CLAWS Newsletter

Cyber Index | Volume II | Issue 11

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

Sudarshan Chakra: India develops new multi-layered air shield to stop missiles, drones & Rockets

Amid escalating geopolitical tensions and the rapid proliferation of asymmetric aerial threat vectors observed in theatres like Ukraine and West Asia, the Government of India and its Defence Research and Development Organisation (DRDO) are accelerating the deployment of a comprehensive, defence-in-depth architecture dubbed the "Sudarshan Chakra" project. As regional adversaries specifically China and Pakistan continue to rapidly expand their ballistic and tactical arsenals, the strategic necessity of a multi-tiered mitigation framework has shifted from a supplementary capability to a core pillar of national security. In a pivotal operational milestone on June 10 and 11, 2026, the DRDO successfully executed three consecutive flight tests validating the nation's indigenous Ballistic Missile Defence (BMD) system. The trials successfully demonstrated advanced kinetic interception protocols against both long-range ballistic missiles and medium-range anti-ship targets.

This technological validation builds upon capabilities recently showcased during "Operation Sindoor," where defenders utilized the Akash missile system and long-range effectors to neutralize aerial assets at distances exceeding 300 kilometres. To counter localized, low-altitude intrusion vectors such as the tactical deployment of unmanned aerial systems (UAS) India is concurrently upgrading legacy gun platforms and expediting the rollout of Very Short Range Air Defence (VSHORAD) systems. Furthermore, defensive research is actively pivoting toward directed-energy weapons, including laser-based mitigation tools, to sustainably counter the economic asymmetry of drone swarm tactics. Ultimately, the Sudarshan Chakra initiative represents a strategic convergence of kinetic interception, advanced targeting sensors, and layered redundancy designed to harden critical civilian and military infrastructure against a full spectrum of threats. For security analysts and defence planners, India's pivot toward this fully integrated shield highlights a broader global paradigm shift: modern deterrence now relies as much on localized, multi-layered airspace resilience and rapid neutralization capabilities as it does on traditional offensive posturing.

Read more: https://timesofindia.indiatimes.com/defence/news/sudarshan-chakra-india-develops-new-multi-layered-air-shield-to-stop-missiles-drones-rockets/articleshow/131705864.cms

Bharat Forge Chair Baba Kalyani Reveals Big Semiconductor Bet

As nations race to secure critical technology supply chains amidst mounting geopolitical tensions and hardware dependencies, Indian manufacturing giant Bharat Forge has formally expanded into the global semiconductor ecosystem. Chairman Baba Kalyani announced strategic collaborations with three of the world's largest semiconductor firms to produce specialized components for lithography machines the highly complex, precision equipment essential for advanced chip fabrication. This strategic pivot by a corporation historically anchored in heavy manufacturing and defence systems signals a broader convergence of national security and critical technology infrastructure. The initiative directly aligns with the India Semiconductor Mission (ISM), a multi-billion-dollar state effort aimed at decoupling from volatile foreign import dependencies and establishing sovereign capabilities across the fabrication, testing, and packaging lifecycle. By targeting the lithography supply chain rather than direct semiconductor fabrication, Bharat Forge is positioning itself within the most highly concentrated and technologically exclusive chokepoint of global chip production, an arena traditionally dominated by a narrow set of Western and East Asian suppliers.

This transition is paralleled by the company's aggressive expansion in its defence portfolio, where it is shifting from supplying individual components to delivering complete combat platforms and securing record military orders. For risk management practitioners and policy stakeholders, this development highlights a critical structural shift: traditional defence contractors are increasingly treating foundational digital hardware as a core extension of sovereign security. As India accelerates its transition to a product-driven technological power, integrating legacy defence capabilities into semiconductor supply chains fundamentally enhances regional resilience. Ultimately, this strategic diversification of hardware production nodes away from contested geopolitical hotspots promises to insulate future digital infrastructure from single-point supply chain shocks,

reinforcing the industrial base necessary for long-term cyber, economic, and operational sovereignty.

Read more: https://www.outlookbusiness.com/corporate/bharat-forge-chair-baba-kalyani-reveals-big-semiconductor-bet

K30 Biho deal back on India's air defence cards; Army to place proposal soon - Details

In response to escalating regional volatility and recent cross-border military engagements under Operation Sindoor, the Indian Army is moving to harden its short-range aerospace defenses by reviving the procurement of the South Korean K30 Biho self-propelled air-defense system. Primary actors driving this acquisition include India's Defence Acquisition Council (DAC), Hanwha Aerospace, and domestic manufacturing partner Bharat Forge. Within a geopolitical risk landscape characterized by rapid kinetic escalation and the persistent threat of localized aerial incursions, modernizing mobile counter-air capabilities has become an operational necessity for forward-deployed forces. The primary development centers on the Army's imminent submission for a fresh Acceptance of Necessity (AoN) from the DAC to acquire the Biho platform. Initially cleared in 2021 before negotiations stalled, the K30 Biho features twin 30mm auto-cannons and secondary missile armaments integrated onto highly mobile tracked and wheeled chassis configurations. To mitigate supply chain vulnerabilities and align with "Make in India" domestic production mandates, the procurement leverages Hanwha's established joint venture with Bharat Forge.

While the strategic requirement encompasses roughly 400 systems, the initial AoN targets a smaller, phased deployment. Concurrently, the defense modernization push includes advancing the procurement of 250 Russian Verba MANPADS offering an upgraded 6.5 km engagement range to replace legacy Igla systems and integrating French-made HAMMER smart glide bombs into the Rafale fighter fleet. For national security stakeholders and strategic risk analysts, this acquisition cycle highlights a critical shift toward multi-layered, highly mobile defense architectures capable of mitigating rapid aerial threat vectors. By decoupling from legacy single-source dependencies and embedding foreign technical systems within localized manufacturing ecosystems, India is systematically enhancing its operational resilience, fortifying its defensive posture against cross-border volatility, and reinforcing stability across contested regional theatres.

Read more: https://www.etnownews.com/news/k30-biho-deal-back-on-indias-air-defence-cards-army-to-place-proposal-soon-details-article-154472521

External

Global Focus Brief

The 5 Eyes Intelligence Issues Intelligence Bulletin on China

In a joint intelligence bulletin released by MI5 and the broader Five Eyes alliance, security agencies have detailed an aggressive, large-scale espionage campaign orchestrated by Chinese military intelligence services targeting Western security clearance holders and military personnel. As geopolitical friction in the Indo-Pacific intensifies, the weaponization of professional networking platforms has emerged as a low-friction, high-yield vector for state-sponsored intelligence gathering. This campaign highlights a strategic shift where adversarial actors bypass traditional network perimeter defences by exploiting the human attack surface specifically targeting the economic vulnerabilities and career mobility of cleared defence, intelligence, and academic personnel to aggregate critical operational data. The operation relies on elaborate social engineering architectures deployed across prominent platforms such as LinkedIn, indeed, and Upwork. Chinese operatives systematically establish fictitious personas representing private consultancies, think tanks, or human resources firms, subsequently posting fraudulent job listings for foreign policy and defence analysts. The recruitment pipeline follows a highly structured methodology: resumes are triaged based on potential access to sensitive environments; candidates undergo virtual interviews designed to probe their networks and unit activities; and

recruits are initially tasked with producing "trial reports" on defence or geopolitical topics.

As the relationship matures, operatives pressure recruits for increasingly privileged information, actively migrating communications to encrypted messaging applications to evade monitoring. Financial compensation for the acquired intelligence is intentionally obfuscated through third-party payment gateways including PayPal, Payoneer, Zelle, and various cryptocurrency networks, often routed through associated accounts to mask the true origin. For risk managers and national security planners, this development underscores the critical inadequacy of purely technical cybersecurity measures when confronted with sophisticated insider threat cultivation. The campaign demonstrates how adversaries synthesize disparate, ostensibly unclassified data points into comprehensive intelligence pictures. Mitigating this pervasive threat demands robust workforce counterintelligence training, continuous insider risk monitoring, and the recognition that professional networking environments are active, hostile domains in modern geopolitical competition.

Read more: https://www.mi5.gov.uk/sites/default/files/2026-06/SAFEGUARDING%20OUR%20SECRETS%20PUBLICATION.pdf

Anthropic 'plants' engineers at NSA despite facing ban by Pentagon

In a highly irregular convergence of commercial artificial intelligence and state-sponsored offensive cyber operations, AI firm Anthropic has embedded "forward-deployed" software engineers within the U.S. National Security Agency (NSA) to actively customize its advanced "Mythos" AI model for intelligence applications, despite a broader Pentagon ban on the company's technology. This clandestine deployment underscores a deepening fracture within the U.S. defense establishment regarding the procurement of frontier AI: the Department of Defense (DoD) recently designated Anthropic a "supply-chain risk" following the company's refusal to permit its systems to be utilized for mass domestic surveillance or lethal autonomous weaponry, yet the NSA has secured an explicit carve-out to leverage the technology. Operationally, approximately half a dozen Anthropic engineers are currently stationed inside the NSA, working to adapt the Mythos model a system previously restricted due to its profound capacity to identify and exploit zero-day vulnerabilities across major operating systems and web browsers for offensive operations. Insiders report the software is specifically tailored to infiltrate the fortified networks of foreign adversaries, including China and Iran, operating under the strategic premise that engineering advanced attack capabilities is essential to developing robust defensive architectures.

While the exact scope of the engineers' involvement in live operations remains classified, this arrangement effectively positions private-sector personnel at the vanguard of nation-state cyber warfare, sidestepping traditional military and intelligence oversight frameworks. As Anthropic simultaneously expands commercial access to Mythos to 150 organizations globally, this development highlights the rapidly eroding boundary between ethical AI guardrails and the operational imperatives of global cyber conflict. For risk managers and policy stakeholders, the NSA's utilization of commercially restricted AI signals a paradigm shift in the digital arms race, where acquiring exquisite offensive capabilities increasingly supersedes standard supply-chain risk mitigation and redefines the rules of engagement in contested cyberspace.

Read more: https://timesofindia.indiatimes.com/technology/tech-news/anthropic-plants-engineers-at-nsa-despite-facing-ban-by-pentagon/articleshow/131528432.cms

US pushes NATO allies to use defence spending to replace Huawei equipment

In a strategic effort to accelerate the technological decoupling of transatlantic infrastructure from Chinese vendors, the United States government is actively pressuring NATO allies to leverage expanded military budgets to fund the removal of Huawei and ZTE equipment from European 5G networks. As telecommunications infrastructure increasingly serves as the backbone for both civilian economies and military logistics, the presence of Chinese hardware is viewed by Washington as an unacceptable national security vulnerability and a latent vector for state-nexus espionage. Operationally, the U.S. State Department has proposed that

NATO members allocate the 1.5 percent "defence-adjacent" portion of their expanded 5 percent GDP defence spending targets to finance this extensive "rip and replace" initiative. While the European Commission has formally designated Huawei and ZTE as "high-risk suppliers" under its cybersecurity framework, the U.S. proposal faces significant friction from key member states, notably Germany and Spain.

These nations currently oppose a binding, bloc-wide ban, citing the immense capital expenditure required to overhaul networks where Chinese vendors currently supply an estimated 30 to 40 percent of the region's 5G hardware as well as the severe risk of economic retaliation from Beijing. By reframing the costly removal of Chinese telecommunications technology as a core NATO defence obligation rather than a purely civilian regulatory challenge, Washington aims to overcome Europe's financial reluctance and unify the alliance's procurement strategy ahead of the upcoming NATO leaders' summit in Turkey. For enterprise network operators and defence planners, this development underscores the rapid convergence of cybersecurity, military readiness, and industrial policy. The aggressive push to subsidize critical network modernization through defence appropriations highlights a fundamental shift in risk management, where isolating the digital supply chain against systemic geopolitical disruption is now prioritized on par with traditional kinetic defence capabilities.

Read more: https://www.firstpost.com/tech/us-pushes-nato-allies-to-use-defence-spending-to-replace-huawei-equipment-heres-why-14020215.html

U.S Getting Strict on Chinese Military Companies

In a major escalation of the technological decoupling between Washington and Beijing, the U.S. Department of defence (DoD) has significantly expanded its Section 1260H list of "Chinese Military Companies" (CMCs), signalling a strategic shift to target China's broader commercial technology ecosystem under the premise of its military-civil fusion strategy. Released on June 8, 2026, the updated roster adds 65 entities including 17 parent companies and 48 subsidiaries capturing market leaders previously viewed as strictly civilian. Prominent additions span cloud computing and artificial intelligence (Alibaba, Baidu), advanced robotics and LiDAR (Unitree, RoboSense), electric vehicles and energy storage (BYD, NIO, CALB), memory semiconductors (YMTC, CXMT), and biotechnology (WuXi AppTec, Novogene). For enterprise risk officers and defense contractors, this development fundamentally alters supply chain compliance dynamics.

While a 1260H designation does not act as an outright economic embargo for general U.S. commercial entities, strict statutory prohibitions enacted under recent National Defense Authorization Acts (NDAAs) are actively materializing. Specifically, direct DoD procurement bans tied to the CMC list take effect this month (June 2026), alongside unprecedented provisions prohibiting defense contractors from engaging lobbyists who concurrently represent 1260H-listed entities. Furthermore, the inclusion of genomics and life-science heavyweights like WuXi AppTec triggers immediate compliance considerations under the BIOSECURE Act framework, which restricts federal funding to designated "Biotechnology Companies of Concern." This expansion reflects a hardening U.S. national security posture that increasingly equates commercial dominance in dual-use technologies such as AI data infrastructure, autonomous mobility, and genomics with latent military capability. As these regulatory boundaries blur, multinational corporations and Defense Industrial Base (DIB) suppliers must urgently conduct deep-tier supply chain audits, map indirect vendor dependencies out to the sub-component level, and prepare for a fundamentally fragmented global procurement landscape where operational resilience increasingly dictates isolating U.S. and Chinese technology stacks.

Read more: https://www.thewirechina.com/2026/06/10/getting-strict-on-chinese-military-companies/

United States of America (USA)

President Trump Executive Order Promoting Advanced Artificial Intelligence Innovation and Security

In a strategic manoeuvre designed to cement United States global dominance in artificial intelligence while addressing escalating threat vectors, the White House has issued a sweeping Executive Order emphasizing rapid, deregulated AI innovation coupled with fortified federal cybersecurity. As state-sponsored actors increasingly target intellectual property and leverage machine learning for offensive operations, the directive reflects a clear policy pivot: eschewing mandatory algorithmic licensing in Favor of voluntary, public-private collaboration to outpace geopolitical rivals. The mandate establishes aggressive 30-day operational timelines for the Department of War, the National Security Agency (NSA), and the Cybersecurity and Infrastructure Security Agency (CISA) to harden national security and civilian federal information systems. Key operational deliverables include the immediate formation of an "AI cybersecurity clearinghouse" to deconflict vulnerability scanning and coordinate patch distribution across critical infrastructure, alongside a classified intelligence benchmarking process to formally designate "covered frontier models."

Crucially, the administration explicitly prohibits mandatory preclearance or governmental licensing for model development. Instead, it proposes a voluntary framework where AI developers can opt to provide the government with up to 30 days of early access to covered frontier models prior to commercial release. Concurrently, the Department of Justice is instructed to aggressively prioritize the prosecution of threat actors employing AI agents to execute unauthorized network intrusions under existing federal cybercrime statutes. For enterprise risk managers, defence planners, and industry stakeholders, this executive action signals a definitive paradigm shift in national cyber resilience: the security of advanced AI ecosystems will rely primarily on voluntary corporate intelligence sharing, aggressive criminal deterrence, and rapid technical remediation via government clearinghouses, rather than pre-emptive regulatory constraints on the tech sector.

Read more: https://www.whitehouse.gov/presidential-actions/2026/06/promoting-advanced-artificial-intelligence-innovation-and-security/

Seeking Counsel: Ongoing Targeted Campaign Against US Law Firms

A rapid-tempo, financially motivated data theft and extortion campaign by the threat cluster UNC3753 (also tracked as Luna Moth, Chatty Spider, or Silent Ransom Group) is actively targeting U.S. professional, legal, and financial services organizations. As traditional perimeter defenses improve, threat actors are increasingly weaponizing human vulnerabilities through advanced social engineering, establishing a fast-moving threat model where the entire attack lifecycle from initial contact to data exfiltration can occur in under an hour. Bypassing automated boundary controls, UNC3753 relies heavily on highly targeted voice phishing (vishing), placing direct calls to employees under the guise of internal IT helpdesk personnel assisting with security or data migration issues. Attackers instruct victims to install commercial screen-sharing and remote monitoring and management (RMM) tools such as Zoom, Quick Assist, and AnyDesk often delivering installation commands via self-destructing Privnote links to evade chat and endpoint telemetry logs.

Once remote control is established, often by pivoting from Bring Your Own Device (BYOD) endpoints into corporate Virtual Desktop Infrastructure (VDI), the actors aggressively enumerate file systems and target document repositories like iManage to harvest proprietary agreements, tax logs, and personally identifiable information (PII). Exfiltration is rapidly executed via portable utilities like WinSCP or direct browser uploads to actor-controlled cloud storage. Notably, this campaign occasionally crosses into the physical domain; in some instances, operatives posing as IT technicians have entered corporate offices to manually exfiltrate data via USB drives. Following data theft, UNC3753 issues unbranded extortion demands within 30 minutes, giving victims a three-day window to negotiate before threatening to publish archives on their "LEAKEDDATA" site and directly contact the victim's clients. This hybrid operational model underscores a critical shift toward extortion-only attacks that bypass ransomware encryption entirely, emphasizing the urgent need for strict identity verification protocols for internal IT support, tighter BYOD security policies, and the essential convergence of physical and cybersecurity risk management.

Read more: https://cloud.google.com/blog/topics/threat-intelligence/targeted-campaign-us-law-firms

The Kingdom of the Netherlands | Dutch

Joint operation by police and NCSC takes down large Botnet, Network

In a significant disruption of global cybercriminal operations, the Dutch National Cyber Security Centre (NCSC) and the Netherlands Police have jointly dismantled a massive botnet commanding at least 17 million compromised devices. As threat actors increasingly weaponize consumer IoT hardware, routers, and mobile devices often leveraging them as "residential proxies" to obfuscate malicious traffic, bypass geo-fencing, and launch high-volume distributed denial-of-service (DDoS) attacks or automated fraud this takedown highlights the escalating risk that poorly secured edge devices pose to the broader digital ecosystem. Triggered by intelligence from an independent security researcher, the collaborative investigation traced the botnet's command-and-control (C2) architecture to 200 servers hosted entirely within the Netherlands.

Acting on these findings, Dutch law enforcement seized critical infrastructure from a local hosting provider, subsequently compelling the host to terminate the remaining operational servers utilized for illicit activities. The dismantled network achieved its immense scale by exploiting vulnerabilities in unpatched software, default credentials, and inadequately secured network protocols to silently recruit computers, smartphones, and smart appliances into its swarm. While the specific threat group and malware variants remain undisclosed, the operational mechanics emphasize the persistent vulnerability of edge environments. For enterprise defenders and risk managers, this incident underscores the imperative of strict patch management, multi-factor authentication (MFA), and comprehensive asset visibility extending to remote and edge networks. Ultimately, the successful NCSC-police intervention demonstrates the strategic value of rapid, public-private intelligence sharing in neutralizing sprawling cybercriminal infrastructure, while reinforcing the reality that global cyber resilience depends heavily on securing the fragmented, deeply interconnected consumer attack surface.

Read more: https://www.ncsc.nl/nieuws/gezamenlijke-actie-politie-en-ncsc-legt-groot-botnetwerk-plat

Afghanistan | Islamic Emirate of Afghanistan

Operation XENOFISCAL: SideCopy deploying persistent XenoRAT targeting the MoF, Afghanistan

In a highly targeted cyberespionage campaign tracked as "Operation Xenofiscal," the Pakistan-linked threat actor SideCopy operating under the broader Transparent Tribe (APT36) umbrella has systematically targeted the Ministry of Finance (MoF) of the Islamic Emirate of Afghanistan. As regional state-sponsored actors increasingly refine their operational tradecraft to surveil rival governments, this campaign highlights the persistent vulnerability of administrative bodies to highly localized, intelligence-gathering operations. The attack sequence initiates via spear-phishing emails delivering a ZIP archive containing a malicious LNK file. Demonstrating deep contextual knowledge of the target environment, the actors utilize a Pashto-language filename masquerading as a psychological warfare seminar attendee list intended for provincial finance officials. Upon execution, the LNK file leverages the legitimate Windows utility mshta. exe in a living-off-the-land (LOLBIN) technique to silently fetch a remote HTML Application (HTA) payload from a compromised Afghan educational domain. This payload decodes obfuscated JavaScript in-memory, utilizing custom Base64 decoding and .NET BinaryFormatter deserialization to bypass traditional file-based endpoint detection.

While presenting the victim with a legitimate decoy document an exhaustive provincial staff directory written in Dari and Pashto the malware establishes persistent access via the Windows Run registry key, disguised as a Microsoft Edge component. Ultimately, the loader deploys version 1.8.7 of XenoRAT, a remote access trojan, which establishes covert communications with bulletproof European command-and-control (C2) infrastructure entirely isolated from the initial delivery phase. For regional security analysts and enterprise defenders, Operation Xenofiscal underscores the critical need to harden environments against LOLBIN abuse and fileless execution chains. By combining highly tailored linguistic lures with heavily obfuscated, in-memory staging mechanisms, SideCopy demonstrates a sophisticated, resilient capability to conduct protracted surveillance against strategic geopolitical

targets in South Asia.

Read more: https://ciso.economictimes.indiatimes.com/news/cybercrime-fraud/operation-xenofiscal-reveals-sophisticated-cyber-espionage/131543107

https://www.seqrite.com/blog/operation-xenofiscal-sidecopy-deploying-persistent-xenorat-targeting-the-mof-afghanistan/

People's Republic of China (PRC) | China

VerdantBamboo: Just Another BRICKSTORM in the Firewall

A sophisticated cyber espionage campaign orchestrated by the Chinese state-nexus threat actor VerdantBamboo (also tracked as WARP PANDA or UNC5221) has successfully compromised multiple organizational networks by targeting unmonitored edge appliances and Managed Service Providers (MSPs). As enterprises increasingly harden traditional endpoints and cloud perimeters, advanced persistent threats are pivoting to "blind spot" infrastructure such as storage arrays and network firewalls lacking Endpoint Detection and Response (EDR) telemetry to establish covert proxy networks and bypass cloud identity controls like Conditional Access policies. In a recently remediated intrusion spanning at least 18 months, VerdantBamboo initially breached a victim organization via their compromised MSP, infecting a FreeBSD-based pfSense firewall and an on-premise Linux-based Egnyte Storage Sync system.

The actors achieved root-level persistence on the Egnyte appliance by exploiting a local privilege escalation misconfiguration in the sudo tee command (since patched in v13.13), subsequently deploying BRICKSTORM, a Golang-based remote access trojan. This implant was utilized to proxy connections into the victim's Microsoft 365 environment, effectively disguising malicious logins as legitimate internal network traffic. The attackers also embedded AGENTPSD, a Python-based reverse shell compiled with PyInstaller, as a scheduled cron job for fallback command-and-control. When the initially compromised systems were taken offline, VerdantBamboo demonstrated high operational resilience by rapidly returning through an exposed, non-MFA-protected firewall administrative interface to deploy PLENET a previously undocumented Linux backdoor written in .NET Core and compiled via Native AOT onto a Synology NAS. This persistent campaign highlights a critical vulnerability in modern enterprise architectures: the implicit trust granted to unmonitored network appliances and third-party service providers. For network defenders, this necessitates an urgent expansion of security monitoring to include edge devices, the strict enforcement of multi-factor authentication across all administrative interfaces, and rigorous supply-chain risk assessments to mitigate the systemic threat posed by compromised MSPs.

Read more: https://www.volexity.com/blog/2026/06/04/verdantbamboo-just-another-brickstorm-in-the-firewall/

TA4922: The Suspected Chinese Crime Group is Going Global

The global cyber threat landscape is witnessing a significant escalation as TA4922, a sophisticated Chinese-speaking cybercriminal cluster, aggressively expands its operations beyond its traditional East Asian targets into Europe and Africa. As the Chinese cybercriminal ecosystem matures, actors are increasingly adopting advanced tradecraft historically reserved for state-nexus espionage groups to execute financially motivated attacks. Operating with a dramatically accelerated tempo since March 2026, TA4922 has broadened its victimology from Japan, Taiwan, and India to include organizations in the U.K., Germany, Italy, and South Africa. The group employs highly localized social engineering lures themed around human resources, payroll, and taxation to deliver a rapidly evolving, multi-objective payload arsenal. While historically reliant on ValleyRAT (Winos4.0) and HoldingHands, recent campaigns introduce novel malware families, including Atlas RAT, RomulusLoader, and SilentRunLoader. In a notable tactical shift, TA4922 actively leverages RomulusLoader to stage legitimate remote monitoring and management (RMM) software, such as AnyDesk and SyncFuture, blending malicious activity with trusted cloud hosting services to evade endpoint telemetry.

The actor's operations are uniquely versatile, seamlessly pivoting among credential phishing, direct financial fraud, credit card theft, and persistent remote access resale, often attempting to shift victim communications from email to encrypted messaging applications. Although TA4922's infrastructure and tooling exhibit overlaps with alleged espionage clusters like Silver Fox and Void Arachne, threat

analysts assess the group's core objectives remain strictly financial. For network defenders and policy stakeholders, TA4922's global pivot underscores the rising systemic risk of advanced persistent cybercrime. This convergence of APT-tier operational security, localized social engineering, and the abuse of legitimate administrative tools demands enhanced behavioral monitoring, rigorous scrutiny of RMM deployments, and robust email security to counter increasingly borderless, multi-vector financial threats.

Read more: https://www.proofpoint.com/us/blog/threat-insight/ta4922-suspected-chinese-crime-group-going-global

Republic of China (ROC) | Taiwan

Operation Dragon Weave: Uncovering a China-Linked Campaign Targeting Czech Republic and Taiwan Using Azure Cloud C2

In a highly targeted espionage campaign dubbed "Operation Dragon Weave," a China-linked threat actor has been observed systematically compromising government, technology, and academic sectors in Taiwan and the Czech Republic. As advanced persistent threat (APT) groups increasingly weaponize trusted cloud infrastructure to obfuscate malicious traffic and adopt modern, memory-safe languages like Rust to bypass legacy signature-based detection, this campaign highlights the evolving sophistication of state-sponsored cyber operations against strategic geopolitical targets. Initially delivered via spearphishing ZIP archives, the attack leverages highly localized lures, including forged Taiwanese project application reviews and Czech Social Security Administration appointment notices, to establish initial access.

The infection sequence utilizes two parallel delivery mechanisms to maximize success: a deceptive LNK shortcut that triggers a VBScript and PowerShell decryption chain, and a self-contained Rust-compiled executable dropper. Both vectors ultimately converge on a DLL sideloading technique, exploiting a legitimate RuntimeBroker_update.exe binary to load a malicious UnityPlayer.dll tracked as "RUSTCLOAK." This custom Rust-based loader subsequently decrypts and executes the final payload, "AZUREVEIL" a tailored Adaptix agent heavily reliant on Microsoft Azure Blob Storage for covert command-and-control (C2) communications and data exfiltration. Notably, operational security oversights by the threat actors, including exposed Rust build paths, assisted analysts in profiling the development environment. For enterprise defenders and national security planners, Operation Dragon Weave underscores the critical imperative of deploying behaviour-based endpoint detection to identify anomalous DLL sideloading, implementing rigorous egress monitoring to catch the abuse of legitimate cloud storage services, and fortifying defences against the rising tide of bespoke, multi-staged malware frameworks deployed in modern geopolitical espionage.

Read more: https://www.seqrite.com/blog/operation-dragon-weave-uncovering-a-china-linked-campaign-targeting-czech-republic-and-taiwan-using-azure-cloud-c2/

Russian Federation | Российская Федерация, Rossiyskaya Federatsiya

FSB Alleges Mass Cyber Spying Involving Global Tech Firms Fastly and Cloudflare

In a significant escalation of cyber-geopolitical friction, Russia's Federal Security Service (FSB) has formally accused Western intelligence agencies of orchestrating a sweeping cyberespionage campaign against high-ranking Russian officials, allegedly with the complicity of major global technology firms including Cloudflare, Fastly, and Apple. As the war in Ukraine protracts, this public attribution reflects a growing Russian strategy of framing Western commercial technology providers as active extensions of state intelligence apparatuses, intensifying the balkanization of the global internet and increasing pressure on foreign tech companies operating within or routing traffic through the Russian Federation. According to the FSB, Western operatives have systematically compromised the smartphones of senior Russian personnel, utilizing sophisticated malware designed to exfiltrate personal data, intercept communications, and remotely activate microphones for ambient surveillance.

The Russian intelligence agency claims this targeted data collection is directly weaponized to facilitate the "systematic" addition of compromised officials to U.S. and EU sanctions lists via the deployment of "compromising materials." While the FSB did not specify the exact malware variant or name the targeted officials, affiliated Russian cybersecurity

firm Kaspersky Lab previously detailed a related 2023 zero-click exploit chain involving manipulated iMessages on Apple devices, a claim Apple has vehemently denied. Concurrently, state media actively implicated infrastructure giants Cloudflare and Fastly, contextualizing the accusations within Russia's ongoing, punitive regulatory campaign against Cloudflare for its refusal to register user data with state databases. The FSB has subsequently initiated a formal criminal investigation into the unauthorized access and malware distribution, strictly prohibiting government officials from discussing confidential information near personal devices. For risk managers and policy stakeholders, these allegations underscore the severe operating risks for Western tech firms in authoritarian jurisdictions, highlighting a threat landscape where technical infrastructure is increasingly targeted not just by cyberattacks, but by state-driven legal and informational warfare aimed at compelling data localization and severing access to global, encrypted services.

Read more: https://www.themoscowtimes.com/2026/06/02/fsb-alleges-mass-cyber-spying-involving-global-tech-firms-fastly-and-cloudflare-a92901

Middle East | West Asia

IAI, Palladyne AI to team up to sell Harpy, Harop UAVs to Department of War

In a significant realignment of the defence technology supply chain to meet accelerating battlefield demands, Israel Aerospace Industries (IAI) has formed a strategic partnership with U.S.-based Palladyne AI to domestically manufacture and integrate its combat-proven loitering munitions for the U.S. Department of War (DOW). As global military postures pivot toward countering sophisticated anti-access/area denial (A2AD) networks, Western defence establishments are increasingly prioritizing the rapid acquisition of autonomous, high-precision strike capabilities over protracted clean-sheet development programs. Under the agreement, Palladyne AI will serve as the primary domestic integrator, adapting IAI's HARPY, HAROP, and Mini HARPY systems to specific U.S. operational requirements while manufacturing key components onshore. These systems operate at the tactical convergence of unmanned aerial vehicles and missiles, specializing in the suppression and destruction of enemy air defences (SEAD/DEAD).

Operationally, the HARPY and HAROP platforms execute autonomous search and engagement protocols against radar sites, missile launchers, and command-and-control nodes, notably functioning effectively without prior intelligence on target coordinates. The Mini HARPY variant enhances this capability by fusing electro-optical/infrared (EO/IR) sensors with an anti-radiation seeker to neutralize adversary emitters, including counter-UAS arrays. By leveraging Palladyne AI's domestic manufacturing footprint and autonomy engineering alongside IAI's extensive operational legacy systems recently fielded by Indian and Azerbaijani forces the collaboration bypasses traditional acquisition bottlenecks to rapidly scale mature technology. For defence policymakers and strategic planners, this partnership underscores a critical evolution in the industrial base: localizing the production of advanced kinetic assets to mitigate supply chain vulnerabilities, while accelerating the deployment of exquisite autonomous weapons to ensure operational superiority in highly contested electromagnetic and physical threat environments.

Read more: https://www.jpost.com/defense-and-tech/article-898844

Data of 600,000 Gaza households exposed in WFP cyber-attack

In a severe breach of humanitarian data security, an undisclosed threat actor compromised the United Nations World Food Programme (WFP), exposing the highly sensitive personal and geographic data of approximately 600,000 households in Gaza. As kinetic conflict in the region escalates, the weaponization of digital identity data presents an acute, physical security risk to vulnerable populations, emphasizing the dangerous gap between the vast data aggregation practices of aid organizations and their operational cybersecurity maturity. The intrusion, executed on May 14, specifically targeted the WFP's Self-Registration Application (SRA) a localized portal utilized by Palestinian beneficiaries to register for food and cash assistance. Threat actors successfully exfiltrated comprehensive personally identifiable information (PII), including full names, national ID numbers, mobile phone numbers, and precise location data. Internal whistleblower reports indicate that the WFP was alerted to the specific SRA vulnerability by an independent researcher two days prior to the compromise.

Despite assurances from the agency's Rome headquarters that the vulnerability had been mitigated, the exploitation occurred on the very same day. In response, the WFP took the SRA platform offline to contain the intrusion and noted that the breach remained isolated from its broader global identity management system, SCOPE; however, the agency waited 17 days before notifying affected beneficiaries via Telegram. This incident unfolds against a backdrop of intense geopolitical friction over data privacy in the region, including recent legal mandates demanding that aid organizations surrender operational data for access. For security practitioners and risk managers in the NGO sector, this event highlights a critical systemic failure: humanitarian agencies are centralizing the data of highly targeted populations without the commensurate technical architecture to defend against sophisticated cyber operations. Ultimately, this breach underscores the urgent necessity for the humanitarian sector to adopt enterprise-grade vulnerability management, rigorous patch deployment, and rapid incident disclosure protocols to prevent digital compromise from translating into kinetic harm.

Read more: https://www.thenewhumanitarian.org/news/2026/06/02/data-600000-gaza-households-exposed-wfp-cyber-attack

Bundesrepublik Deutschland | Federal Republic of Germany

Germany's Cobra 600 Is A Jet Powered Interceptor Drone That Slings An IRIS-T Missile

Amid the rapid proliferation of asymmetric aerial threats and the persistent use of low-cost drones and cruise missiles in modern conflict zones, German defence contractor Diehl Defence and aerospace start-up Polaris Raumflugzeuge have unveiled the Cobra 600, a novel jet-powered interceptor drone designed to drastically expand ground-based air defence (GBAD) architectures. Developed under the Airborne Launching and Attack System (AirLAS) program, the Cobra 600 functions as a loitering „missile taxi," integrating a standard Eurofighter pylon to carry a single IRIS-T interceptor. By physically projecting the launch point into contested airspace, the platform extends the effective interception radius of tethered IRIS-T SLM and SLS batteries from a maximum of 25 miles to approximately 250 miles. Operationally, the delta-wing drone powered by up to four JetCat-P1000-PRO micro turbojets and equipped with retractable runway gear acts as a forward-positioned effector.

It relies on the primary GBAD radar for initial target detection and vectoring via a secure datalink. Once positioned, the system utilizes a Lock-On-After-Launch (LOAL) protocol, relying on the missile's integral imaging infrared seeker for terminal guidance. While adversary groups and state actors like Russia have previously attempted to arm one-way attack munitions such as the Shahed-136 with legacy MANPADS or R-60 missiles, those ad-hoc solutions suffer from sluggish kinematics and poor situational awareness. In contrast, the Cobra 600's jet propulsion ensures rapid response times, while its deep integration into established C2 networks maintains a rigorous, human-supervised kill chain. For defence planners and risk managers, this development represents a critical evolution in multi-layered airspace resilience. By leveraging relatively expendable, loitering platforms to screen threat corridors and neutralize targets at extended standoff ranges, militaries can effectively multiply the footprint of their exquisite surface-to-air systems while strategically mitigating the economic asymmetry of modern drone warfare.

Read more: https://www.twz.com/air/germanys-cobra-600-is-a-jet-powered-interceptor-drone-that-slings-an-iris-t-missile

The French Republic | République française

French government's encrypted instant messaging service, compromised

A targeted account takeover on Tchap, the French government's sovereign secure messaging platform, has exposed the persistent vulnerability of internal state communications to identity-centric attacks. As global governments increasingly transition to localized, encrypted communication tools to mitigate state-nexus espionage, this incident highlights the latent risks within hybrid enterprise environments where legitimate identity grants broad internal visibility. On June 7, 2026, an unidentified threat actor compromised a valid user account, enabling unauthorized access to the platform's unencrypted public forums. According to the French Interministerial Directorate for Digital Affairs (DINUM), acting in coordination with the national cybersecurity agency (ANSSI), the intrusion was rapidly contained by identifying and blocking the compromised account to sever persistent access. Crucially, the platform's cryptographic architecture held firm: end-to-end encryption successfully protected all private

conversations, shielding historical data from the attacker despite the compromised identity. However, the actor successfully enumerated and scraped data from public channels, potentially compromising the personally identifiable information (PII) of 73,467 government agents—approximately 9% of the platform's user base. The exposed data includes full names, government email addresses, departmental affiliations, user avatars, and any operational content inadvertently posted to the public forums. DINUM has formally notified the national data protection authority (CNIL) and is conducting extensive log analysis to map the exact exfiltration vectors. This breach underscores a critical lesson in enterprise risk management: even within heavily fortified, sovereign communication networks, unencrypted broad-access channels provide a lucrative reconnaissance environment for adversaries who successfully bypass initial identity controls. For network defenders and policy stakeholders, the Tchap incident validates the architectural necessity of end-to-end encryption for compartmentalizing a breach's blast radius, while urgently reinforcing the need for continuous behavioral identity verification and strict data hygiene protocols to prevent sensitive information spillage in internal open forums.

Read more: https://www.numerique.gouv.fr/sinformer/espace-presse/incident-tchap/

Malware & Vulnerabilities

Microsoft Disables Dozens of GitHub Repos After Security Breach

A sophisticated software supply chain attack targeting the integration between modern codebases and artificial intelligence-assisted development environments has prompted Microsoft to temporarily disable 73 of its own GitHub repositories, highlighting a critical vulnerability in emerging developer workflows. As enterprise engineering teams rapidly adopt autonomous coding tools which inherently require extensive access to local configuration files, terminal environments, and authentication tokens threat actors are pivoting to exploit the native functionalities of these agents rather than relying on developers to manually execute malicious binaries. In this highly targeted campaign, attackers linked to the threat cluster TeamPCP injected malicious configuration files into prominent Microsoft repositories, including the entire Azure Functions organization, the Durable Task development suite, and various AI-oriented sample applications. These payloads were specifically engineered to trigger covert credential harvesting when the compromised repositories were opened within popular AI-enabled platforms such as Cursor, Visual Studio Code, Claude Code, or the Gemini CLI. The immediate defensive response, which saw GitHub take down the affected repositories in a matter of minutes, caused significant downstream disruption, breaking GitHub Actions and deployment pipelines for organizations relying on these trusted dependencies. This incident follows TeamPCP's prior compromise of the Durable Task project in May 2026, indicating a persistent and evolving effort to weaponize foundational development infrastructure. For enterprise security teams and risk officers, this breach represents a fundamental expansion of the software supply chain attack surface. It demonstrates that as the industry embraces AI-assisted engineering, defence-in-depth strategies must evolve to rigorously audit repository configuration files and tightly monitor the telemetry, execution permissions, and network access of AI coding assistants, treating them as high-privilege entities susceptible to automated, repository-driven exploitation.

Read more: https://nationalcioreview.com/articles-insights/extra-bytes/microsoft-disables-dozens-of-github-repos-after-security-breach/

PCPJack Hijacked 230 AWS, GCP, and Azure Servers to Run a Hidden SMTP Relay Network

In a sophisticated campaign highlighting the increasing weaponization of legitimate cloud environments, threat actors tracked as PCPJack compromised at least 230 Linux servers across AWS, Google Cloud, and Azure to establish a massive, hidden SMTP relay proxy network. As cybercriminal syndicates increasingly demand high-reputation, geographically diverse infrastructure to bypass stringent email security gateways and execute large-scale phishing and smishing operations, the automated hijacking of enterprise cloud instances has become a highly lucrative operational model. The campaign's inner workings were recently exposed when unauthenticated open directories on PCPJack's command-and-control (C2) infrastructure inadvertently revealed the threat actor's complete deployment toolkit, including Sliver C2 configurations, active scanners, and custom Python deployers. The infection sequence relies heavily on multi-architecture compatibility,

dropping unmodified, open-source Chisel binaries across AMD64, ARM64, and i386 systems to establish SOCKS5 reverse tunnels.

To ensure the network's efficacy for illicit email delivery, the deployer scripts feature an automated "SMTP quality gate," actively testing outbound connectivity to port 587 (smtp.gmail.com) and silently discarding nodes incapable of mail relay. Verified proxies are subsequently enriched with geolocation data and synchronized every five minutes to downstream operational servers. Persistence is achieved via stealthy mechanisms, dropping a hidden .xs binary in /var/tmp and blending into legitimate processes through systemd services or cron jobs named xsync. By leveraging unmodified public tools and deterministic port mapping, PCPJack effectively evades traditional hash-based detection mechanisms. For enterprise defenders and cloud architects, this campaign underscores the critical imperative of strictly enforcing egress filtering, particularly restricting outbound SMTP traffic from non-mail servers. Furthermore, the incident demonstrates that securing modern cloud environments requires continuous monitoring for anomalous reverse tunneling activity, robust asset visibility, and the rapid mitigation of web application vulnerabilities that serve as initial access vectors for these automated proxy-building botnets.

Read more: https://hunt.io/blog/pcpjack-230-cloud-servers-smtp-proxy-network-sliver-chisel

The Blight Reaches Microsoft: 73 Repos Disabled in 105 Seconds

A massive, automated takedown of 73 Microsoft repositories across four GitHub organizations has caused widespread disruption within the global software supply chain, exposing critical fragility in continuous integration and continuous deployment (CI/CD) pipelines. On June 5, 2026, GitHub's abuse detection mechanisms disabled mission-critical repositories within a 105-second window, impacting the entire Azure Functions ecosystem, the Durable Task family, and numerous AI sample applications. The epicenter of this incident is the durabletask repository, which suffered a previous compromise in May linked to the threat actor TeamPCP, indicating that attackers likely maintained persistent unauthorized access. Security analysts assess the takedown was heavily correlated with the Miasma worm an advanced iteration of the open-source Mini Shai-Hulud toolkit. Recently updated with specialized collectors targeting Azure CLI authentication caches and managed-identity tokens, Miasma propagates by harvesting credentials, generating unauthorized public repositories, and committing stolen secrets as JSON files.

This automated mass-creation of repositories tripped GitHub's Terms of Service enforcements, inadvertently severing access to widely utilized deployment tools. The operational fallout was immediate: because the critical Azure/functions-action repository was disabled, thousands of global CI/CD pipelines relying on mutable floating tags (such as @v1) failed to resolve, halting deployments worldwide. This incident exposes the systemic risk of the "mutable-tag tax" in DevOps architectures, where unpinned dependencies can instantly translate a localized repository suspension into a global operational outage. Immediate defensive measures require organizations to transition from floating tags to pinned commit SHAs, proactively rotate all Azure CLI, GitHub Actions OIDC, and managed-identity tokens, and actively hunt for Miasma's execution signature, specifically preinstall scripts invoking Bun against an obfuscated _index.js loader. More broadly, this development underscores the imperative for rigorous secrets management, supply-chain resilience, and zero-trust integration within automated development environments to counter the escalating threat of self-propagating credential stealers.

Read more: https://opensourcemalware.com/blog/miasma-reaches-azure

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