLUN F leveraged a proximity sensor to engage an armoured personnel carrier, utilizing selectable impact angles and proprietary anti-spoofing software designed to bypass GNSS denial. Finally, the TOLUN P deployed its ASAF-Hard Target time-delayed fuze and penetrating warhead to breach a two-story reinforced concrete structure, detonating precisely at the programmed internal layer. Each variant relies on a unified GNSS/INS guidance architecture fortified by a four-channel CRPA anti-jam antenna, delivering a standoff range

of up to 55 nautical miles from fighter platforms and 31 nautical miles from UAVs. For global defence planners and intelligence analysts, this successful deployment signals a substantial hardening of Turkey's indigenous combat-air ecosystem and its aggressive push into the international arms export market. By proving that mid-tier UCAVs can reliably execute deep-strike, anti-bunker missions historically reserved for heavy fighter aircraft, ASELSAN is fundamentally altering the tactical risk calculus and lowering the barrier to entry for advanced standoff lethality.

Read more: <https://www.aeromagasia.com/news/uav/aselsan-tolun-deep-strike-demo>

Malware & Vulnerabilities

Death by a Thousand PaperCuts: AI-Driven Exploitation at Scale

A sophisticated exploitation campaign targeting internet-facing PaperCut servers is demonstrating how threat actors are operationalizing artificial intelligence not just for code generation, but to scale the entire attack lifecycle. Blackpoint Cyber's Adversary Pursuit Group (APG) recently disrupted an attack leveraging two critical PaperCut vulnerabilities: CVE-2026-81578 (unauthenticated configuration manipulation) and CVE-2026-82078 (unsafe database connector behavior leading to remote code execution). Post-incident analysis traced the activity back to exposed operator infrastructure (45.142.193[.]132), which revealed a highly organized, AI-assisted development project rather than a simple script-kiddie operation. The recovered directories containing target lists, multithreaded scanning tools, and timestamped state files read like persistent coding agent memory logs, capturing an iterative workflow managed by tools like Hindsight and AionUI.

The AI assistant continuously preserved project context across sessions, tracking vulnerability research (such as diffing patched and unpatched PaperCut builds), proof-of-concept development, target filtering (geolocating and executing country-specific exclusions), failure analysis, and retry logic. The campaign managed a target set exceeding 500 systems, utilizing tooling capable of processing up to 200 concurrent targets and cycling failed attempts through as many as 100 retry rounds while preserving successful footholds. Notably, when automated scans encountered performance blockers, the AI context

engine recorded user interruptions and proposed engineering optimizations, such as deploying a pre-filter to bypass systems lacking a PaperCut footprint. This discovery is a watershed moment, showing that the most significant impact of AI in cybercrime is the drastic reduction of human engineering effort required to debug, classify, and retry exploitation across hundreds of targets simultaneously. For defenders, this signals an era where opportunistic attacks operate with the efficiency of mature software development pipelines, reinforcing the critical need for rapid patch deployment, strict attack surface management, and AI-resilient detection capabilities capable of matching automated, highly iterative exploitation at scale.

Read more: <https://blackpointcyber.com/blog/death-by-a-thousand-papercuts-ai-driven-exploitation-at-scale/>

Mini Shai-Hulud's Latest Wave: 280 New Places It Hunts for Your Secrets

A resurgence in the abuse of the Node.js runtime environment is allowing threat actors, including initial access brokers linked to prominent ransomware syndicates, to evade detection and establish robust persistence on victim networks. According to recent intelligence, actors such as Woodgnat (aka KongTuke) a group historically tied to ransomware families like Qilin, Akira, Black Basta, and Rhysida have adopted this “living-off-the-trusted-land” technique to compromise targets spanning government, technology, and financial sectors across the U.S. and Asia. The tactical shift leverages the fact that node.exe is a legitimate, cryptographically signed developer tool. Rather than dropping conventional malicious binaries that trigger signature-based security controls, attackers download the official Node.js installer directly from nodejs.org and use it to execute malicious logic hidden within interpreted JavaScript or bytecode. In a documented intrusion at an Asian technology firm, attackers utilizing “ClickFix” lures initially failed to deploy AdaptixC2 and Cobalt Strike payloads due to active blocking.

Pivoting to the Node.js technique, they successfully launched a persistent implant configured to contact Ethereum blockchain gateways (eth.llamarpc[.]com and mainnet.gateway.tenderly[.]co). This “EtherHiding” method allows the malware to retrieve commands or secondary payloads covertly from

blockchain smart contracts. In a parallel attack on a U.S. fintech company sharing the same command-and-control infrastructure (datalayerservice[.]com), the actors deployed a Rust-based backdoor known as C2Looper. This escalating abuse of trusted runtime environments highlights a significant challenge for enterprise defenders, as malicious code execution blends seamlessly with benign developer activity. To counter this threat, organizations must implement strict application control policies to restrict unauthorized use of developer tools like Node.js on non-developer endpoints, enhance behavioral monitoring of registry modifications for persistence mechanisms (such as abnormal Run key entries calling node.exe), and deploy advanced network heuristics to detect anomalous outbound traffic to blockchain RPC gateways.

Read more: <https://blog.gitguardian.com/keyv-mini-shai-hulud/>

Node.js: Old Technique Makes a Comeback

A resurgence in the abuse of the Node.js runtime environment is allowing threat actors, including initial access brokers linked to prominent ransomware syndicates, to evade detection and establish robust persistence on victim networks. According to recent intelligence, actors such as Woodgnat (aka KongTuke) a group historically tied to ransomware families like Qilin, Akira, Black Basta, and Rhysida have adopted this “living-off-the-trusted-land” technique to compromise targets spanning government, technology, and financial sectors across the U.S. and Asia. The tactical shift leverages the fact that node.exe is a legitimate, cryptographically signed developer tool. Rather than dropping conventional malicious binaries that trigger signature-based security controls, attackers download the official Node.js installer directly from nodejs.org and use it to execute malicious logic hidden within interpreted JavaScript or bytecode. In a documented intrusion at an Asian technology firm, attackers utilizing “ClickFix” lures initially failed to deploy AdaptixC2 and Cobalt Strike payloads due to active blocking. Pivoting to the Node.js technique, they successfully launched a persistent implant configured to contact Ethereum blockchain gateways (eth.llamarpc[.]com and mainnet.gateway.tenderly[.]co).

This “EtherHiding” method allows the malware to

retrieve commands or secondary payloads covertly from blockchain smart contracts. In a parallel attack on a U.S. fintech company sharing the same command-and-control infrastructure (datalayerservice[.]com), the actors deployed a Rust-based backdoor known as C2Looper. This escalating abuse of trusted runtime environments highlights a significant challenge for enterprise defenders, as malicious code execution blends seamlessly with benign developer activity. To counter this threat, organizations must implement strict application control policies to restrict unauthorized use of developer tools like Node.js on non-developer endpoints, enhance behavioral monitoring of registry modifications for persistence mechanisms (such as abnormal Run key entries calling node.exe), and deploy advanced network heuristics to detect anomalous outbound traffic to blockchain RPC gateways.

Read more: <https://www.security.com/threat-intelligence/node-js-returns-ransomware>

GitSpawn: A Single Flaw Lets Untrusted Repos Run Code in Claude Code, Codex, Cursor, and Grok

A systemic vulnerability dubbed “GitSpawn” is exposing developers to zero-click arbitrary code execution across leading AI coding agents, including Claude Code, OpenAI Codex, Cursor, and Grok Build. As AI-assisted development tools see massive adoption, their integration into local environments introduces novel attack surfaces where traditional security controls, such as Endpoint Detection and Response (EDR), often fail to distinguish malicious autonomous actions from legitimate developer workflows. Discovered by Manifold Security, the flaw exploits how these command-line agents silently gather project context. To assess the workspace frequently before displaying workspace-trust prompts or requiring user authentication agents execute standard background commands like git status or git diff. Because these subprocesses fail to sanitize local repository configurations, attackers can weaponize configuration sinks such as core.fsmonitor within a maliciously crafted .git/config file. If a target opens an untrusted repository delivered as a complete directory (via a shared .zip or USB drive, which bypasses the inherent sanitization of a standard git clone), the agent’s background index refresh automatically triggers the embedded payload.

This grants the attacker silent, unsandboxed execution with the developer’s full host privileges, immediately

compromising SSH keys, cloud credentials, and local infrastructure. While vendors like OpenAI and Cursor have patched the vulnerability, four of the eight identified variants remain unpatched across tools like Qwen Code, Hermes, Grok Build, and Claude Code’s ultrareview function as of September 2026. This vulnerability underscores a critical paradigm shift in supply chain risk management: as AI agents operate with increasing local autonomy, securing the underlying execution plumbing between the model and the host operating system is just as vital as securing the AI itself. The GitSpawn flaw serves as a stark warning to enterprise defenders that safely adopting autonomous coding tools requires stringent runtime monitoring and zero-trust scrutiny of file handoffs to prevent catastrophic host compromise.

Read more: <https://www.manifold.security/blog/ai-coding-agents-git-hijack>

Infostealers are hijacking Claude accounts at users’ expense

In an escalating trend of adversaries targeting high-value artificial intelligence assets, cybercriminals are leveraging common infostealer malware to hijack Anthropic’s Claude accounts and illicitly consume users’ paid compute capacity. As traditional credential harvesting faces friction from multi-factor authentication (MFA), threat actors are increasingly pivoting to session hijacking, extracting active browser session cookies from compromised endpoints to bypass authentication controls entirely. Recent disclosures from Anthropic reveal that attackers are utilizing these stolen sessions to access authenticated Claude profiles, draining included usage limits and exploiting consumption-based billing features such as usage credits and auto-reload functionality to incur unauthorized charges at standard API rates. The primary motive appears to be the theft of premium AI resources, which adversaries can weaponize at scale to generate sophisticated phishing lures, develop or obfuscate malware, and streamline campaign infrastructure without bearing the operational costs of large language model access.

In response, Anthropic has initiated incident mitigation protocols, forcibly terminating compromised sessions, stripping saved payment methods from affected accounts, and refunding unauthorized transactions while advising users to conduct rigorous endpoint remediation. This development underscores a critical shift in the broader

cyber risk landscape: as generative AI becomes a foundational tool for both enterprise productivity and malicious operations, the digital identities and active sessions gating these models are now prime targets. For defenders and policy stakeholders, this activity highlights the diminishing efficacy of standard MFA against endpoint-level compromises and reinforces the imperative for robust endpoint detection and response (EDR), continuous behavioral session validation, and strict financial guardrails on API consumption to protect against resource exhaustion and downstream infrastructural abuse.

Read more: <https://www.malwarebytes.com/blog/news/2026/09/infostealers-are-hijacking-claude-accounts-at-users-expense>

China-Aligned Hackers Hide PeckBirdy Malware C2 Inside Casino and Adult Websites

In a sophisticated evolution of defense evasion tactics, China-aligned threat actors are increasingly weaponizing low-quality, Chinese-language casino and adult websites as operational cover to conceal command-and-control (C2) infrastructure for the PeckBirdy malware framework. Operating against a backdrop where illegal online gambling and “scambling” sites comprise millions of domains across Southeast Asia, these state-linked actors are exploiting systemic defensive blind spots, blending espionage-oriented communications into high-volume, nuisance-level internet traffic. Building on previous discoveries by Trend Micro regarding PeckBirdy’s targeting of Asian government, education, and financial entities, a recent Infoblox investigation details how operators employ the flexible JScript-based framework to achieve remote JavaScript execution and modular backdoor delivery (such as MKDOOR and HOLODONUT) via living-off-the-land techniques. The attack chain leverages domains like the decoy casino site vip311[.]cc that embed JavaScript connecting to C2 nodes via WebSocket communications, effectively registering service workers that bypass conventional web scanning and reputation filters.

By rotating through disposable infrastructure with zero to minimal VirusTotal detections, the campaign demonstrates a high degree of operational security designed to circumvent automated blocking. The strategy highlights a critical vulnerability in standard enterprise network monitoring, where security teams often dismiss gambling or adult traffic as mere policy

violations rather than investigating the underlying DNS, JavaScript, or network behavior. For cyber defenders and risk managers, this development underscores the diminishing efficacy of static domain blocking and the urgent need for advanced DNS telemetry analysis, proxy log inspection for service-worker delivery, and behavioral correlation of outbound WebSocket activity. Ultimately, it signals a strategic shift where advanced persistent threats co-opt the expansive infrastructure of transnational organized crime, complicating attribution and demanding that analysts treat suspicious, low-reputation web traffic not just as a nuisance, but as a potential indicator of targeted intrusion.

Read more: <https://gbhackers.com/peckbirdy-malware-c2/>

Critical File-Upload Validation Flaw (CVE-2026-14894) Sparks 440k Exploit Attempts on WordPress Super Forms Plugin

A massive exploitation campaign is currently targeting a critical remote code execution (RCE) vulnerability in the WordPress Super Forms plugin, underscoring the rapid weaponization of third-party web components by opportunistic threat actors. Tracked as CVE-2026-14894 and carrying a severity rating of CVSS 9.8, the flaw stems from a missing file-type validation mechanism within the Super Forms Drag & Drop Form Builder. This severe architectural oversight permits unauthenticated attackers to bypass standard security controls and upload arbitrary executable files directly to the host server, predictably leading to complete system compromise. The exploitation activity coincides with a related RCE vulnerability affecting Elementor Pro, compounding the exposed attack surface across the vast WordPress ecosystem. Threat actors have aggressively capitalized on these weaknesses, generating over 440,000 recorded exploit attempts in the wild a surge directly accelerated by the public circulation of proof-of-concept (PoC) exploit scripts.

This high-volume, automated targeting highlights a broader trend where unpatched or unmanaged content management system (CMS) plugins serve as reliable ingress points for initial access brokers and botnet operators. To disrupt this activity, enterprise defenders must immediately deploy vendor-issued patches for all affected versions of Super Forms and Elementor Pro. Furthermore, security engineering teams should enforce strict file-type allow-lists at

the application and web-server layers, explicitly block script execution within upload directories, and leverage software composition analysis (SCA) to maintain real-time visibility into plugin inventories. Routing detailed file-upload telemetry into a SIEM for anomaly detection is equally critical for identifying post-exploitation behaviour. Ultimately, this intense wave of automated attacks reinforces the strategic necessity of continuous third-party component monitoring and rigorous supply-chain hygiene, demonstrating that proactive vulnerability management and defence-in-depth configurations remain fundamental to preserving operational resilience and satisfying compliance mandates in a highly aggressive cyber threat landscape.

Read more: <https://www.verisq.ai/intelligence/over-440-000-exploit-attempts-target-super-forms-and-elementor-pro-rce-flaws-58660>

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.