CLAWS Newsletter

Cyber Index | Volume II | Issue 12

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

India's Tomahawk: DRDO conducts successful flight-test of indigenously-developed Long Range Land Attack Cruise Missile

In a significant advancement for regional deterrence, India's Defence Research and Development Organisation (DRDO), alongside the Aeronautical Development Establishment (ADE) and domestic industrial partners, successfully flight-tested its indigenously developed Long Range Land Attack Cruise Missile (LRLACM) from Dr. APJ Abdul Kalam Island. This successful deployment enters the geopolitical landscape amid escalating maritime tensions in the Indo-Pacific and a shifting global security paradigm, where indigenous long-range strike capabilities are paramount for reducing foreign military dependencies. Often described as India's equivalent to the American Tomahawk, the LRLACM is a subsonic, low-flying cruise missile designed as an upgraded successor to the older Nirbhay programme. The latest operational test verified the weapon system's core capabilities, demonstrating precise waypoint navigation and pinpoint precision while manoeuvring across multiple altitudes and speeds to strike land targets at ranges extending up to 1,500 kilometres

Monitored by the Integrated Test Range in Chandipur using an array of tracking instruments, the mission successfully validated the platform's advanced guidance systems, radar signatures, and low-altitude propulsion technologies. For defence decision-makers and regional planners, this development significantly expands the Indian Air Force and Navy's power-projection capabilities, enabling low-observable, deep-penetration strikes that can bypass sophisticated adversary air defence networks. Ultimately, the successful flight test underscores a broader pattern of accelerated military modernization and cyber-physical systems resilience within South Asia, forcing tactical shifts in risk management and establishing a highly capable, self-reliant precision-strike baseline that fundamentally alters the strategic balance across the contested maritime and terrestrial frontiers.

Read more: https://timesofindia.indiatimes.com/india/indias-tomahawk-drdo-conducts-successful-flight-test-of-indigenously-developed-long-range-land-attack-cruise-missile/articleshow/131747584.cms

Indian Army, Zoho sign MoU to advance indigenous digital transformation under JAI mission

The Indian Army and homegrown enterprise software major Zoho Corporation have signed a strategic Memorandum of Understanding (MoU) to accelerate the military's indigenous digital transformation. Executed by Lieutenant General Harsh Chhibber, Director General Information Systems, and Rajendran Dandapani, Zoho's Director of Engineering, this partnership is anchored under the broader Jointness, Atmanirbharta, and Innovation (JAI) mission a strategic framework championed by Prime Minister Narendra Modi to modernise the country's defense architecture. This development arrives amid escalating global geopolitical tensions and a heightened technological risk landscape, where state-sponsored threat actors and Advanced Persistent Threats (APTs) increasingly target critical defense infrastructure, making sovereign control over codebases and digital supply chains a national security priority for defenders.

Factually, the collaborative framework mandates application-oriented research and development focused on creating highly secure, sustainable, and custom-built digital solutions alongside dedicated technology skill development within the armed forces. Operationally, the initiative aims to systematically phase out dependencies on vulnerable foreign enterprise platforms by establishing an insulated, indigenously engineered software baseline designed to secure sensitive data assets and defence networks. By mitigating the structural vulnerabilities inherent in third-party international software vendors such as hidden backdoors or weaponized supply chain exploits the enterprise directly addresses the threat of digital espionage. For security analysts and risk managers, the broader implications of this defence-industry fusion signal a decisive pivot toward strategic cyber resilience and technological self-reliance. By embedding proprietary, localized defences within the military's operational core, India is establishing a robust security blueprint capable of withstanding sophisticated electronic warfare and cyber-kinetic disruptions, effectively reshaping the balance of digital deterrence in South Asia.

Read more: https://www.fortuneindia.com/business-news/indian-army-zoho-sign-mou-to-advance-indigenous-digital-transformation-under-jai-mission/144573

India And Thailand Agree to Deepen Defence Cooperation

In a strategic move to fortify regional security architectures, the defence ministries of India and Thailand successfully concluded their 10th Defence Dialogue in Bangkok, agreeing to deepen bilateral collaboration across military manufacturing, joint research, innovation, and capability development. Co-chaired by India's Joint Secretary of the Ministry of Defence, Satyajit Mohanty, and Thailand's Deputy Permanent Secretary for Defence, Admiral Nuttapol Diewvanich, this high-level diplomatic alignment unfolds amidst escalating geopolitical friction and a volatile cyber-physical threat landscape in the Indo-Pacific. For security defenders and policy stakeholders, tracking these defence pacts is increasingly critical; modern statecraft dictates that physical military collaborations are invariably paired with digital supply chain interdependencies, rendering joint manufacturing and research hubs lucrative targets for Advanced Persistent Threats (APTs) and state-sponsored espionage operations seeking to exfiltrate proprietary technologies.

Factually, the dialogue established operational vectors to expand military-to-military engagements, maritime security cooperation, and capacity-building frameworks, while leveraging multilateral platforms such as the Association of Southeast Asian Nations (ASEAN) defence mechanisms. Technical implementation is anticipated to involve shared protocols for tactical communications, cross-border training data exchanges, and aligned logistics frameworks for co-production initiatives. From a risk management perspective, the broader implications of this defence fusion underscore a concerted pivot toward localized, cooperative resilience designed to counterbalance asymmetric regional assertiveness. As India and Thailand synchronize their defence-industrial bases, corporate and national security analysts must anticipate strict new cybersecurity compliance baselines to safeguard joint research repositories from sophisticated supply-chain compromises, highlighting how traditional geopolitical stabilization efforts are now inextricably linked to the broader imperatives of global cyber resilience and digital sovereignty.

Read more: https://newsonair.gov.in/india-and-thailand-agree-to-deepen-defence-cooperation-in-manufacturing-research-and-innovation-during-10th-defence-dialogue/

External

Global Focus Brief

Redeploying Fable 5

Artificial intelligence safety framework protocols face a critical evolutionary inflection point following Anthropic's restoration of its frontier models, Claude Fable 5 and Mythos 5, which were abruptly sidelined due to immediate-effect U.S. government export control directives. The regulatory freeze was triggered after Amazon researchers discovered a prompt injection jailbreak that bypassed Fable 5's defensive guardrails, enabling the model to identify software vulnerabilities and generate functional exploit demonstration code. This incident highlights a mounting geopolitical and technological risk landscape where highly capable LLMs possess dual-use capabilities that could drastically accelerate offensive cyber operations if compromised. In response to the June 12 suspension, Anthropic deployed an engineered safety classifier that mitigates the specific exploit-generation prompt sequence in greater than 99% of tested cases, enforcing a broadened "safety margin" designed to catch ambiguous prompts at the expense of elevated false positives for benign developer workflows. Crucially, the mitigation efforts revealed that the vulnerability discovery behaviour was not unique to Fable 5; cross-model analysis confirmed identical exploit generation capabilities across baseline models, including Claude Opus 4.8, GPT-5.5, and Kimi K2.7.

Recognizing the lack of standard triage metrics like the traditional Common Vulnerability Scoring System (CVSS) for AI systems, Anthropic, alongside industry stakeholders Amazon, Microsoft, and Google, has

proposed a consensus AI jailbreak severity framework based on four distinct pillars: capability gain, breadth of task application, ease of weaponization, and discoverability. Furthermore, Anthropic is formalizing pre-release government access and establishing 24/7 monitoring channels via a new Hacker One bug bounty program. Ultimately, this operational disruption underscores that the boundary between routine cyber defence and weaponized AI utility remains profoundly fluid, requiring enterprise risk managers to shift from passive trust models toward rigorous, automated verification of LLM output constraints to preserve institutional resilience.

Read more: https://www.anthropic.com/news/redeploying-fable-5

Beyond Claude Code: the Chinese AI tools poised to benefit after back-door alert

The global cyber threat landscape has entered a highly militarized phase of automated warfare following the unveiling of "Yitian Tulong," a dual-model artificial intelligence framework developed by Chinese cybersecurity giant 360 Security Technology. Introduced by founder Zhou Hongyi at the ISC.AI 2026 conference in Beijing, the platform represents China's direct strategic counterweight to Anthropic's restricted Claude Mythos system. This development unfolds within an intensifying geopolitical risk landscape defined by severe U.S. chip export controls and aggressive techno-nationalism, driving Beijing to establish what it explicitly frames as a "cyber-nuclear deterrent" to prevent a state of "one-way transparency" where Western offensive AI architectures monopolize vulnerability scanning against Chinese infrastructure. Factually, the Yitian Tulong suite bifurcates offensive and defensive operational logic: the first model, "Tulongfeng," focuses exclusively on machine-speed vulnerability discovery, while the second, "Yitianzhen," automates incident response and defensive orchestration. Operationally, 360 Security claims Tulongfeng has already autonomously flagged 3,432 software flaws, with 105 verified by Chinese authorities.

While admitting a 20% to 30% baseline capability gap in raw compute and model reasoning compared to American frontier systems, the architecture systematically bridges this deficit by discarding the Western "genius hacker" paradigm of relying on a singular massive model. Instead, it utilizes an advanced, multi-agent collaborative framework that integrates lighter open-weight models with proprietary vulnerability databases, security expertise layers, and automated tooling to achieve continuous, high-volume pipeline execution. Ultimately, this industrialization of bug hunting carries profound implications for risk management and international stability; it signals a permanent transition to algorithmic saturation testing, warning enterprise network defenders that traditional patch cycles are fundamentally obsolete against continuous AI-driven exploitation pipelines and mandating a shift toward zero-trust runtime containment and automated, AI-augmented defence logic.

Read more: https://www.scmp.com/tech/tech-trends/article/3360148/beyond-claude-code-chinese-ai-tools-poised-benefit-after-back-door-alert?module=top_story&pgtype=homepage

Anthropic's Fable 5 Disruption Signals a New Era of Aggressive AI Export Controls and Safety Compliance

A high-stakes regulatory showdown between frontier artificial intelligence labs and the U.S. government has intensified following critical policy disclosures surrounding the global suspension of Anthropic's advanced models, Claude Fable 5 and Mythos 5. Made public via commentary by former White House AI advisor and President's AI council co-chair David Sacks, the revelation underscores a volatile technological risk landscape where the rapid dual-use capabilities of frontier models outpace traditional software regulatory frameworks. The administrative friction points to a broader geopolitical dilemma: while private labs rush to deploy next-generation architectures to preserve Western technological dominance, federal security stakeholders increasingly view unrestricted model capabilities specifically advanced automated exploitation and zero-day discovery mechanics as critical vectors for potential national security threats. Factually, the friction culminated on June 12 when the U.S. government issued an immediate export control directive following an Amazon research discovery that revealed a prompt injection jailbreak capable of bypassing Fable 5's safety guardrails

to generate working exploit demonstration code. Sacks clarified that because Fable 5 shares its core engine with the highly restricted defensive cybersecurity model Mythos 5, any structural safeguard failure effectively leaks classified offensive capabilities to unverified entities. Rather than establishing unfeasible real-time nationality verification protocols to comply with the order, Anthropic temporarily suspended global access before deploying a robust safety classifier that neutralizes the specific prompt vulnerability sequence in 99% of tested instances. Ultimately, this confrontation signals a permanent shift in corporate risk management and AI governance, highlighting that regulatory frameworks are transitioning from passive compliance checklists toward aggressive pre-release validation models, forcing enterprise decision-makers to implement rigorous, independent zero-trust validation layers on top of commercial AI outputs to guarantee systemic resilience against sophisticated digital and cognitive vulnerabilities.

Read more: https://x.com/davidsacks/status/2065853007619588171?

Europe's biggest chip equipment company to US: Don't blame us for China getting

The global semiconductor supply chain and international trade perimeters face an unprecedented diplomatic and regulatory rift following sharp accusations from the United States government targeting Dutch chipmaking titan ASML Holding NV. U.S. Commerce Secretary Howard Lutnick and senior administration officials have confronted ASML's leadership with assertions that the firm has not acted in good faith, alleging that proprietary components and specialized transportation equipment related to its premier extreme ultraviolet (EUV) lithography systems have been illicitly exported to China. This dispute escalates a highly volatile technological risk landscape where semiconductor lithography is treated as a foundational pillar of national security. Because ASML maintains a strict global monopoly on the bus-sized EUV systems required to print the sub-7-nanometer silicon architectures powering advanced artificial intelligence and military systems, any leakage of this technology threatens to puncture the multi-layered export controls the U.S. has spent years establishing to contain Beijing's semiconductor capabilities. Mechanically, the U.S. alleges that peripheral infrastructure capable of facilitating EUV transport has crossed into Chinese borders, potentially offering a backdoor for underground acquisition networks or localized engineering replication. ASML has issued a flat denial, releasing an internal crisis dossier detailing that of the 314 operational EUV systems globally, none reside in China.

The firm highlights its robust logical and operational telemetry, which actively monitors system connectivity, alongside strict internal firewalls that isolate China-based personnel from EUV core logic. Compounding the financial stakes, China accounts for roughly 20% of ASML's projected 2026 revenue, driven largely by permissible legacy Deep Ultraviolet (DUV) shipments. Ultimately, this confrontation signals a profound shift for enterprise risk managers and geopolitical analysts; it underscores that technological sovereignty is increasingly enforced through aggressive, extraterritorial compliance mandates like the pending U.S. MATCH Act, warning global technology suppliers that maintaining access to contested markets will trigger relentless regulatory friction and intensive state-level monitoring of physical asset telemetry.

Read more: https://timesofindia.indiatimes.com/technology/tech-news/europes-biggest-chip-equipment-company-to-us-dont-blame-us-for-china-getting-/articleshow/131889900.cms

CL-STA-1062 Targets Southeast Asian Governments and Critical Infrastructure

A sustained cyberespionage campaign targeting Southeast Asian critical infrastructure and government bodies has been exposed following a technical analysis by Palo Alto Networks Unit 42. Attributed to a Chinese-speaking advanced persistent threat (APT) actor tracked as CL-STA-1062 which shares significant overlaps with the cluster UAT-7237 the activity signals a deliberate geopolitical focus on monitoring state-owned enterprises within strategic sectors like energy. This development occurs within a highly volatile regional risk landscape where nation-state adversaries increasingly pair common open-source utilities with tailored, bespoke payloads to blend into enterprise networks while evading standard detection. Factual telemetry indicates that since mid-2025, the threat actor has compromised at least ten distinct regional organizations.

Initial access is achieved either by deploying ASPX web shells onto public-facing web applications or through an AppDomainManager injection chain distributed via a weaponized chrome_setup.zip archive.

Once code execution is established, the loaders communicate with a staging server at 139[.]180[.]134[.]221 to pull down the newly discovered "TinyRCT" backdoor, a lightweight C#/.NET remote access trojan that masquerades as a legitimate Microsoft Visual Studio telemetry component (PerfWatson2.exe). Technically, TinyRCT relies on an environment validation check that terminates execution if run outside %LOCALAPPDATA% to thwart automated sandbox analysis. The backdoor establishes persistent beaconing to a command-and-control (C2) node at 45[.]32[.]113[.]172 using HTTP traffic wrapped in AES-128 encryption in CBC mode. It allows operators to execute arbitrary commands, capture screenshots, and perform file exfiltration, utilizing a built-in self-destruct routine that deletes persistence tasks like forged GoogleUpdater entries to wipe forensic footprints. Ultimately, CL-STA-1062's hybrid operational model highlights a critical paradigm for risk management; enterprise defenders can no longer rely purely on signature-based defenses against masqueraded infrastructure tools like SoftEther VPN or VNT, necessitating a transition toward strict application whitelisting, continuous behavioral monitoring, and zero-trust verification inside localized host directories.

Read more: https://unit42.paloaltonetworks.com/cl-sta-1062-tinyrct-backdoor/

Microsoft Tests DeepSeek-V4 in Copilot Cowork for Lower-Cost, Multi-Model AI

The financial architecture and compliance perimeters of enterprise artificial intelligence are undergoing a profound re-engineering as Microsoft initiates internal testing of a self-hosted iteration of DeepSeek-V4 within its Copilot Cowork productivity suite. Pioneered under Microsoft's broader multi-model strategy inside Microsoft 365 and managed via Azure AI Foundry, the move signals a critical shift in the technological risk landscape, transitioning generative AI from an unmetered feature to a consumption-based, usage-billed utility. This operational pivot addresses the reality facing enterprise defenders and cloud architects: autonomous AI agents executing multi-step reasoning, tool-calling, and cross-platform file manipulation consume vast volumes of tokens, creating an unsustainable inference cost profile when routed exclusively through premium closed APIs.

To establish a cost-efficiency pressure valve and reduce strategic dependence on partners like OpenAI or Anthropic, Microsoft is exploring open-weight models that can execute routine cognitive workflows such as data classification and internal document summarization at a fraction of the cost. However, embedding a model family of Chinese origin directly into the Microsoft 365 environment introduces severe geopolitical vulnerabilities and regulatory friction. The initiative occurs in an environment where federal authorities have demonstrated a willingness to directly restrict model access via national security executive actions, forcing Microsoft to defend its deployment framework. Microsoft's technical mitigation strategy relies on wrapping the open-weight model entirely inside U.S.-hosted Azure compliance perimeters, isolating customer data from external APIs, and binding the deployment to enterprise-grade governance controls via Microsoft Purview and Microsoft Entra. Ultimately, this development alters long-term risk management paradigms; it demonstrates that AI orchestration layers are becoming decoupled from specific underlying engines, warning enterprise risk managers that maintaining robust cyber resilience will require granular administrative switches to log, restrict, and audit model execution by department, workload, and geographic data residency constraints.

Read more: https://windowsforum.com/threads/microsoft-tests-deepseek-v4-in-copilot-cowork-for-lower-cost-multi-model-ai.427104/

United States of America (USA)

U.S. Army contracts with General Atomics for long-range manoeuvring projectile program

In a definitive step addressing the reality of modern electronic warfare, the U.S. Army has awarded General Atomics Electromagnetic Systems (GA-EMS) a pivotal development contract under its Extended Range Artillery Projectile (ERAP) program. This development addresses a critical vulnerability in modern conflict zones, where sophisticated adversarial jamming has repeatedly neutralized standard GPS-guided weapons, creating an urgent demand for precision munitions that can operate autonomously in contested airspace. Strategically positioned alongside competitors BAE Systems and General Dynamics Ordnance and Tactical Systems, the GA-EMS contract advances the XM1155 sub-program to deliver a manoeuvring 155mm sub-caliber projectile capable of striking targets beyond 65 kilometres and potentially exceeding 120 kilometres without traditional rocket assistance. The technical architecture relies on deployable wings that allow the shell to transition into a sustained glide after reaching peak apogee, significantly broadening the kinetic engagement zone.

Crucially for military defenders and cyber-security practitioners, the munition integrates a highly resilient design featuring redundant, non-GPS guidance mechanics such as advanced optical navigation systems engineered specifically to bypass localized radio-frequency interference and cyber-spoofing countermeasures. Aiming for an Initial Operational Capability by fiscal year 2030, with low-rate production slated for 2029, the program utilizes automated fabrication at the GA-EMS Manufacturing Center of Excellence in Tupelo, Mississippi, to ensure baseline scalability. Ultimately, this initiative marks a systemic shift toward cyber-resilient, sovereign defence supply chains, rewriting tactical risk management blueprints by ensuring that long-range precision fires remain lethal and functional even when the broader digital battlefield is completely compromised.

Read more: https://www.hydesmith.senate.gov/us-army-contracts-general-atomics-long-range-maneuvering-projectile-program

The FBI built its own replica small town to simulate real-world cyberattacks

Federal law enforcement training frameworks are undergoing a radical shift from static classrooms to hyper-realistic tactical environments following the public unveiling of the Federal Bureau of Investigation's (FBI) newly expanded "Kinetic Cyber Range" (KCR). Situated at the Bureau's North Campus on the Redstone Arsenal in Huntsville, Alabama, the purpose-built, 22,000-square-foot indoor replica town was engineered by the FBI's Operational Technology Division to counter an unprecedented surge in critical national infrastructure targets. This development comes at a critical juncture in the threat landscape, underscored by the FBI's latest Internet Crime Report revealing that annual domestic cybercrime losses surged 26% to a record $20.9 billion, driven primarily by industrialized ransomware syndicates and state-backed actors leveraging automated AI tools to exploit software vulnerabilities at scale. Operationally, the KCR bypasses abstract theory by placing agents, analysts, and interagency partners including NASA and the U.S. Army directly into eleven fully functional, interconnected target environments.

The mock town features wired residential homes, a hotel, a gas station, a courthouse, a power company, and a functioning hospital network, all linked to a localized data centre running over 200 physical Windows and Linux servers. During high-pressure live-fire simulations, instructors deploy zero-day exploits and ransomware strains to trigger real-time physical disruptions, such as knocking a hospital's clinical systems dark. Trainees are forced to simultaneously crack encrypted internet-of-things (IoT) devices, execute vehicle forensics, trace command-and-control (C2) vectors, and manage the human variables of critical incident response by negotiating with role players acting as corporate executives and legal teams. Ultimately, this infrastructure investment reflects a key maturity phase in risk management and national cyber resilience. By simulating the cascading real-world dependencies of a municipal breach, the FBI is establishing a new baseline for multi-jurisdictional defence, preparing cyber investigators to neutralize highly volatile threats before their downstream societal consequences can manifest in the wild.

Read more: https://techcrunch.com/2026/06/13/the-fbi-built-its-own-replica-small-town-to-simulate-real-world-cyberattacks/

FBI Cleveland, in coordination with Google and Lumen's Black Lotus Labs, conducted a technical takedown operation against Outsider, a Chinese phishing-as-a-service platform (PhaaS)

The FBI Cleveland Field Office, in coordination with the Internet Crime Complaint Center (IC3), has issued an urgent technical alert warning organizations of an escalating operational trend: the weaponization of sophisticated Traffic Distribution Systems (TDSs) by cybercriminal syndicates to execute stealthy ransomware deployment and complex financial fraud. This development marks a significant shift in the cyber threat landscape, as threat actors increasingly pivot away from rigid, easily flagged landing pages toward dynamic, multi-layered redirection infrastructures. By exploiting compromised legitimate websites frequently via outdated Content Management System (CMS) plugins or weak administrative credentials as well as deploying aggressive Search Engine Optimization (SEO) poisoning campaigns, attackers inject stealthy redirect code that seamlessly funnels unsuspecting corporate traffic into the malicious TDS ecosystem.

Operating as an intelligent, context-aware gatekeeper, the malicious TDS evaluates incoming connections in real time, analyzing variables such as geographic location, device fingerprint, browser user-agent, and local software versions. This granular filtering allows the system to distinctively deliver dangerous drive-by malware payloads and highly convincing credential-harvesting pages to valuable enterprise targets, while simultaneously routing security researchers, automated sandbox tools, and corporate network scanners to benign decoy sites to evade detection. To counter these advanced evasion techniques, federal authorities urge network defenders to implement aggressive endpoint and network hardening strategies. Key technical mitigations include modifying default file associations for JavaScript files, continuously auditing hosting and CMS accounts for unauthorized layout alterations, and closely monitoring script execution processes specifically wscript.exe for anomalous outbound web requests. Ultimately, this warning underscores that traditional perimeter firewalls are no longer sufficient against dynamic delivery chains; risk managers must adopt rigorous defense-in-depth frameworks, combining zero-trust network monitoring with offline backup architectures, to cultivate systemic cyber resilience against highly adaptable, evasion-centric threats.

Read more: https://x.com/FBICleveland/status/2067725344258306515

United Kingdom of Great Britain and Northern Ireland

NCSC CEO: Hostile states linked to three-quarters of cyber attacks affecting UK's critical systems

A stark escalation in nation-state activity targeting critical national infrastructure (CNI) has surfaced following a public disclosure by Richard Horne, Chief Executive of the United Kingdom's National Cyber Security Centre (NCSC). Speaking at the Royal United Services Institute (RUSI), Horne revealed that hostile states predominantly Russia, China, and Iran are linked to approximately 75% of all cyber incidents impacting the UK's essential services and supporting ecosystems. This development signals a significant shift in the strategic risk landscape, shifting the primary threat vector away from opportunistic cybercrime toward systemic, conflict-oriented infrastructure positioning. Operationally, the NCSC managed more than 200 CNI-related incidents in the year leading up to May 2026, finding that state-sponsored actors are actively executing "pre-positioning" campaigns. Rather than launching immediate extortion schemes, these adversaries are establishing persistent footholds inside operational technology (OT) and aging legacy frameworks to enable rapid disruption during future geopolitical flashpoints.

This behaviour mirrors known patterns associated with advanced persistent threat groups like China's Volt Typhoon, which focus on low-and-slow infiltration rather than noisy payloads. Adding to the long-term risk profile, NCSC assessments project that by 2028, adversaries will highly likely weaponize artificial intelligence to rapidly discover and exploit zero-day and unpatched flaws in CNI environments. To combat these invisible incursions, the UK government is advancing the Cyber Security and Resilience Bill to legally mandate stringent baseline protections across essential services. Ultimately, the NCSC's shifting directive emphasizes that peace-time operational vulnerability is directly correlated with wartime kinetic risk. Network defenders must transition away from standard competitive benchmarking toward a relentless, continuous validation of defensive postures, treating basic system hardening not as compliance overhead, but as an essential element of

modern deterrence.

Read more: https://www.ncsc.gov.uk/news/ncsc-ceo-hostile-states-linked-to-three-quarters-of-cyber-attacks

Republic of Finland

Finland Charges Russian Captain and Crew Member with Sabotaging Undersea Cables

The physical security of the global internet backbone faces an escalating threat landscape following the formal indictment of the Russian captain and a senior Azerbaijani crew member of the cargo vessel Fitburg by Finland's National Prosecution Authority. The charges, which include "aggravated criminal mischief" and "aggravated interference with telecommunications," stem from an incident on New Year's Eve where the vessel severed two critical undersea telecommunications cables connecting Finland and Estonia in the Gulf of Finland.

This development highlights a mounting geopolitical risk landscape where hybrid warfare tactics blend maritime operations with critical national infrastructure disruption, demonstrating how physical sabotage can sever digital connectivity as effectively as a sophisticated cyberattack. Factually, investigators allege that the defendants intentionally dropped and dragged a damaged anchor across the seabed for over 130 kilometres (80 miles), successfully severing the two primary subsea links and attempting to compromise eight adjacent telecommunications, gas, and electricity lines before being intercepted by the Finnish Border Guard. While the defendants deny the charges and plan a jurisdictional defence noting the damage occurred within Estonia's exclusive economic zone the incident caused immediate infrastructure disruption and underscores the fragility of trans-baltic digital transit paths. Ultimately, this prosecution marks a critical evolution in threat attribution, signalling to network defenders and risk management stakeholders that cyber resilience no longer stops at logical perimeter firewalls; modern defence-in-depth strategies must explicitly account for physical infrastructure vulnerabilities and coordinate with maritime security frameworks to secure the baseline data protocols underpinning international connectivity.

Read more: https://www.themoscowtimes.com/2026/06/15/finland-charges-russian-captain-and-crew-member-with-sabotaging-undersea-cables-a93020

The Kingdom of the Netherlands | Dutch

Netherlands moves to join US-led 'Pax Silica'Chinese expert warns of risks to high-tech competitiveness

The global technology supply chain is undergoing an aggressive structural alignment as the Netherlands moves to formalize its membership in "Pax Silica," a United States-led artificial intelligence and semiconductor supply chain initiative. The integration highlights a shifting geopolitical risk landscape where technology dominance is treated as a core element of national security, transitioning from unilateral export controls toward a highly institutionalized alliance framework. This development carries severe strategic weight for global enterprise risk managers and semiconductor stakeholders, as the initiative aims to build a closed technological bloc designed to explicitly restrict China's access to advanced chipmaking tools and AI semiconductors. The diplomatic escalation crystallized in Washington when Dutch Trade Minister Sjoerd Sjoerdsma signed the Pax Silica declaration with US Commerce Secretary Howard Lutnick, simultaneously raising concerns over the U.S. Match Act a bipartisan bill that could pressure allies into implementing even more stringent compliance perimeters against Chinese semiconductor entities. While Dutch technology giants, most notably ASML, navigate a precarious balancing act between U.S. regulatory alignment and maintaining lucrative access to the massive Chinese market, Chinese state analysts warn that sacrificing technological autonomy to external pressure risks fragmenting the global ecosystem and inflating industrial compliance costs.

Beyond the Netherlands, other prominent European nations, including Germany and Greece, have joined the U.S. tech diplomacy initiative, which is orchestrated by U.S. Under Secretary of State Jacob Helberg. Ultimately, this development underscores that semiconductor supply chains are being heavily weaponized as tools of statecraft; decision-makers must adjust their long-term supply resilience blueprints to account for an era of permanent market balkanization, where access to advanced hardware components and chip manufacturing logic is dictated by strict geopolitical boundaries rather than traditional market forces.

Read more: https://www.globaltimes.cn/page/202606/1364374.shtml

People's Republic of China (PRC) | China

The secret Chinese surveillance programme tracking people like me

A profound expansion of Beijing's domestic tracking capabilities has come to light following cybersecurity and journalistic exposure of a leaked Chinese state intelligence operation known as the "Dynamic Control Platform." Investigated by The Telegraph, this intelligence disclosure marks a major shift in the technological risk landscape, revealing that China's domestic security apparatus has systematically expanded its mass surveillance architecture to comprehensively monitor foreign nationals and designated individuals "of interest" within the country. This development occurs amid heightened geopolitical tensions and global concern over techno-authoritarian data aggregation, signalling to enterprise defenders and international policy stakeholders that traditional data privacy baselines are entirely bypassed when operating within Chinese jurisdiction.

Factually, the leaked data platform acts as a centralized data fusion hub, automatically ingestive of millions of distinct, real-time data points. The technical architecture orchestrates data ingestion from widespread public AI-enabled facial recognition cameras, official immigration and visa registries, financial transaction histories, and hospitality check-in logs. Crucially for intelligence analysts and risk managers, the platform incorporates advanced big-data analytical capabilities, most notably automated relational mapping features. This behavioral pattern tracking maps physical associations in real time, registering who a targeted individual meets with, establishing proximity metrics, and auto-generating alerts when individuals deviate from expected geographic routines or interface with unauthorized cohorts. Ultimately, this structural leak underscores the vanishing boundary between public corporate data and state intelligence assets in highly securitized environments, warning global enterprises that standard operational security (OPSEC) parameters are fundamentally compromised in countries utilizing omnipresent digital tracking, thereby forcing risk management stakeholders to adopt zero-trust deployment protocols and rigorous device isolation strategies for personnel traveling to contested regions.

Read more: https://www.telegraph.co.uk/world-news/2026/05/19/leaked-secret-chinese-surveillance-programme-tracks-foreign/

China-Nexus Actor UNC6508 Infiltrates U.S. Medical and Military Research Networks via REDCap Vulnerabilities

A sophisticated, long-term cyber espionage campaign targeting the North American academic, medical, and military research community has been uncovered by the Google Threat Intelligence Group (GTIG) and its subsidiary Mandiant Consulting. Attributed to the People's Republic of China (PRC)-nexus threat group tracked as UNC6508, the operation highlights an escalating geopolitical trend where state-sponsored actors aggressively plunder advanced medical intelligence, artificial intelligence breakthroughs, and defence-related public health data to bolster domestic strategic sectors. Factually, the intrusion activity dates back to September 2023, with the threat actor maintaining persistent, undetected access inside compromised networks for over a year. The initial compromise vector involved targeting externally facing Research Electronic Data Capture (REDCap) servers, a web application ubiquitous in clinical research. UNC6508 systematically exploited REDCap's architectural design which permits administrators to run legacy software components side-by-side with current versions by executing downgrade attacks against unpatched, legacy modules. Once inside, the group deployed a bespoke, three-part modular malware suite dubbed INFINITERED. This tailored malware trojanized legitimate REDCap system files to intercept authentication traffic, harvesting usernames and passwords from login POST requests and encrypting them inside a local sessions database table tagged with the unique identifier xc32038474a. UNC6508 then utilized these compromised administrative credentials to pivot laterally to internal domain controller accounts.

To evade geographic anomalies, the actors routed all command-and-control (C2) traffic through a covert proxy network utilizing exclusively U.S.-based IP addresses, ultimately exfiltrating data including research on the mosquito-borne Chikungunya virus by manipulating domain content compliance rules. For enterprise risk managers, this campaign

underscores the critical vulnerability of research supply chains and the danger of unmonitored legacy systems; defenders must move beyond standard edge perimeters, enforce mandatory multi-factor authentication across all third-party identity providers, and continuously audit and purge legacy software segments to prevent advanced persistent threats from establishing long-term cognitive and technological persistence.

Read more: https://cloud.google.com/blog/topics/threat-intelligence/prc-targets-us-medical-research

Russian Federation | Российская Федерация, Rossiyskaya Federatsiya

Russia Wants AI Sovereignty. It Has a Chip Problem

The intersection of global technological sovereignty and state-level military modernization faces a critical bottleneck as the Russian Federation attempts to accelerate its domestic artificial intelligence ecosystem while navigating crippling Western hardware sanctions. Spearheaded by the newly established Presidential Commission on AI and supported by Moscow State University's new AI faculty headed by Vladimir Putin's daughter, Katerina Vladimirovna Tikhonova the Kremlin's strategic focus relies on developing homegrown mathematical talent to compensate for a severe post-invasion technical brain drain. However, this human-capital pivot occurs within a highly restricted technological risk landscape defined by a complete lack of advanced semiconductor fabrication facilities and strict international export controls, explaining why achieving true AI autonomy has become a primary survival objective for Russian national security planners. Operationally, the Kremlin is attempting to establish a symbiotic technology pipeline with Beijing to mitigate these hardware deficiencies. In exchange for advanced Chinese AI chips and dual-use microelectronics, Moscow is leveraging its extensive, real-time kinetic battlefield data accumulated during the ongoing conflict in Ukraine a highly valuable asset for a Chinese military that has not fought a major ground war in decades and desperately requires raw data to train its own offensive AI and autonomous weapons models.

Despite these alignment efforts, semiconductor market realities complicate Russia's digital strategy, as domestic Chinese chip fabricators barely satisfy internal demand, placing the Kremlin lower on Beijing's customer hierarchy than regions where China is directly contesting U.S. influence. Ultimately, this development carries profound implications for international stability and cyber resilience; it demonstrates that under intense sanctions, adversarial states will actively trade tactical physical warfare telemetry for computational infrastructure, warning risk management stakeholders that long-term defensive blueprints must focus on choking underground chip-smuggling networks and monitoring dual-use hardware supply lines to prevent the emergence of localized, sanctions-resistant military AI capabilities.

Read more: https://time.com/article/2026/06/18/russia-ai-putin-chip-us-china/

The French Republic | République française

Renault teams up with Thales to boost France's drone production

In an era defined by a shift toward a "wartime economy" and rapidly evolving electronic warfare tactics, the French Ministry of the Armed Forces has catalyzed a major defence manufacturing pivot by bridging traditional automotive infrastructure with advanced military engineering. Unveiled at the Eurosatory defence fair, automaker Renault Group and defence technology leader Thales have entered into a strategic partnership to mass-produce the Toutatis short-range loitering munition, signalling a critical push to secure a sovereign, highly resilient drone supply chain within Europe. This development directly addresses the stark supply pressures and electronic combat lessons emerging from the conflict in Ukraine, where traditional, low-volume defence manufacturing cycles have failed to keep pace with operational attrition. Under this agreement, Renault will leverage its high-volume automotive production expertise to overhaul Thales' current manufacturing methods, transitioning from low-capacity 3D printing to large-scale plastic injection moulding, which will slash the drone's components and fasteners by 40% to significantly optimize unit costs.

The Toutatis loitering munition is structurally engineered for high-intensity battlefields, featuring an operational range of 10 to 30 kilometres, a mission-configurable warhead capable of neutralizing combat vehicles, and scalable swarm capabilities that adapt dynamically to evolving ground theatre requirements. Crucially for modern cyber defence

and electronic warfare specialists, the platform integrates robust resistance against electromagnetic jamming while retaining a strict human-in-the-loop decision architectural framework to ensure precision command and control. Slated to begin production as early as 2027, the collaboration aims to rapidly scale output to 1,000 units per month from its first year of operation. Ultimately, this integration of commercial industrial capacity with advanced defence technologies establishes a new precedent for cyber-resilient autonomous systems, reinforcing European military self-reliance and providing a scalable blueprint for defence-industrial mobilization against sophisticated electronic and kinetic threats.

Read more: https://www.reuters.com/business/aerospace-defense/renault-make-drones-with-thales-support-french-defence-sector-2026-06-16/

New report raises concerns over Russian propaganda spread by Europe's flagship AI company Mistral

European digital sovereignty initiatives face a critical security vulnerability following independent research revealing that large language models developed by Mistral AI, Europe's premier artificial intelligence champion, are highly susceptible to amplifying Russian state-sponsored disinformation. Conducted by Estonian threat intelligence researchers and supported by a parallel audit from NewsGuard, the discovery injects severe geopolitical risk into the enterprise technology landscape. This development comes as European Union bodies and domestic organizations aggressively seek "sovereign" AI alternatives to minimize reliance on U.S. Big Tech, inadvertently opening a backdoor for adversarial cognitive operations and narrative warfare. Factually, testing of Mistral's most advanced generative model architecture ranked the system 47th out of 60 global models scrutinized, with its guardrails scoring below 40% in filtering out malicious propaganda.

Specifically, audits of Mistral's consumer-facing chatbot, Le Chat, revealed that the system repeated state-sanctioned falsehoods regarding the Russia-Ukraine conflict and broader regional conflicts up to 50% of the time in English prompts, and exceeding 56% in French-language queries. This failure profile contrasts sharply with commercial American models like Anthropic's Claude and Grok, which maintained significantly higher filtering thresholds against foreign influence content. The underlying vulnerability stems from architectural trade-offs in Mistral's open-weights framework and lighter safety alignment margins, which allow malicious actors to exploit lax semantic boundaries during standard prompt execution. Ultimately, these findings pose a profound risk management dilemma for national security and corporate compliance stakeholders; a sovereign model that fails to neutralize hostile information operations ceases to be a defense mechanism, instead functioning as a vector for foreign interference, signaling that true digital independence requires balancing open innovation with rigorous, automated safety classifiers to preserve institutional resilience.

Read more: https://www.euronews.com/next/2026/06/16/new-report-raises-concerns-over-russian-propaganda-spread-by-europes-flagship-ai-company-m

Malware & Vulnerabilities

New Actors Deploy Shai-Hulud Clones: TeamPCP Copycats Are Here

The open-source software ecosystem faces an escalating threat wave as independent copycat actors rapidly deploy unauthorized clones of the notorious Shai-Hulud supply-chain malware. Uncovered by threat intelligence researchers at OX Security, the campaign directly stems from a source code leak published by the original TeamPCP cybercrime group, which ignited an aggressive supply-chain attack competition on BreachForums. This development underscores a broader, highly volatile risk landscape where the proliferation of leaked offensive frameworks lowers the entry barrier for secondary threat actors, allowing them to instantly operationalize complex exfiltration infrastructure against developer environments. Factually, the campaign leverages a cluster of malicious typo-squatting packages published to the npm registry under a single user account, including chalk-tempalte, @deadcode09284814/axios-util, axois-utils, and color-style-utils. A technical breakdown of the chalk-tempalte variant reveals a direct, non-obfuscated implementation of the Shai-Hulud codebase configured to direct exfiltrated tokens and environment variables to a dedicated Command and Control (C2) domain at 87e0bbc636999b[.]lhr[.]life.

Parallel variants uploaded under the same profile demonstrate distinct payload divergence; the axois-

utils package introduces an embedded "phantom bot" compiled in GoLang that establishes persistent local services and functions as a distributed denial-of-service (DDoS) botnet capability. Concurrently, the remaining variants are engineered to target local environment configurations, exfiltrating cryptographic wallets, host geolocation metrics, and cloud credentials (AWS, GCP, and Azure) via network callbacks to 80[.]200[.]28[.]28:2222. Ultimately, the rapid distribution of these functional clones highlights a severe risk management challenge for automated DevOps pipelines. As multi-functional, "vibe coded" threats increasingly bypass traditional static analysis, security teams must reject superficial metadata checks and enforce strict repository drift automation, mandatory code-signing, and continuous network isolation for developer workstations to preserve supply-chain integrity.

Read more: https://www.ox.security/blog/new-actors-deploy-shai-hulud-clones-teampcp-copycats-are-here/

GitHub dismissed security reports on flaws now exploited by supply-chain worm, researchers say

The security posture of major software supply-chain repositories is under scrutiny following GitHub's dismissal of vulnerability reports submitted by Deep Specter Research regarding the "Shai-Hulud" supply-chain worm. This malware, which has been linked to compromises at organizations including the European Commission and Red Hat, exploits fundamental design characteristics of the Git version control system to facilitate sophisticated repository infiltration. Deep Specter's findings highlight two specific mechanisms enabling this activity: the ability for attackers to backdate commit timestamps to mask malicious activity as long-standing, and the manipulation of commit author metadata to impersonate trusted developers. While GitHub categorizes these behaviours as inherent Git properties rather than exploitable vulnerabilities advocating for the adoption of GPG and SSH commit signing the research underscores a dangerous visibility gap.

The platform's user interface often fails to expose the verifiable account identity of the individual who pushed a commit, relying instead on potentially forged metadata, while valid push identity data remains accessible only via an expiring Events API. This discrepancy significantly complicates detection efforts, as attackers leverage these "features" to bypass automated security checks and maintain persistence across thousands of repositories. The incident highlights a critical inflection point for security practitioners: reliance on repository metadata for authenticity is increasingly insufficient. As threat actors continue to weaponize these inherent repository behaviours, the onus falls on organizations to move beyond standard platform-level trust mechanisms and adopt mandatory cryptographic commit signing alongside rigorous, identity-based pipeline verification to preserve supply-chain integrity against a landscape where trusted identities are now a primary attack vector.

Read more: https://therecord.media/github-dismissed-reports-shai-hulud-deep-specter

StrikeShark: investigating a new campaign delivering Cobalt Strike through SharkLoader

A global cyberespionage threat vector has emerged following the exposure of "StrikeShark," an opportunistic campaign delivering a custom, previously undocumented malware family dubbed "SharkLoader." Discovered by threat researchers at Kaspersky's Global Research & Analysis Team (GReAT), the operation targeting critical sectors reflects a highly decentralized risk landscape where adversaries weaponize public proof-of-concept (PoC) exploits alongside custom evasion tools. The observed victimology spans diplomatic entities in Indonesia, government agencies in Taiwan, and software development firms across Hong Kong, Syria, Colombia, and Serbia. Although not definitively attributed to a specific Advanced Persistent Threat (APT) group, the actor is strongly suspected of being Chinese-speaking due to the post-compromise deployment of open-source reconnaissance tools like FScan and Pillager. Factually, the threat actors execute a dual-track infection strategy. Initial access is achieved either via malicious installer droppers and decoy PDFs masquerading as legitimate updates (e.g., Google Update, Cisco AnyConnect) or by exploiting unpatched edge vulnerabilities in internet-facing servers, including Microsoft Exchange (ProxyLogon, CVE-2021-26855) and Openfire (CVE-2023-32315). To establish persistence, attackers deploy web shells to trigger a DLL side-loading chain utilizing the trusted Windows binary SystemSettings.exe (CVE-2021-27076) to load SharkLoader (SystemSettings.dll).

Technically, SharkLoader functions by decrypting

an encrypted payload file (SyncRes.dat), registering a Vectored Exception Handler (VEH) to manage access violations, and utilizing MinHook to inject custom API hooks specifically targeting Sleep functions to bypass memory scanners looking for read-write-execute (RWX) regions before ultimately injecting a Cobalt Strike Beacon. Post-exploitation involves Active Directory enumeration and credential dumping via LSASS and NTDS database targeting. Ultimately, the StrikeShark campaign underscores a critical threat paradigm: corporate defenders cannot rely on traditional indicator-based memory hunting, requiring risk management stakeholders to enforce aggressive edge-patch management, zero-trust network boundary isolation, and continuous runtime behavior monitoring to suppress highly adaptable, modular intrusion sets.

Read more: https://securelist.com/strikeshark-campaign/120326/

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