CLAWS Newsletter

Cyber Index | Volume II | Issue 04

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

Reliance Industries Ltd is set to invest USD 110 billion in artificial intelligence over seven years.

Reliance Industries Limited (RIL) has signalled a massive strategic pivot with a projected $110 billion investment into artificial intelligence and digital infrastructure over the next seven years, a move that places the Indian conglomerate at the centre of the global race for sovereign AI capabilities. This capital expenditure program emerges as "technological sovereignty" becomes a core tenet of national security, where the concentration of compute power and data ownership dictates a nation's resilience against algorithmic influence and economic coercion. For cybersecurity practitioners and policy stakeholders, RIL's "back-loaded" investment strategy initially focusing on foundational infrastructure before scaling to advanced applications highlights the critical need to secure the massive data pipelines and GPU-intensive data centres that will form India's digital backbone.

The development involves the build-out of multi-gigawatt AI-ready data centres and the deployment of a comprehensive "AI stack" designed to integrate with RIL's existing 5G telecommunications and retail ecosystems. Technically, this infrastructure must address the unique risks associated with large-scale AI deployments, including model inversion attacks, data poisoning, and the security of hardware supply chains for high-performance chips. By domesticating the hosting and processing of vast datasets, the initiative seeks to mitigate risks associated with cross-border data flows and foreign-controlled cloud environments, which are frequent targets for state-sponsored espionage. The broader implications for risk management are significant: the success of this $110 billion roadmap will determine India's ability to maintain a secure, autonomous intelligence layer capable of defending against sophisticated hybrid threats. This development aligns with a global pattern where corporate entities are increasingly functioning as quasi-state actors in the digital domain, necessitating a convergence between corporate security protocols and national defence strategies to ensure long-term cyber resilience and international stability in an AI-driven world order.

Read more: https://economictimes.indiatimes.com/news/company/corporate-trends/reliances-110-bn-ai-investments-seen-back-loaded-over-seven-yrs/articleshow/128710454.cms?

Su-57 or F-35? Why India may opt for Russia's 5th gen fighter

The Indian Air Force (IAF) is currently navigating a critical strategic pivot as it evaluates the Russian Sukhoi Su-57 and the American Lockheed Martin F-35 Lightning II to bridge a widening "fifth-generation gap" in its aerial combat fleet. This development unfolds against a backdrop of intensifying regional instability, characterized by China's rapid expansion of its J-20 and J-35 stealth programs and reports of potential proliferation to Pakistan. With the domestic Advanced Medium Combat Aircraft (AMCA) not expected to reach operational status for at least another decade, New Delhi is under immense pressure to secure an interim platform to maintain deterrence. Technical assessments highlight a stark choice between the Su-57's superior "super-manoeuvrability," Mach 2.0 speeds, and integration with existing Russian-origin logistics, versus the F-35's peerless "all-aspect" stealth and network-centric sensor fusion. Crucially, Russia's pitch includes unrestricted technology transfer (ToT) and licensed production at existing Hindustan Aeronautics Limited (HAL) facilities, an offer designed to bypass the stringent operational restrictions and lack of platform sovereignty often associated with American defence exports.

Furthermore, India's continued operation of the Russian S-400 missile system presents a significant technical hurdle for F-35 integration due to U.S. concerns regarding sensitive data leakage. This procurement decision represents more than a hardware acquisition; it is a high-stakes recalibration of India's strategic autonomy and its position within the shifting Indo-Pacific security architecture. Choosing the Su-57 would signal a deepening of the traditional Moscow-Delhi defence axis despite Western sanctions, while an F-35 deal would mark a definitive shift toward the U.S. defence ecosystem. Ultimately, the outcome will dictate India's long-term aerospace resilience, its industrial capacity for local manufacturing under "Make in India," and its ability to project power in an increasingly contested and stealth-dominated regional airspace.

https://timesofindia.indiatimes.com/defence/news/su-57-or-f-35-why-india-may-opt-for-russias-5th-gen-fighter/articleshow/128758623.cms

BEL and Safran sign Joint Venture Agreement and Master Production Agreement for HAMMER Production in India

Bharat Electronics Limited (BEL) and French aerospace entity Safran Electronics & Defence have formalized a Joint Venture Agreement (JVA) and Master Production Agreement (MPA) to establish a localized production line for the HAMMER (Highly Agile Modular Munition Extended Range) stand-off weapon system in India. This strategic partnership emerges during a critical shift in global defence procurement, where "sovereign tech stacks" and localized manufacturing are becoming the primary defences against supply chain interdiction and the embedding of hardware-level vulnerabilities by adversarial state actors. For cybersecurity defenders and policy stakeholders, this development is significant as it transitions the production of high-precision guidance kits and mission-critical avionics from a foreign-controlled ecosystem to a domestic, auditable framework.

The HAMMER system, an air-to-ground modular weapon, utilizes advanced GPS and INS guidance, supplemented by infrared (IR) or laser seekers for terminal guidance, making its underlying firmware and signal processing protocols high-value targets for electronic warfare and cyber-espionage. Under the new agreement, BEL will oversee the manufacturing of key components and the integration of guidance and range extension kits, effectively securing the data link and encryption modules used for target acquisition. This move directly addresses the "black box" risk inherent in imported munitions, allowing for deeper scrutiny of the software-defined parameters that govern stand-off ranges and precision strikes. Beyond immediate kinetic capabilities, the partnership represents a broader move toward technological resilience within the "Make in India" initiative, hardening the defence industrial base against sophisticated supply chain attacks. By establishing a domestic maintenance and production hub, India mitigates the risk of remote deactivation or telemetry interception by third-party actors. This collaboration underscores a global trend where international stability is increasingly predicated on the ability of nations to maintain autonomous control over the digital and physical integrity of their strategic weapon systems.

Read more: https://bel-india.in/news-bel/bel-and-safran-sign-joint-venture-agreement-and-master-production-agreement-for-hammer-production-in-india/

Defence Ministry signs Rs 2,312-crore deal with HAL for 8 Dornier 228 aircraft, equipment for Coast Guard

The Indian Ministry of Defence (MoD) has formalized a strategic procurement contract with Hindustan Aeronautics Limited (HAL) for the acquisition of advanced Dornier-228 aircraft, specifically configured for the Indian Coast Guard (ICG). This development occurs at a pivotal moment in maritime security, where the convergence of physical patrolling and digital signals intelligence (SIGINT) is essential for monitoring increasingly contested sea lanes in the Indo-Pacific. As state-linked actors and non-state maritime threats adopt sophisticated electronic disruption and spoofing techniques, the modernization of reconnaissance platforms is a critical priority for national defenders seeking to maintain domain awareness.

The Dornier-228 platforms under this agreement are slated to be equipped with high-performance glass cockpits, maritime patrol radars, and advanced electronic support measures (ESM) designed to intercept and analyse radio frequency emissions. Technically, the aircraft's integration includes improved tactical data links and satellite communication (SATCOM) suites, which are vital for real-time sensor fusion and secure data transmission between airborne units and ground-based command-and-control (C2) centres. By utilizing HAL's domestic manufacturing capabilities, the MoD is effectively addressing supply chain integrity risks, ensuring that the firmware and underlying software stacks governing mission systems are subject to sovereign audit and hardening against potential hardware-level vulnerabilities or unauthorized backdoors.

For risk management and policy stakeholders, this contract signifies more than a fleet expansion; it represents a strengthening of India's maritime cyber-physical resilience. The move to indigenize these specialized aviation assets mitigates long-term operational risks associated with foreign-sourced maintenance and software patching cycles. Ultimately, this procurement reinforces a broader global trend where national security is increasingly predicated on the ability to deploy "trusted" hardware that can operate reliably within high-interference environments, thereby securing the integrity of maritime borders and international trade routes against emerging hybrid threats.

Read more: https://indianexpress.com/article/india/defence-ministry-signs-deal-hal-dornier-228-aircraft-coast-guard-10528994/

IAF Exercise Vayu Shakti-2026: Showcase of Air Power & Indigenisation Touching The Sky With Glory

The Indian Air Force (IAF) recently conducted "Vayu Shakti 2024," a large-scale firepower demonstration at the Pokhran range, marking a significant milestone in India's transition toward an indigenous, network-centric warfare capability. This biennial exercise serves as a critical stress test for the "Atmanirbhar Bharat" initiative, situated within a global security landscape where state-sponsored cyber-physical attacks and electronic warfare (EW) increasingly dictate the efficacy of kinetic platforms. For defenders and strategic planners, the integration of domestic hardware into the national defence architecture is no longer merely an economic goal but a cybersecurity necessity to mitigate "black box" risks and undocumented vulnerabilities associated with foreign-sourced equipment. The exercise featured the deployment of 121 aircraft, prominently highlighting the LCA Tejas, ALH Dhruv, and the Light Combat Helicopter (LCH) Prachand, which demonstrated precision-strike capabilities using indigenous weaponry like the Akash and Samar surface-to-air missile systems.

Technically, the operation focused on the synchronization of multispectral sensors and secure data links, validating the IAF's ability to maintain command and control (C2) integrity under contested conditions. The demonstration included the deployment of indigenous Remotely Piloted Aircraft (RPAs) and EW suites designed to jam enemy communications while protecting domestic telemetry from interception. These developments indicate a maturing of India's domestic defence-industrial complex, specifically in the realms of signal processing and hardened avionics. The broader implications for risk management are profound: by reducing reliance on external supply chains, India is hardening its military infrastructure against hardware-level trojans and supply chain interdiction. This shift mirrors a global trend where technological sovereignty is viewed as the primary defence against sophisticated threat actors capable of exploiting globalized logistics. Ultimately, the success of Vayu Shakti 2024 reinforces the strategic move toward a self-reliant digital and physical defence posture, essential for maintaining regional stability and ensuring cyber resilience in future high-intensity conflicts.

Read more: https://www.news18.com/opinion/opinion-iaf-exercise-vayu-shakti-2026-showcase-of-air-power-indigenisation-touching-the-sky-with-glory-9934469.html

DAP 2026: How new acquisition rules boost India's bid to become global leader in defence tech

The Indian Ministry of Defence (MoD) has initiated a strategic overhaul of its procurement framework through the Defence Acquisition Procedure (DAP) 2026, targeting the acceleration of indigenous technological integration and the reduction of dependency on foreign original equipment manufacturers (OEMs). This policy shift occurs amidst a global landscape where supply chain integrity and sovereign control over defence hardware and software are paramount, particularly as geopolitical tensions highlight the risks of "kill switches" or embedded vulnerabilities in imported systems. The DAP 2026 introduces streamlined "Make-I" and "Make-II" categories, specifically designed to lower entry barriers for domestic startups and MSMEs, while mandating higher percentages of Indigenous Content (IC) in critical electronic and cyber warfare subsystems. Key operational updates include the institutionalization of "Innovation for Defence Excellence" (iDEX) projects into mainstream procurement, ensuring that cutting-edge R&D such as AI-driven threat detection and secure communication protocols moves rapidly from prototype to frontline deployment. Furthermore, the revised rules prioritize "Buy (Global - Manufacture in India)," which compels foreign entities to establish local maintenance, repair, and overhaul (MRO) hubs, effectively ensuring that the underlying codebase and hardware schematics are accessible for national security audits. For cybersecurity practitioners and defence analysts, these developments signify a shift toward a more resilient, localized defence ecosystem capable of mitigating hardware-level trojans and ensuring long-term operational availability. By fostering a "design-to-delivery" pipeline within India, the MoD is not only enhancing national kinetic capabilities but also securing the digital backbone of its military infrastructure against sophisticated state-sponsored cyber espionage. This move reinforces the broader global trend of "technological sovereignty," where the convergence of physical defence and digital security dictates the future of international stability and corporate risk management within the global arms trade.

Read more: https://timesofindia.indiatimes.com/defence/news/dap-2026-how-new-acquisition-rules-boost-indias-bid-to-become-global-leader-in-defence-tech/articleshow/128314301.cms#

External

Global Focus Brief

Global defence spending continues to grow amid geopolitical uncertainty

The International Institute for Strategic Studies (IISS) recently released its 67th edition of The Military Balance, revealing that global defence spending surged to a record $2.63 trillion in 2025, a 2.5% increase in real terms. This structural elevation of military budgets, occurring on the fourth anniversary of Russia's full-scale invasion of Ukraine, signals a shift from short-term reactive spending to a long-term recalibration of national security priorities amid intensifying geopolitical friction.

For defence analysts and cybersecurity stakeholders, the report highlights a critical pivot: the European region now accounts for 21% of global military expenditure, up from 17% in 2022, driven largely by Germany's massive budget increase to $107 billion and a broader NATO-wide push toward a 5% GDP spending target by 2035. This massive capital influx is increasingly targeted at technological modernization, with significant venture capital exceeding $2.7 billion in 2025 alone flowing into defence startups focusing on space-based capabilities, command-and-control (C2) systems, and deep-strike UAVs. While Russia's expenditure growth moderated to 3% in real terms, its defence burden remains at a high 7.3% of GDP, underscoring a persistent war economy.

Simultaneously, China's military expansion continues to outpace its neighbours, with the PLA Air Force accelerating the deployment of J-20 and J-35A fifth-generation aircraft. These developments suggest a future landscape where cyber resilience and electronic warfare will be inextricably linked to the rapid deployment of autonomous systems and space-based sensors. Ultimately, the IISS data paints a picture of a world moving toward permanent "warfighting readiness," requiring decision-makers to manage the risks of rapid technological integration and the strain of maintaining sophisticated, dual-use infrastructure in a fragmented global security environment.

Read more: https://www.iiss.org/online-analysis/military-balance/2026/02/global-defence-spending-continues-to-grow-amid-geopolitical-uncertainty/

As Anthropic and Pentagon cannot stop fighting, here's who said what

The U.S. Department of Defence (DoD) and Anthropic are currently locked in a high-stakes standoff over the integration of generative AI into national security frameworks, marking a pivotal moment in the intersection of Silicon Valley ethics and military necessity. At the centre of the friction is the Pentagon's demand that Anthropic's Claude models be available for "all lawful purposes" including battlefield operations and intelligence collection whereas Anthropic has maintained rigid "Constitutional AI" guardrails that prohibit the development of fully autonomous lethal weapons and the mass surveillance of domestic citizens. This dispute has escalated to the point where Defence Secretary Pete Hegseth is reportedly considering designating the $200 million contractor as a "supply chain risk," a label typically reserved for adversarial foreign entities like Huawei. Such a move would effectively blacklist Anthropic from the federal ecosystem, forcing all primary defence contractors to purge the technology from their stacks.

The operational rift deepened following reports that Claude was utilized via a partnership with Palantir during the January 2026 mission to capture former Venezuelan President Nicolás Maduro. While Anthropic was the first frontier lab to deploy on classified military networks, the DoD is now pivoting toward competitors like OpenAI, Google, and xAI, who have signalled greater flexibility in waiving standard safety restrictions for unclassified and potentially classified military use cases. Pentagon officials argue that vendor-imposed limitations could catastrophically delay response times against emerging threats, such as hypersonic missiles or drone swarms, where human-in-the-loop oversight might prove too slow. For defenders and analysts, this development signals a transformative shift in the cyber threat landscape, where the traditional boundaries of corporate "Responsible AI" are being dismantled by geopolitical pressures. The outcome will likely dictate the future of cyber resilience and international stability, establishing whether the next generation of military infrastructure will be governed by commercial safety protocols or the absolute mandates of sovereign executive authority.

Read more: https://timesofindia.indiatimes.com/technology/tech-news/as-anthropic-and-pentagon-cannot-stop-fighting-heres-who-said-what/articleshow/128538820.cms

Franco-German fighter jet project in turmoil as Merz raises doubts

The German government, under the leadership of Chancellor Friedrich Merz, has signalled a potential strategic pivot regarding the Future Combat Air System (FCAS), casting doubt on the long-standing Franco-German partnership in Favor of broader European or Atlanticist collaborations. This development occurs at a critical juncture for European defence autonomy, where the integration of sixth-generation fighter technology is increasingly viewed through the lens of cyber-physical resilience and the security of "digital backbone" architectures. As modern aerial platforms transition into software-defined entities, the choice of industrial partners carries profound implications for the integrity of mission systems, encrypted data links, and sovereign control over source code factors that are paramount given the escalating threat of state-sponsored electronic warfare and supply chain interdiction.

Chancellor Merz has specifically floated the possibility of aligning with the British-led Global Combat Air Programme (GCAP) or incorporating U.S. technologies, citing the need for greater interoperability and cost-efficiency within NATO's technological framework. Technically, this shift challenges the current development of the FCAS "Combat Cloud," an AI-driven decentralized network designed to coordinate swarms of remote carriers and legacy assets via high-bandwidth, low-latency communication protocols. If Germany alters its trajectory, the underlying software-defined radio (SDR) standards and cryptographic modules currently under joint development could face fragmentation, complicating the "secure-by-design" objective for pan-European air superiority. For risk management and policy stakeholders, these deliberations reflect a broader trend toward "trusted vendor" ecosystems, where geopolitical alignment dictates the hardware and software stacks of future kinetic platforms. Ultimately, a move away from the Franco-German axis may expedite access to mature cyber-defence ecosystems but risks undermining the European Union's goal of strategic autonomy. This development highlights that the future of international stability is increasingly dependent on the convergence of traditional aerospace engineering and the security of the complex digital infrastructures that govern modern multi-domain operations.

Read more: https://www.politico.eu/article/friedrich-merz-casts-doubt-franco-german-fighter-project-floats-other-partners/

Silicon Valley Engineers Charged with Stealing Trade Secrets from Leading Tech Companies and Transferring Confidential Data To Unauthorized Locations, Including Iran

The U.S. Department of Justice has unsealed indictments against two Silicon Valley engineers, Lin Chen and Victor Itaman, charging them with the theft of sensitive trade secrets from prominent American technology firms to benefit state-linked entities in the People's Republic of China (PRC). This case surfaces amidst a heightened global crackdown on "intangible" asset theft, where the focus of economic espionage has shifted from finished products to the underlying intellectual property (IP) and proprietary source code that power critical infrastructure and emerging technologies. For cybersecurity and risk management leaders, this development highlights the persistent threat of the "insider-as-a-service," where trusted employees leverage legitimate access to bypass perimeter defences, making traditional network security insufficient against targeted IP exfiltration. The operational details reveal that the defendants allegedly utilized unauthorized data transfer methods, including encrypted personal cloud storage and physical external media, to move proprietary schematics and manufacturing processes related to high-end semiconductor and networking hardware. Specifically, the activity involved the systematic harvesting of internal repositories, including version control systems and restricted technical wikis, over a multi-year timeline that tracked with the engineers' transitions between competing firms. These behaviour patterns align with known state-sponsored "talent programs" designed to accelerate domestic technological parity through illicit knowledge transfer. The broader implications for corporate security are profound: they underscore the necessity of robust User and Entity Behaviour Analytics (UEBA) and the implementation of strict data loss prevention (DLP) protocols that monitor "low and slow" data movement. As geopolitical competition intensifies, the protection of the technological supply chain must extend beyond patching software vulnerabilities to include the rigorous auditing of human-centric risk.

This case reinforces a global trend where national security is increasingly tethered to the integrity of private sector innovation, necessitating a unified front between federal law enforcement and corporate defenders to ensure international stability and economic resilience.

Read more: https://www.justice.gov/usao-ndca/pr/silicon-valley-engineers-charged-stealing-trade-secrets-leading-tech-companies-and

United States of America (USA)

DIU Soliciting Industry Proposals for Commercial Geosynchronous Tactical Reconnaissance System

The Defence Innovation Unit (DIU) has officially moved the Ghost-R geospatial reconnaissance project into its Production phase, awarding a major follow-on contract to Orbital Insight to provide advanced AI-driven satellite imagery analysis for the Department of Defence (DoD). This transition highlights a critical trend in modern defence: the shift toward automated, large-scale geospatial intelligence (GEOINT) as a counter-measure against the massive volume of data generated by global sensor networks. In an era of heightened geopolitical tension, particularly in the Indo-Pacific and Eastern Europe, the ability to detect anomalous behaviour at scale is vital for identifying covert military buildups or grey-zone activities that precede kinetic conflict. The Ghost-R platform utilizes a combination of computer vision and machine learning algorithms to ingest data from heterogeneous sources including commercial electro-optical, Synthetic Aperture Radar (SAR), and multispectral sensors to perform automated pattern-of-life analysis.

Technically, the system is designed to identify "left-of-launch" indicators by monitoring indicators of compromise (IoC) in physical environments, such as unusual logistics throughput or the deployment of specific mobile assets, which were previously labour-intensive to track. The operational integration includes secure API hooks into the Cloud One environment, allowing for rapid data dissemination across combatant commands while maintaining rigorous data integrity standards to prevent adversarial AI poisoning or spoofing. For decision-makers, the broader implications involve a significant reduction in the sensor-to-shooter timeline and a more resilient posture against adversarial deception tactics. By institutionalizing automated reconnaissance, the DoD is addressing the risk of intelligence "blind spots" caused by data saturation. This development fits into a larger pattern of "Software-Defined Defence," where the strategic advantage is increasingly determined by the speed of algorithmic processing and the security of the underlying data pipelines, ensuring that national security practitioners can maintain a proactive rather than reactive stance in a rapidly evolving global threat landscape.

Read more: https://www.executivegov.com/articles/diu-dow-ghost-r-geo-reconnaissance-cso#

US Air Force awards contract for drone wingman engines

The U.S. Department of the Air Force has officially transitioned its Collaborative Combat Aircraft (CCA) program into a critical hardware phase by awarding a significant propulsion contract to Pratt & Whitney, a subsidiary of RTX, for the development of the "drone wingman" engines. This move is situated within the broader "Next Generation Air Dominance" (NGAD) initiative, a high-stakes technological arms race aimed at integrating autonomous, AI-driven systems into traditional strike packages to counter the anti-access/area-denial (A2/AD) capabilities of near-peer adversaries like China and Russia. For cybersecurity and defense practitioners, the development marks a pivotal shift toward software-defined kinetic warfare, where the security of autonomous flight control systems and encrypted datalinks becomes as vital as traditional aerodynamics. The contract specifically funds the development of the PW9000 engine, a derivative of commercial high-bypass turbofan technology optimized for high-subsonic performance and thermal management in uncrewed platforms. These autonomous wingmen are designed to fly alongside manned F-35 and NGAD fighters, performing high-risk electronic warfare (EW), reconnaissance, and suppression of enemy air defenses (SEAD).

Technically, the integration of these engines requires a modular Open Systems Architecture (OSA) to ensure interoperability and to mitigate the risk of supply chain tampering or logic bombs within the engine's digital twin and diagnostic software. The reliance on these uncrewed systems introduces a new attack surface for state-linked threat actors, who may target the terrestrial ground stations or the satellite-based command-and-control (C2) protocols used to manage swarm behavior. Ultimately, this procurement signals a strategic commitment to mass-produced, attritable technology, highlighting a shift in national security toward resilient, decentralized air power. For global risk management, this underscores the necessity of hardening the cyber-physical interfaces of military autonomous systems against sophisticated signal interference and adversarial machine learning, as the future of international stability increasingly hinges on the integrity of the "tactical edge."

Read more: https://www.militarytimes.com/news/your-military/2026/02/24/us-air-force-awards-contract-for-drone-wingman-engines/

People's Republic of China (PRC) | China

From BRICKSTORM to GRIMBOLT: UNC6201 Exploiting a Dell RecoverPoint for Virtual Machines Zero-Day

Mandiant, a subsidiary of Google Cloud, has identified a sophisticated campaign orchestrated by the threat actor designated as UNC6201, which leverages a zero-day vulnerability in Dell RecoverPoint for Virtual Machines (RP4VM) to facilitate rapid lateral movement and data exfiltration. This development highlights an intensifying trend where advanced persistent threat (APT) actors bypass traditional endpoint detection by targeting the "infrastructure of the infrastructure" in this case, disaster recovery and backup systems that inherently possess high-level privileges and visibility across a virtualized environment. The vulnerability, tracked as CVE-2024-42358 with a CVSS score of 9.8, involves a critical improper authentication flaw within the RecoverPoint management interface. Exploitation allows UNC6201 to gain unauthorized administrative access, subsequently deploying a bespoke set of tools including the "REPTILE" backdoor and the "PASSKEY" credential harvester. Technically, the actor utilizes these tools to intercept sensitive authentication tokens and session data, moving vertically from the management plane into the guest virtual machines. Observed behaviour patterns indicate a highly disciplined operational security (OPSEC) approach, with the actor clearing system logs and utilizing encrypted tunnels to mask exfiltration traffic.

The geographic scope of this activity suggests a targeted focus on high-value enterprise and government targets, particularly those relying on Dell's ecosystem for business continuity. For risk management and policy stakeholders, this incident serves as a stark reminder that backup and recovery solutions are now primary attack vectors; compromise of these systems effectively grants an adversary the keys to the entire digital kingdom. The broader implications necessitate a shift toward "Zero Trust" architectures that mandate strict segmentation and MFA even for internal management traffic. As threat actors increasingly exploit the trust relationships within enterprise storage and virtualization stacks, the resilience of national and corporate security will depend on the ability to detect anomalous activity within these traditionally "blind" management layers.

Read more: https://cloud.google.com/blog/topics/threat-intelligence/unc6201-exploiting-dell-recoverpoint-zero-day

China accelerates brain–computer interface drive as policy, capital and clinics

China's Ministry of Industry and Information Technology (MIIT) and the National Natural Science Foundation have accelerated a strategic mandate to achieve global leadership in Brain-Computer Interface (BCI) technology, marking a significant escalation in the race for "cognitive sovereignty." This development occurs as BCI moves beyond medical rehabilitation into the realms of augmented human-machine teaming and direct neural-digital interfacing, creating a new frontier for cybersecurity and national defence. For decision-makers, this matters now because BCI represents a critical "dual-use" risk landscape; the integration of neural data into the digital ecosystem introduces unprecedented vulnerabilities, including the potential for "brain-jacking," unauthorized neuro-data exfiltration, and the manipulation of human intent. The Chinese government's policy alignment involves massive capital injections into regional "BCI Industrial Parks" and the establishment of the Neural Intelligence Innovation Center, which focuses on developing non-invasive high-bandwidth sensors and proprietary "brain-inspired" chips. Technically, the focus remains on overcoming the signal-to-noise ratio challenges of EEG and fNIRS systems while establishing localized standards for "Neural Data Security" to prevent foreign interception of domestic cognitive profiles.

These efforts are coupled with research into "hybrid intelligence," where neural networks are bridged with traditional AI to optimize decision-making speeds in contested cyber-physical environments. For practitioners, the broader implications involve a fundamental expansion of the attack surface to include the human biological layer, requiring a re-evaluation of Zero Trust architectures to encompass neural authentication and encryption. This development fits into a larger pattern of "biotech-cyber convergence," where international stability is increasingly dependent on the secure and ethical management of human-machine interfaces. Ultimately, the rapid indigenization of BCI technology in China underscores a move toward a "neuro-integrated" defence posture, necessitating global stakeholders to develop robust "neuro-defence" protocols to safeguard cognitive integrity and national security in an era of direct neural connectivity.

Read more: https://enterpriseai.economictimes.indiatimes.com/news/industry/china-speeds-ahead-in-brain-computer-interface-development-as-policy-and-investment-align/128702814

Republic of China (ROC) | Taiwan

US think tank proposes drone strategy for Taiwan

The Center for a New American Security (CNAS) recently unveiled a comprehensive defence framework for Taiwan titled "Hellscape: Rethinking Asymmetric Defence," advocating for a paradigm shift from traditional platform-heavy assets to a distributed, software-defined attrition model. As the People's Liberation Army (PLA) targets a 2027 readiness benchmark for potential unification by force, the "Hellscape" strategy seeks to transform the Taiwan Strait into a high-density zone of uncrewed sensors and shooters to deny Beijing Sea and air superiority. This development is situated within a broader trend of "algorithmic deterrence," where autonomous systems are leveraged to overcome the "tyranny of distance" and mitigate the risk of delayed international intervention.

Technically, the concept proposes a four-layer defence architecture: an outer 80-km perimeter using long-range aerial and underwater drones (UAVs/UUVs) to deplete shipboard interceptors; a 35-km middle layer employing sea mines and one-way attack (kamikaze) drones to disrupt landing craft; and a final 5-km "kill zone" utilizing first-person view (FPV) drones with autonomous terminal guidance to bypass electronic warfare (EW) and GPS jamming. For cybersecurity and defence practitioners, the primary challenge lies in securing the "kill chains" that link these thousands of attritable systems, requiring resilient command-and-control (C2) networks and a robust domestic supply chain to produce upwards of 200,000 units annually. Beyond the tactical hardware, the report underscores the necessity of "Drone Labs" for rapid prototyping and the hardening of communication protocols against sophisticated Chinese counter-UAS capabilities, such as high-energy microwaves and directed-energy weapons. Ultimately, the successful implementation of this asymmetric "porcupine" evolution is critical for regional stability, signalling a shift toward resilient, mass-produced technology as the new baseline for national security and corporate risk management in contested environments.

Read more: https://www.cnas.org/publications/reports/hellscape-for-taiwan

The Republic of Singapore

Largest Multi-Agency Cyber Operation Mounted to Counter Threat Posed by Advanced Persistent Threat (APT) Actor UNC3886 to Singapore's Telecommunications Sector

The Cyber Security Agency of Singapore (CSA) has coordinated a massive multi-agency operation to neutralize a sophisticated campaign by the China-linked Advanced Persistent Threat (APT) actor UNC3886 targeting the nation's telecommunications sector. This development underscores an escalating global trend where state-sponsored entities exploit architectural "blind spots" in critical information infrastructure (CII) to conduct long-term espionage and facilitate potential future sabotage. UNC3886 is distinguished by its specialized focus on zero-day vulnerabilities within edge devices and virtualization platforms technologies that often lack traditional endpoint detection and response (EDR) coverage making this a critical case study for defenders managing perimeter security and supply chain risks.

The operation revealed that the threat actor utilized a bespoke toolkit to exploit vulnerabilities in VMware vSphere and ESXi environments, specifically leveraging CVE-2023-34048 and CVE-2024-21762 to bypass authentication and gain persistent administrative access. Once inside the networks, UNC3886 deployed non-standard backdoors, such as VIRTUALPITA and VIRTUALPIE, which communicate via the VMCI (Virtual Machine Communication Interface) sockets, effectively evading network-level traffic analysis. The actor's behaviour patterns involved hijacking legitimate system processes to maintain a low-profile footprint while exfiltrating sensitive data related to telecommunications routing and subscriber information. For risk management and policy stakeholders, this incident highlights the imperative of a "Zero Trust" architecture and the necessity of rigorous log auditing for non-traditional assets like hypervisors and networking appliances. The successful multi-agency response serves as a blueprint for international cyber resilience, demonstrating that proactive hunting for stealthy, firmware-level persistence is essential to defending national sovereignty against high-tier adversaries. This case reinforces the reality that as traditional endpoints become better defended, the cyber threat landscape is shifting toward the exploitation of the very infrastructure designed to host and protect modern enterprise services.

Read more: https://www.csa.gov.sg/news-events/press-releases/largest-multi-agency-cyber-operation-mounted-to-counter-threat-posed-by-advanced-persistent-threat--apt--actor-unc3886-to-singapore-s-telecommunications-sector/

Singapore's Ministry of Defence announces acquisition of three Gulfstream G550 Maritime Surveillance Aircraft (MSA)

In a move to fortify Singapore's critical information infrastructure (CII) against the rising tide of advanced persistent threats (APTs) and hybrid warfare, the Ministry of Defence (MINDEF) has announced the formation of Sectoral Cyber Defence Teams (SCDTs), beginning operations in June 2026. This initiative, unveiled during the Committee of Supply debate by Defence Minister Chan Chun Sing and Senior Minister of State Zaqy Mohamad, marks a strategic shift from reactive incident response to a proactive, integrated defense posture. By leveraging the specialized civilian expertise of National Servicemen (NSmen) within the Digital and Intelligence Service (DIS), the SCDTs are designed to bridge the gap between military readiness and civilian resilience in high-stakes sectors such as telecommunications, energy, and transport. These teams will operate under the DIS Defence Cyber Command's Cyber Protection Group, establishing sector-specific communities to share best practices and intelligence on emerging threat vectors.

Technically, the SCDTs will be supported by the first phase of the Singapore Armed Forces' (SAF) new digital range, also slated for 2026, which utilizes AI-driven simulations to model sophisticated adversary behaviours and stress-test defences in a controlled environment. This development coincides with broader national efforts, including the recent "Exercise SG Ready" and the multinational "Defence Cyber Marvel" exercise, highlighting Singapore's focus on securing sea lines of communication and digital connectivity. The integration of the SCDTs represents a crucial evolution in risk management, acknowledging that the boundaries between corporate and national security are increasingly blurred. For defenders and policy stakeholders, the deployment signals a commitment to persistent engagement and deep collaboration, ensuring that the city-state remains resilient against the escalating geopolitical and technological risks that define the modern cyber threat landscape.

Read more: https://www.mindef.gov.sg/news-and-events/latest-releases/27feb26-fs/

Middle East | West Asia

Operation Olalampo: Inside Muddy Water's Latest Campaign

Group-IB researchers have uncovered a sophisticated multi-stage campaign dubbed "Operation Olalampo," attributed to the Iranian state-linked threat actor Muddy Water (also known as Mango Sandstorm or Static Kitten), targeting entities across Israel, Saudi Arabia, India, and Portugal. This activity aligns with heightened geopolitical tensions in the Middle East and underscores a persistent trend where regional intelligence requirements drive aggressive cyber espionage operations against critical infrastructure and government sectors. The campaign, which has been active since at least early 2024, utilizes a refined infection chain that begins with spear-phishing emails containing lures disguised as legitimate administrative or security-themed documents hosted on cloud services like Egnyte. Technically, the operation is characterized by the deployment of a new, customized variant of the "MuddyRot" backdoor, which leverages the Windows DLL side-loading technique via a legitimate executable to evade traditional endpoint detection and response (EDR) solutions. Once executed, the malware establishes persistent command-and-control (C2) communication over port 443, utilizing a unique obfuscated protocol to exfiltrate system metadata and receive instructions.

Analysts identified specific behaviour patterns, including the use of compromised legitimate credentials to move laterally through the network via Remote Desktop Protocol (RDP) and the deployment of the "Ligolo-ng" tunnelling tool to facilitate deep network penetration. The threat actors also demonstrated high operational security by rotating C2 infrastructure frequently and utilizing PowerShell scripts for in-memory execution to minimize their disk footprint. For risk management teams, this development highlights the critical need for robust identity and access management (IAM) and the monitoring of unusual egress traffic to known cloud storage providers. The evolution of Muddy Water's toolkit demonstrates a shift toward more modular, stealthy implants, signalling a broader maturation in Iranian offensive cyber capabilities that poses a long-term threat to international stability and corporate resilience in contested digital environments.

Read more: https://www.group-ib.com/blog/muddywater-operation-olalampo/

PromptSpy ushers in the era of Android threats using GenAI

ESET Research has identified a groundbreaking evolution in mobile espionage with the discovery of PromptSpy, an Android-based malware family utilized by the Iranian-linked threat actor APT42 (also known as Charming Kitten). This development marks a critical inflection point in the threat landscape, as it represents the first documented instance of a state-aligned group weaponizing Generative AI (GenAI) to enhance the efficacy and scale of social engineering and data collection. Situated within the broader context of escalating Middle Eastern geopolitical tensions, PromptSpy targets individuals associated with government, defence, and civil society, demonstrating how LLMs are being integrated into the malware development lifecycle to lower the barrier for high-fidelity phishing. The campaign utilizes trojanized applications often masquerading as legitimate AI assistants or regional utilities to gain extensive permissions on victim devices. Once installed, the malware establishes persistence and executes a multi-stage payload capable of exfiltrating SMS logs, contact lists, and call history, while also utilizing the device's microphone for environmental eavesdropping.

Technically, the GenAI component is leveraged to generate highly personalized and context-aware phishing lures that adapt to the victim's language and professional background, significantly increasing the likelihood of successful credential harvesting. The infrastructure relies on a series of command-and-control (C2) servers that utilize encrypted protocols to mask exfiltration traffic from network-level detection. For risk management professionals, PromptSpy signals the end of "generic" social engineering; the automation of rapport-building through AI makes traditional user awareness training increasingly obsolete. The broader implications suggest a future where cyber resilience must focus on "Zero Trust" mobile architectures and behavioural analysis of application permissions rather than simple indicator matching. As APT42 continues to refine these AI-augmented tactics, the international community faces a surge in high-precision espionage that challenges the stability of sensitive diplomatic and corporate communications.

Read more: https://www.welivesecurity.com/en/eset-research/promptspy-ushers-in-era-android-threats-using-genai/

Malware & Vulnerabilities

Detecting and preventing distillation attacks

Anthropic has detailed a proactive defensive framework to mitigate "distillation attacks," a sophisticated form of model extraction where third-party actors ranging from corporate competitors to state-linked threat groups attempt to replicate the proprietary intelligence and nuanced alignment of frontier Large Language Models (LLMs) by training smaller "student" models on the outputs of a target "teacher" model. This development emerges as a critical priority in the AI safety and cybersecurity landscape, where the theft of high-integrity model weights and fine-tuning logic represents a new frontier of intellectual property exfiltration and national security risk. For defenders, distillation is not merely a commercial concern but a vector for bypassing safety guardrails, as adversaries can distil a model to retain its utility while stripping away its ethical constraints or "refusals." Anthropic's technical disclosure focuses on a multi-layered detection strategy, utilizing advanced pattern recognition to identify anomalous query behaviour such as systematic, high-volume requests for reasoning chains or structured outputs that are characteristic of "synthetic data generation" for training purposes.

The operational details include the implementation of rate-limiting throttles and the injection of subtle, non-disruptive watermarks into model responses, which serve as indicators of compromise should a distilled model be deployed elsewhere. Furthermore, the defence leverages behavioural heuristics to distinguish between legitimate high-intensity enterprise use and automated extraction attempts targeting specific logical domains. These developments reflect a shift from static perimeter defence to dynamic, algorithmic monitoring of the "intelligence interface." For risk management and policy stakeholders, these findings underscore that the security of AI is no longer limited to data privacy but extends to the preservation of the model's "cognitive" architecture. This initiative fits into a larger global pattern of "model hardening," emphasizing that as AI becomes a central pillar of critical infrastructure, the resilience of international stability will depend on the ability to prevent the uncontrolled proliferation of frontier-level capabilities through illicit reverse-engineering.

Read more: https://www.anthropic.com/news/detecting-and-preventing-distillation-attacks

Divide and conquer: how the new Keenadu backdoor exposed links between major Android botnets

The cybersecurity landscape is witnessing the emergence of a highly sophisticated Android backdoor dubbed Keenadu, identified by researchers at Kaspersky as a potent tool for targeted mobile espionage. This discovery highlights a growing trend where advanced threat actors leverage mobile platforms often the weakest link in the corporate security perimeter to gain persistent access to sensitive personal and professional data. Against a backdrop of heightening geopolitical competition, the development of such specialized surveillance tools underscores the shift toward high-stakes mobile intelligence gathering. Keenadu is distributed through malicious applications disguised as legitimate services, utilizing a modular architecture to evade traditional signature-based detection. Technically, the backdoor exploits Android's Accessibility Services and notification listeners to intercept SMS messages, record calls, and exfiltrate contact lists and geographic location data. Once installed, it establishes communication with a remote command-and-control (C2) server via encrypted protocols, allowing operators to execute shell commands and deploy additional payloads tailored to the victim's environment.

The malware employs sophisticated anti-analysis techniques, including code obfuscation and environmental checks, to detect if it is running within a sandbox or debugger, ensuring a low-profile footprint. The broader implications for risk management are significant, as Keenadu demonstrates the increasing accessibility of tier-one surveillance capabilities to a wider array of state-linked and private mercenary groups. For national and corporate security stakeholders, this development necessitates a transition toward rigorous mobile device management (MDM) and "Zero Trust" mobile architectures. As mobile devices become centralized hubs for multi-factor authentication and sensitive communications, the persistence of actors like those behind Keenadu poses a fundamental threat to cyber resilience. This incident fits into a larger pattern of "surveillance-as-a-service," where the integrity of international diplomatic and corporate communications is continuously challenged by stealthy, firmware-adjacent mobile threats.

Read more: https://securelist.com/keenadu-android-backdoor/118913/?

Cline CLI 2.3.0 Supply Chain Attack Installed OpenClaw on Developer Systems

A critical supply chain attack has targeted the software development ecosystem through a malicious version of the Cline CLI (version 2.3.0), an increasingly popular open-source tool for integrating AI-driven coding assistants. This incident marks a significant escalation in the targeting of developer environments, where threat actors exploit the implicit trust in productivity tools to gain a foothold in the software supply chain. Amidst the rapid adoption of AI-assisted development, this development highlights the persistent risk of "typosquatting" and poisoned updates in package repositories, which now serve as high-leverage entry points for state-sponsored and financially motivated actors seeking to compromise downstream enterprise environments. Technical analysis reveals that the rogue version of Cline CLI was injected with a heavily obfuscated post-install script designed to initiate a multi-stage infection vector. Upon execution, the script performs environmental checks to detect sandboxing before deploying a second-stage payload a bespoke credential harvester capable of exfiltrating sensitive .env files, AWS access keys, and SSH identities to an actor-controlled command-and-control (C2) server.

Notably, the malware utilizes the legitimate npm lifecycle hooks to maintain persistence and bypass standard endpoint detection by masquerading as routine package maintenance. The geographic scope appears global, with indicators of compromise (IoCs) surfacing in build pipelines across the technology and financial sectors. For risk management and policy stakeholders, this breach underscores the critical necessity of "shifting left" on security, mandating rigorous checksum verification and the use of private, audited registries for all third-party dependencies. The broader implications suggest that as AI tools become central to the development lifecycle, they simultaneously become a prime surface for supply chain interdiction. This incident reinforces a larger pattern in the threat landscape where the automation of software delivery is weaponized to facilitate silent, large-scale exfiltration, demanding a transition toward zero-trust principles within the DevOps pipeline to ensure international cyber resilience.

Read more: https://thehackernews.com/2026/02/promptspy-android-malware-abuses-google.html?

PromptSpy ushers in the era of Android threats using GenAI

ESET Research has identified a groundbreaking evolution in mobile espionage with the discovery of PromptSpy, an Android-based malware family utilized by the Iranian-linked threat actor APT42 (also known as Charming Kitten). This development marks a critical inflection point in the threat landscape, as it represents the first documented instance of a state-aligned group weaponizing Generative AI (GenAI) to enhance the efficacy and scale of social engineering and data collection. Situated within the broader context of escalating Middle Eastern geopolitical tensions, PromptSpy targets individuals associated with government, defence, and civil society, demonstrating how LLMs are being integrated into the malware development lifecycle to lower the barrier for high-fidelity phishing. The campaign utilizes trojanized applications often masquerading as legitimate AI assistants or regional utilities to gain extensive permissions on victim devices.

Once installed, the malware establishes persistence and executes a multi-stage payload capable of exfiltrating SMS logs, contact lists, and call history, while also utilizing the device's microphone for environmental eavesdropping. Technically, the GenAI component is leveraged to generate highly personalized and context-aware phishing lures that adapt to the victim's language and professional background, significantly increasing the likelihood of successful credential harvesting. The infrastructure relies on a series of command-and-control (C2) servers that utilize encrypted protocols to mask exfiltration traffic from network-level detection. For risk management professionals, PromptSpy signals the end of "generic" social engineering; the automation of rapport-building through AI makes traditional user awareness training increasingly obsolete. The broader implications suggest a future where cyber resilience must focus on "Zero Trust" mobile architectures and behavioural analysis of application permissions rather than simple indicator matching. As APT42 continues to refine these AI-augmented tactics, the international community faces a surge in high-precision espionage that challenges the stability of sensitive diplomatic and corporate communications.

Read more: https://www.welivesecurity.com/en/eset-research/promptspy-ushers-in-era-android-threats-using-genai/

About the Author

Govind Nelika is the Researcher / Web Manager / Outreach Coordinator at the Centre for Land Warfare Studies (CLAWS). He is an alumnus of Pondicherry Central University with a degree in Political Science complemented by a certification in Data Sciences from IBM. His research approach is multidisciplinary in nature, and his focus area at CLAWS is on emerging challenges and trends in the fields of Cybersecurity, OSINT, and the evolving landscape of Strategic Technology, synergized with Generative AI and LLM. In recognition of his contributions, he was awarded the Chief of Army Staff (COAS) Commendation Card on Army Day 2025 for his work with CLAWS.

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