CLAWS Newsletter

Cyber Index | Volume II | Issue 03

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

DRDO tests ramjet technology: Why it is big boost for India’s defence

In a major leap for indigenous aerospace engineering, India’s Defence Research and Development Organisation (DRDO) successfully demonstrated its Solid Fuel Ducted Ramjet (SFDR) technology on February 3, 2026. This breakthrough, conducted at the Integrated Test Range in Chandipur, Odisha, addresses a critical gap in high-altitude aerial dominance and long-range interception capabilities. In the contemporary geopolitical landscape, the mastery of air-breathing propulsion is a strategic imperative, allowing defenders to outpace conventional rocket-powered threats that lose kinetic energy in their terminal phases. By utilizing atmospheric oxygen rather than carrying a heavy internal oxidizer, the SFDR system provides sustained thrust, significantly expanding the “No-Escape Zone” for beyond-visual-range (BVR) engagements.

The flight test validated several high-precision subsystems, including a nozzle-less booster, a solid fuel gas generator, and a sophisticated fuel flow controller. Operational details confirm that the missile was initially accelerated by a ground booster to a specific Mach number, after which the ramjet sustainer ignited, drawing air through cheek-mounted titanium-alloy intakes to maintain supersonic speeds between Mach 2 and Mach 3.8. Technically, the system utilizes a boron-based high-energy fuel and an indigenous hot gas valve capable of regulating combustion at temperatures up to 1400K. These advancements are specifically slated for integration into the Astra Mk-III missile program, aiming for strike ranges between 250 km and 350 km. For practitioners, this development signals a shift toward throttleable thrust control in missile design, enabling manoeuvres that can overcome the high-g evasive tactics of modern agile aircraft.

Ultimately, the SFDR success elevates India into an elite tier of nations alongside the U.S., Russia, and select European powers possessing operational ramjet capabilities. This achievement bolsters national security by reducing reliance on foreign propulsion technologies and provides a credible deterrent in regional high-stakes theatres. For the global threat landscape, the proliferation of such long-range precision engagement tools necessitates a re-evaluation of current electronic warfare and kinetic defence architectures, as the era of “first look, first-shoot” air combat increasingly favours platforms capable of sustained supersonic persistence.

Read more: https://www.firstpost.com/explainers/drdo-sfdr-ramjet-technology-india-defence-significance-13976224.html

HORIBA acquires Pristine Deeptech Private Limited in India

In a move that underscores the tightening intersection of industrial automation, semiconductor supply chains, and specialized technology acquisition, Japanese precision instrument manufacturer Horiba, through its subsidiary Horiba India, has successfully acquired Pristine Deeptech Private Limited. This strategic integration occurs against a backdrop of intensified global competition for high-purity fluid and gas management systems critical components in the fabrication of advanced semiconductors and high-performance chemicals. As nations move to secure their “deeptech” sovereign capabilities, the consolidation of niche technical expertise by global conglomerates like Horiba highlights a shift toward vertical integration as a defence against supply chain volatility. Pristine Deeptech, an Indian enterprise specializing in high-precision fluid handling solutions, brings critical operational capabilities in the design and manufacture of mass flow controllers (MFCs), liquid delivery systems, and pressure control technologies.

Technically, the acquisition targets Pristine’s proficiency in managing ultra-high-purity (UHP) environments, where even microscopic contamination can lead to catastrophic yield loss in semiconductor manufacturing. These systems utilize sophisticated sensor-actuator loops and digital communication protocols such as EtherCAT and DeviceNet to regulate the precise volumetric flow of corrosive and pyrophoric gases. From a cybersecurity perspective, the integration of these industrial control system (ICS) components into Horiba’s global framework necessitates rigorous vetting of firmware integrity and supply chain provenance to prevent downstream hardware-level vulnerabilities or “backdoor” exploits in critical manufacturing infrastructures.

The move signals Horiba's intent to leverage India not just as a consumer market, but as a specialized R&D hub for the next generation of precision hardware. For risk management and policy stakeholders, this development reflects the expanding footprint of the Quad-aligned technology ecosystem, emphasizing that the resilience of the global cyber-physical landscape is increasingly dependent on the secure, localized production of high-precision instrumentation that sits at the foundation of modern digital infrastructure.

Read more: https://etedge-insights.com/in-focus/trending/horiba-acquires-pristine-deeptech-private-limited-in-india/

Adani Defence & Aerospace and Leonardo Forge Strategic Partnership to Build India's Helicopter Ecosystem

In a significant move for India's indigenous defence industrial base, Adani Defence & Aerospace and Italy's Leonardo S.p.A. have signed a landmark Memorandum of Understanding (MoU) to establish a comprehensive helicopter ecosystem in India. This strategic partnership emerges amidst a global shift toward localized defence manufacturing and "friend-shoring," as nations seek to mitigate supply chain vulnerabilities and technological dependencies on traditional power blocs. For defenders and decision-makers, this development is a critical marker in the "Aatmanirbhar Bharat" (Self-Reliant India) initiative, reflecting a broader geopolitical trend where private corporate giants are increasingly integrated into national security architectures. The collaboration specifically targets the design, manufacturing, and lifecycle support of advanced rotorcraft, positioning the partnership to compete for major Indian military contracts, including the Naval Utility Helicopter (NUH) and Indian Multirole Helicopter (IMRH) programs.

Operationally, the agreement focuses on the co-production of Leonardo's AW149 a multi-role medium-lift helicopter and potentially the AW109 and AW139 platforms. Technical integration involves the transfer of critical technologies for structural components, high-precision transmission systems, and advanced avionics, with plans to establish a Global Maintenance, Repair, and Overhaul (MRO) facility in India. This move addresses the operational fatigue of India's aging legacy fleets, such as the Cheetah and Chetak, by introducing platforms equipped with modern sensor suites, secure communication protocols, and enhanced ballistic protection. From a risk management perspective, the localized production of these systems significantly reduces the "cyber-physical" risk associated with foreign-sourced software updates and hardware components, ensuring greater sovereign control over the integrity of military assets. Ultimately, this partnership signals a maturing of India's private defence sector, evolving from a parts supplier to a systems integrator. For international stability and regional power dynamics, the Adani-Leonardo alliance strengthens India's domestic aerospace resilience, providing a blueprint for how large-scale industrial partnerships can reshape the global arms trade and the technological risk landscape of the 21st century.

Read more: https://www.leonardo.com/en/press-release-detail/-/detail/03-02-2026-adani-defence-aerospace-and-leonardo-forge-strategic-partnership-to-build-india-s-helicopter-ecosystem

Will ban you for sharing users' personal data, SC warns WhatsApp

In a significant escalation of judicial oversight within the world's largest internet market, the Supreme Court of India has issued a stern warning to Meta Platforms and its subsidiary WhatsApp, threatening a total ban on the platform's data-sharing practices if strict privacy safeguards are not guaranteed. The intervention, led by Chief Justice Surya Kant on February 3, 2026, centres on a long-standing dispute regarding WhatsApp's 2021 privacy policy, which the Competition Commission of India (CCI) previously flagged as an abuse of market dominance. This development underscores a growing global regulatory shift toward scrutinizing "surveillance capitalism," where the "take-it-or-leave-it" consent models of dominant digital utilities are increasingly viewed as coercive rather than voluntary.

The bench characterized the automated extraction of metadata for commercial exploitation as a "decent way of committing theft," specifically targeting Meta's practice of leveraging cross-platform behavioural data such as monitoring user interactions to serve targeted ads on Instagram and Facebook even while message content remains end-to-end encrypted. Strategically, the court impleaded the Ministry of Electronics and Information Technology (MeitY) to address the limitations of the Digital Personal Data Protection (DPDP) Act of 2023, which judges noted lacks specific provisions for the economic valuation and "rent-sharing" of user data. Defenders should note the court's skepticism toward technically complex opt-out mechanisms, which it deemed unintelligible to the average consumer.

With an interim directive expected on February 10, the case signals a potential judicial redefinition of data ownership and "manufactured consent." For global tech entities, this serves as a critical indicator that operational persistence in India will increasingly require de-linking core messaging services from secondary advertising-driven data harvesting, potentially disrupting established monetization frameworks across the broader cyber threat and risk landscape.

Read more: https://timesofindia.indiatimes.com/india/will-ban-you-for-sharing-users-personal-data-sc-warns-whatsapp/articleshow/127896776.cms

External

Global Focus Brief

Senior Officials Announced for the War Department's Six Critical Technology Areas

The United States Department of Defence (DoD), spearheaded by the Office of the Under Secretary of Defence for Research and Engineering (OUSD(R&E)), has solidified a centralized leadership structure for its Critical Technology Areas (CTAs), marking a pivotal shift in how the Pentagon prioritizes emerging cybersecurity and dual-use technological risks. This strategic consolidation arrives as global geopolitical tensions accelerate the race for "technological sovereignty," where dominance in sectors like microelectronics, quantum science, and future-generation wireless (5G/NextG) serves as the primary determinant of national security and cyber resilience. By appointing senior officials to oversee these specific domains, the DoD aims to bridge the "valley of death" between laboratory innovation and operational deployment, specifically addressing the vulnerabilities inherent in globalized hardware supply chains and the rapid advancement of adversary AI capabilities. The formalized oversight structure focuses on fourteen distinct CTAs, categorized into three strategic pillars: Seizing the Initiative, Defence-Specific, and Foundational Technologies.

Operational details indicate a heavy emphasis on hardening Trusted AI and Autonomy frameworks, securing microelectronics through "quantifiable assurance" programs, and advancing Directed Energy and Hypersonic areas where data integrity and signal protection are critical to kinetic mission success. For cybersecurity practitioners, this move signals a transition toward a "secure-by-design" mandate for the next generation of defence infrastructure, prioritizing the mitigation of side-channel attacks on quantum-resistant cryptography and the protection of software-defined networking (SDN) protocols. The broader implications for risk management are significant; it signals to industry and international partners that the U.S. will increasingly tie its procurement and defence cooperation to rigorous cybersecurity standards within these high-priority verticals. Ultimately, this structural development reflects a maturing threat landscape where the distinction between commercial innovation and military application has largely dissolved, necessitating a unified, policy-driven approach to maintaining a strategic advantage in an era of persistent, multi-domain cyber competition.

Read more: https://www.cto.mil/cta-senior-officials/

SpaceX seeks FCC nod for solar-powered satellite data centres for AI

SpaceX has formally petitioned the Federal Communications Commission (FCC) for authority to deploy a massive constellation of up to one million solar-powered satellites designed to function as an "Orbital Data

Center" system. This strategic move, which follows reports of a potential merger between SpaceX and Elon Musk's AI venture, xAI, marks an aggressive pivot from satellite-based telecommunications to space-resident high-performance computing (HPC). By situating AI infrastructure in low Earth orbit (LEO), SpaceX aims to bypass the terrestrial "capacity crunch" defined by escalating power grid instability, land-use restrictions, and the immense water requirements of traditional cooling systems. The proposed architecture leverages narrow orbital shells between 500 km and 2,000 km, utilizing sun-synchronous inclinations to ensure near-constant solar irradiance and employing radiative heat dissipation to manage the thermal loads of dense AI inference.

Technically, the system will rely on high-bandwidth optical inter-satellite links (ISLs) to form a space-based mesh network, effectively treating the existing Starlink constellation as a secondary backhaul layer. SpaceX's filing outlines a vision where a million tonnes of orbiting mass could deliver approximately 100 gigawatts of compute capacity, with data processing occurring "in-situ" to reduce terrestrial bandwidth demand by up to 90%. For defenders and policymakers, this development signals a fundamental shift in the cyber threat landscape, introducing a decentralized, orbital edge-computing layer that exists beyond traditional sovereign jurisdictions. While the proposal faces significant regulatory hurdles including FCC scrutiny over orbital debris and spectrum interference it establishes a new frontier for cyber resilience and international competition. If realized, this orbital fabric would redefine cloud infrastructure, necessitating novel risk management frameworks for space-based assets that are critical to global AI workloads and national economic security.

Read more: https://www.reuters.com/business/aerospace-defense/spacex-seeks-fcc-nod-solar-powered-satellite-data-centers-ai-2026-01-31/

The Shadow Campaigns: Uncovering Global Espionage

In a sophisticated demonstration of cross-continental cyber espionage, Unit 42 has identified a sprawling series of "shadow campaigns" attributed to the Chinese state-linked threat actor group, likely operating under the umbrella of APT41 or a closely related cluster. This activity emerges at a critical juncture in the global threat landscape, where state-sponsored entities are increasingly pivoting from noisy, disruptive attacks to long-term, stealthy persistent presence within high-value targets. This development matters to defenders because it highlights a shift toward "infrastructure-as-a-service" exploitation, where actors weaponize legitimate cloud and edge-of-network resources to mask their origins, complicating attribution and defensive response. The primary actors have targeted a diverse array of sectors, including government ministries, telecommunications providers, and technology firms across Southeast Asia, Europe, and North America, signalling a strategic priority for data exfiltration and intellectual property theft.

Technically, the campaigns are characterized by the use of bespoke malware frameworks, specifically the "ShadowPad" modular trojan and a newly identified backdoor dubbed "SPARK." Operational details reveal a high reliance on "living-off-the-land" (LotL) techniques, such as the abuse of legitimate Windows binaries (Side-Loading) to execute malicious code while bypassing signature-based detection. The actors have been observed exploiting N-day vulnerabilities in public-facing software, specifically targeting VPN gateways and web servers to establish initial access. Once inside, they employ advanced credential harvesting tools and utilize specific command-and-control (C2) protocols that mimic legitimate HTTP/S traffic, making detection via traditional firewalls difficult. Indicators of compromise (IoCs) point to a sustained operational timeline spanning over eighteen months, with specific geographic clusters suggesting a coordinated effort to monitor regional geopolitical developments.

The broader implications for risk management are significant, as these shadow campaigns underscore the erosion of traditional network perimeters and the necessity for deep, behavioural-based telemetry. For corporate and national security stakeholders, this fits into a larger pattern of "silent" espionage where the goal is not disruption but the slow, methodical siphoning of strategic data. This development mandates that organizations transition toward a Zero Trust posture and prioritize the hardening of edge devices, which have become the primary entry points for state-level adversaries. Ultimately, maintaining cyber resilience in this environment requires a departure from reactive patching toward proactive threat hunting and the integration of high-fidelity intelligence to unmask the infrastructure used by sophisticated state actors before they achieve their long-term objectives.

Read more: https://unit42.paloaltonetworks.com/shadow-campaigns-uncovering-global-espionage/

Russian Stealth Jets Arrive in North Africa, Captured on Video by Algerian Farmer

Open-source intelligence (OSINT) surfacing in February 2026 suggests a pivotal shift in North Africa's military landscape following the apparent delivery of Russia's Su-57 "Felon" stealth fighters to the Algerian Air Force. This development, captured in civilian footage near the Oum El Bouaghi Air Base, positions Algeria as the first international operator of the fifth-generation platform, marking a strategic success for the Kremlin in bypassing Western isolation and the Countering America's Adversaries Through Sanctions Act (CAATSA).

The arrival follows an October 2025 data breach by the hacker collective Black Mirror, which leaked internal Rostec documents detailing a $2 billion procurement for 14 Su-57 aircraft and 14 Su-34 fighter-bombers. These leaked spreadsheets, linked to the AO KRET avionics firm, specified a $200 million package for advanced electronics, including the N036 Byelka AESA radar and the L402 Himalayan electronic warfare suite. Technical analysis of the recent flight visuals indicates the airframes likely feature the latest "new technical configuration" recently touted by United Aircraft Corporation (UAC), which integrates updated mission computers for sensor fusion and passive optical-electronic tracking to maintain low observability.

For defenders and regional analysts, this deployment introduces sophisticated signals intelligence (SIGINT) and low-probability-of-intercept (LPI) radar capabilities into a highly contested airspace, complicating NATO's southern flank maritime and aerial surveillance. The integration of these stealth assets not only intensifies the longstanding arms race between Algiers and Rabat but also signals a broader trend where state-linked aerospace entities utilize non-aligned markets to sustain high-tech production despite global sanctions. Ultimately, the move reinforces a multipolar cyber and technological risk environment, as advanced Russian avionics and stealth-driven doctrines are successfully exported to regional powerhouses, challenging traditional Western air superiority and necessitating a recalibration of regional deterrence strategies.

Read more: https://news.defcros.com/russian-stealth-jets-arrive-in-north-africa-captured-on-video-by-algerian-farmer/

Lockheed Martin and Fujitsu to accelerate dual-use technology development

Fujitsu Limited has officially announced the launch of a pioneering "AI Trust Infrastructure," a comprehensive suite of security and governance technologies designed to address the escalating risk of adversarial machine learning and the proliferation of sophisticated deepfakes in corporate environments. This strategic rollout arrives at a critical juncture as organizations face a surge in "identity-centric" attacks, where generative AI is increasingly weaponized by state-linked groups and cybercriminal syndicates to bypass biometric authentication and execute social engineering at scale. By integrating specialized authenticity-verification layers directly into the data lifecycle, Fujitsu seeks to provide a definitive countermeasure to the "hallucination" and "poisoning" vulnerabilities inherent in Large Language Models (LLMs) and automated decision-making systems. Technically, the infrastructure utilizes a fusion of digital watermarking, blockchain-backed provenance tracking, and real-time anomaly detection to verify the integrity of both data inputs and AI-generated outputs.

A core component of the release is the "AI Audit Trail" protocol, which provides a transparent, tamper-proof record of model training and inference processes, effectively mitigating the risk of subtle parameter tampering or unauthorized data exfiltration via model inversion. For cybersecurity practitioners, this development signals a shift from traditional perimeter defense to a "Content-Zero Trust" model, where the veracity of digital assets must be continuously validated. The broader implications for risk management are profound; as AI becomes foundational to critical infrastructure and financial services, the ability to ensure "Truth-as-a-Service" is essential for maintaining operational resilience and public trust. Fujitsu's move highlights a growing global trend toward the institutionalization of AI governance, underscoring that the next phase of the cyber threat landscape will be defined by the struggle to secure the data supply chains that fuel automated intelligence. For decision-makers, this framework offers a necessary blueprint for navigating the dual challenges of rapid AI adoption and the persistent threat of sophisticated digital deception.

Read more: https://global.fujitsu/en-global/pr/news/2026/02/02-02?

United Kingdom of Great Britain and Northern Ireland

The Information Commissioner's Office (ICO) UK, announces investigation into Grok

In a significant move targeting the intersection of generative AI and data sovereignty, the UK's Information Commissioner's Office (ICO) launched a formal investigation into X Internet Unlimited Company (XIUC) and xAI LLC on February 3, 2026. The probe focuses on the Grok artificial intelligence system and its role in the mass production of non-consensual sexualized deepfakes, including content depicting minors. This regulatory escalation reflects a broader global crackdown on "unconstrained" AI development, where the speed of innovation often outpaces the implementation of necessary safety guardrails. For defenders and practitioners, the case serves as a critical test of the "Privacy by Design" mandate under the UK GDPR, especially as AI models increasingly ingest and manipulate personal data at an unprecedented scale.

The ICO is specifically scrutinizing whether xAI and X processed personal data lawfully, fairly, and transparently during the development and deployment of Grok. Operational details suggest that Grok's image generation tools were exploited to produce approximately 3 million sexualized images in less than two weeks, bypassing initial filters. The investigation will examine the technical design choices, the adequacy of safeguards built into the model to prevent the generation of harmful synthetic media, and the legal bases for utilizing living individuals' data in such high-risk contexts. This inquiry coincides with a physical raid by the Paris prosecutor's cybercrime unit on X's French headquarters, highlighting a coordinated European effort to hold tech giants accountable for algorithmic harms.

The broader implications for risk management are profound, as the ICO wields the power to impose fines of up to £17.5 million or 4% of global annual turnover. For the corporate security landscape, this development underscores that AI safety is no longer just an ethical concern but a high-stakes legal liability. As SpaceX recently announced the acquisition of xAI in a $1.25 trillion merger, the regulatory fallout could influence the valuation and operational standards of the next generation of "agentic" AI systems. Ultimately, the Grok investigation signals that regulators will aggressively bridge the gap between data protection and online safety, requiring AI developers to prioritize robust, verifiable safeguards before releasing transformative technologies into the public domain.

Read more: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2026/02/ico-announces-investigation-into-grok/

United States of America (USA)

UAE National Security Adviser Buy Secret Stake in Trump Company

$500 million investment for 49% of World Liberty came months before U.A.E. won access to tightly guarded American AI chips

In a significant intersection of digital finance and geopolitical strategy, a $500 million investment by Emirati officials into World Liberty Financial (WLF), a cryptocurrency venture controlled by the Trump family, has emerged as a focal point for national security scrutiny. The central figure, Sheikh Tahnoon bin Zayed Al Nahyan the United Arab Emirates' National Security Adviser often termed the "spy sheikh" leveraged Aryam Investment 1 to acquire a 49% stake in WLF just four days prior to the 2025 presidential inauguration. This development highlights the escalating risk landscape where nascent Decentralized Finance (DeFi) platforms serve as conduits for massive foreign capital inflows to high-ranking domestic officials, potentially bypassing traditional financial oversight and creating profound conflicts of interest. Factual disclosures indicate that an initial $250 million instalment saw approximately $187 million directed toward Trump-linked entities like DT Marks DEFI LLC, with another $31 million flowing to associates of Steve Witkoff, the U.S. Special Envoy to the Middle East.

Technically, the deal's implications expanded in March 2025 when MGX, another Tahnoon-led entity, utilized WLF's USD1 stablecoin to facilitate a $2 billion investment into the Binance exchange, effectively bootstrapping the stablecoin's liquidity and market capitalization. Analysts observe that these financial manoeuvres closely preceded the administration's pivotal policy shift to approve the export of 500,000 advanced H100-class AI semiconductors to the UAE a move previously restricted due to concerns over technology leakage to the People's Republic of China (PRC). For defenders and risk managers, this pattern underscores a evolving threat model where "crypto-cleptocracy" and the monetization of policy access through stablecoin ecosystems challenge international stability and supply chain integrity. The convergence of sovereign wealth, emerging fintech, and dual-use technology transfers suggests that future cyber resilience must account for the strategic use of crypto-assets as tools of statecraft and influence.

Read more: https://www.wsj.com/politics/policy/spy-sheikh-secret-stake-trump-crypto-tahnoon-ea4d97e8

Musk reorganizes xAI after SpaceX merger and ahead of blockbuster IPO

Elon Musk's recent restructuring of xAI marks a pivotal shift in the artificial intelligence landscape, characterized by the company's absorption into SpaceX to form a $1.25 trillion conglomerate ahead of a planned 2026 initial public offering. This reorganization, occurring amid high-profile leadership attrition with co-founders Tony Wu and Jimmy Ba joining an exodus that has halved the original founding team signals a transition from a research-heavy startup to a vertically integrated enterprise focused on "velocity and acceleration." The operational pivot establishes four primary development verticals: Grok (chatbot and voice), Imagine (multimedia and video generation), Coding, and a newly formed "Macrohard" division led by Toby Pohlen. Macrohard is specifically tasked with developing autonomous AI agents capable of managing corporate workflows and decision-making, reflecting a broader industry trend toward agentic AI that acts as an operator rather than a mere interface.

From a technical and risk perspective, the restructure emphasizes a massive scaling of infrastructure, with xAI leveraging a 1 million Nvidia H100 GPU-equivalent training cluster and proposing 200-gigawatt space-based data centres supported by SpaceX. However, this expansion is shadowed by significant regulatory and safety concerns; Grok has recently drawn international scrutiny and French cybercrime investigations over its role in generating non-consensual explicit deepfakes and disseminating disinformation. For cybersecurity practitioners and policy stakeholders, xAI's evolution into a dual-use space and AI entity heightens the stakes for supply chain integrity and the secure deployment of autonomous agents. The development suggests that the next frontier of cyber risk will not only involve the models themselves but the orbital infrastructure and autonomous administrative layers that underpin them, necessitating a more robust framework for cross-domain resilience as AI begins to operate at "interstellar" scale.

Read more: https://www.reuters.com/business/musk-says-xai-was-reorganized-2026-02-11/

Kingdom of Saudi Arabia – PATRIOT Advanced Capability-3 Missile Segment Enhancement Missiles

The U.S. State Department has formally approved a potential $2.24 billion Foreign Military Sale to the Kingdom of Saudi Arabia for Patriot Advanced Capability-3 (PAC-3) Missile Segment Enhancement (MSE) missiles, a move that reinforces the critical nexus between kinetic defence and the cybersecurity of integrated air and missile defence (IAMD) systems. Situated within a volatile Middle Eastern security landscape, this development responds to the persistent threat of sophisticated unmanned aerial systems (UAS) and ballistic missiles deployed by regional adversaries and non-state actors. For defenders, the PAC-3 MSE represents more than an interceptor; it is a node in a highly networked environment where the security of data links and command-and-control (C2) integrity is paramount. The sale includes 250 PAC-3 MSE missiles, along with the necessary telemetry kits, technical documentation, and logistical support infrastructure. Technically, the PAC-3 MSE utilizes the Link-16 tactical data link protocol and advanced radar seek-and-track algorithms to facilitate hit-to-kill interceptions.

The reliance on these digitized communications channels introduces a significant attack surface for electronic warfare (EW) and signal intelligence (SIGINT) exploitation, as state-linked threat actors increasingly target the firmware and RF-based protocols governing tactical networks. This transaction underscores a broader shift toward "network-centric warfare," where the resilience of hardware is inextricably linked to the cybersecurity of the underlying software architectures. For global risk managers, the integration of these systems into the Saudi Royal Air Defence Forces highlights the necessity of robust supply chain security and the hardening of mission-critical systems against cyber-kinetic disruptions. As high-altitude defences become more data-dependent, the ability to maintain "integrity of intent" within these automated systems will be a defining factor in regional stability and the future of international defence cooperation.

Read more: https://www.dsca.mil/Press-Media/Major-Arms-Sales/Article-Display/Article/4394629/kingdom-of-saudi-arabia-patriot-advanced-capability-3-missile-segment-enhanceme

Lockheed Martin Unveils Lamprey MMAUV

Lockheed Martin's unveiling of the Lamprey Multi-Mission Autonomous Underwater Vehicle (MMAUV) marks a significant inflection point in the securitization of subsea critical infrastructure, a domain increasingly targeted by state-aligned threat actors for espionage and sabotage. As geopolitical tensions migrate toward the seabed the literal backbone of global internet traffic and energy distribution the Lamprey represents a shift toward persistent, autonomous defense and surveillance designed to mitigate risks to fiber-optic cables and energy pipelines. Technically, the system distinguishes itself through a modular open systems architecture (MOSA), allowing for rapid integration of specialized sensors for acoustic intelligence (ACINT) and electromagnetic sensing.

A critical feature of the Lamprey is its "non-tethered" autonomous navigation suite, which utilizes advanced sonar-based Simultaneous Localization and Mapping (SLAM) and inertial navigation systems (INS) to operate in GPS-denied environments. These capabilities are specifically engineered to counter "gray zone" activities, such as the deployment of parasitic taps or localized signal jamming by adversarial submersibles. For cybersecurity practitioners and national security stakeholders, the deployment of such platforms introduces a new layer of "underwater OT" (Operational Technology) that must be secured against electronic warfare and signal spoofing. The move reflects a broader trend in the defense landscape toward "Software-Defined Submersibles," where the primary value lies in the fusion of sensor data and autonomous decision-making algorithms rather than just physical durability. Ultimately, the Lamprey's introduction underscores the escalating necessity for integrated, cross-domain cyber resilience; as autonomous systems become the sentinels of the deep, the integrity of their data links and the security of their firmware become as vital to international stability as the physical infrastructure they are built to protect.

Read more: https://news.lockheedmartin.com/2026-02-09-Lockheed-Martin-Unveils-Lamprey-MMAUV-The-Deep-Doesnt-Let-Go

Elon Musk's SpaceX unveils 'Stargaze' to track thousands of satellites in real time

In a significant expansion of its orbital infrastructure, SpaceX has officially unveiled "Stargaze," a sophisticated situational awareness platform designed to provide real-time tracking and telemetry for the rapidly proliferating population of satellites in Low Earth Orbit (LEO). This development arrives at a critical juncture in the "New Space" era, where the collision of commercial interests and geopolitical rivalries has turned the orbital environment into a contested domain vulnerable to both physical debris and cyber-kinetic interference. For cybersecurity practitioners, Stargaze represents a pivotal shift toward a data-driven "Orbital Edge" security model, offering a centralized visibility layer that is essential for defending against satellite spoofing, signal jamming, and unauthorized orbital manoeuvres. Technically, the platform leverages high-fidelity data feeds from the Starlink constellation and terrestrial ground stations, employing automated algorithms to predict conjunction events and detect anomalous behaviour patterns consistent with state-sponsored interference.

By providing precise spatial coordinates and velocity vectors for thousands of assets, Stargaze addresses the "visibility gap" that has long plagued satellite operators, particularly as adversaries develop sophisticated anti-satellite (ASAT) capabilities and RF-based exploitation tools targeting the Link-16 and CCSDS protocols. The platform's integration of real-time monitoring suggests a move toward a "Zero Trust" framework for space assets, where the continuous verification of an object's position and signal integrity becomes the primary defence against orbital hijacking. Ultimately, the rollout of Stargaze signals a maturation of the space-based supply chain, highlighting that the future of international stability and corporate security now depends on the transparency of the orbital commons. For risk managers and policy stakeholders, this moves underscores the necessity of harmonizing cybersecurity standards with orbital traffic management to ensure that the rapid expansion of satellite constellations does not outpace the industry's ability to secure the critical data links sustaining global connectivity.

Read more: https://timesofindia.indiatimes.com/science/elon-musks-spacex-unveils-stargaze-to-track-thousands-of-satellites-in-real-time/articleshow/127888455.cms

People's Republic of China (PRC) | China

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

Singapore's Cyber Security Agency (CSA) has disclosed "Operation Cyber Guardian," a massive, 11-month multi-agency response to a sophisticated espionage campaign by the China-nexus threat actor UNC3886 targeting the nation's entire telecommunications sector. This disclosure highlights a critical shift in the threat landscape where state-linked groups prioritize edge devices and virtualization infrastructure to bypass traditional endpoint detection and response (EDR) solutions. In a series of deliberate and well-planned intrusions, UNC3886 targeted all four major Singaporean telcos Singtel, StarHub, M1, and SIMBA Telecom utilizing deep technical capabilities to gain a foothold in critical systems. The actor's toolkit included the weaponization of zero-day exploits to bypass perimeter firewalls and the deployment of advanced rootkits, such as the open-source REPTILE and MEDUSA, to maintain persistent, kernel-level access while evading forensic detection.

Technical analysis reveals that the group also utilized custom backdoors like MOPSLED and RIFLESPINE, which leverage trusted third-party services like GitHub and Google Drive for command-and-control (C2) traffic to blend in with legitimate network noise. While the CSA reports that the operation successfully contained the threat without service disruptions or large-scale data exfiltration, the group did manage to siphon network-related technical data to refine future targeting. For global defenders, this incident serves as a stark reminder of the strategic value of telecommunications as foundational national infrastructure. The campaign underscores the necessity of a coordinated "Whole-of-Government" defence doctrine and emphasizes that security for critical information infrastructure (CII) must now extend beyond the endpoint to include rigorous monitoring of hypervisors, network appliances, and encrypted C2 channels.

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/

The Chrysalis Backdoor: A Deep Dive into Lotus Blossom's toolkit

The threat research team at Rapid7 has released a comprehensive technical analysis of "Chrysalis," a sophisticated backdoor attributed to the state-sponsored threat group Lotus Blossom (also known as Spring Dragon or Billbug). This development highlights the enduring risk posed by persistent, Asia-based Advanced Persistent Threats (APTs) that target government and defence sectors to facilitate long-term espionage. In a landscape where defenders are increasingly focused on living-off-the-land (LotL) techniques, Chrysalis represents a return to specialized, modular malware designed for stealthy persistence and granular control over compromised Windows environments. Technically, the backdoor is characterized by its multi-stage loading process, typically initiating through DLL side-loading a technique that hijacks legitimate service execution to evade detection by standard Endpoint Detection and Response (EDR) solutions.

The malware employs an encrypted configuration block and custom communication protocols to establish a command-and-control (C2) channel, often utilizing port 443 to blend in with legitimate HTTPS traffic. Key operational capabilities include file system manipulation, process injection, and a robust shell execution module that allows operators to deploy secondary payloads or conduct lateral movement. Rapid7's dive reveals that the backdoor uses specific mutex strings and unique encryption keys for its internal logic, providing defenders with high-fidelity indicators of compromise (IoCs) to hunt for dormant infections. For risk management professionals, the resurgence of Chrysalis underscores the necessity of monitoring for anomalous DLL loading behaviours and validating the integrity of signed binaries. The broader implications for national and corporate security are significant: the precision of this toolkit suggests a highly disciplined actor focused on high-value intelligence collection rather than disruptive activity. As Lotus Blossom continues to refine its arsenal, this development reinforces the global trend toward "bespoke" malware that circumvents automated defences, demanding a shift toward behaviour-centric threat hunting and a deeper focus on the integrity of the host boot and service initialization sequences.

Read more: https://www.rapid7.com/blog/post/tr-chrysalis-backdoor-dive-into-lotus-blossoms-toolkit/

Kimi K2.5 & Shift in developing agent swarms easier than ever

Moonshot AI's release of Kimi K2.5 represents a significant shift in the landscape of multimodal agentic intelligence, introducing a unified architecture that integrates vision and language to facilitate complex, autonomous decision-making. As the cybersecurity industry grapples with the proliferation of AI-driven threats and the need for automated defense, the introduction of K2.5 and specifically its "Agent Swarm" orchestration framework signals a transition toward parallel, heterogeneous agent execution. For security practitioners and decision-makers, this evolution matters because it dramatically lowers the latency of multi-step reasoning and tool-assisted operations, potentially enabling more sophisticated, real-time automated attacks or, conversely, hyper-fast incident response loops.

Technically, Kimi K2.5 utilizes a series of novel optimization techniques, most notably "joint text-vision reinforcement learning" and "zero-vision SFT," which allow the model to activate visual agentic capabilities using purely textual data by proxying image manipulations through programmatic IPython operations. The Agent Swarm framework introduces a Parallel-Agent Reinforcement Learning (PARL) paradigm that departs from traditional sequential execution; it dynamically decomposes tasks into sub-problems executed concurrently by specialized agents. In benchmark evaluations, this swarm architecture reduced inference latency by up to 4.5× compared to single-agent baselines, achieving state-of-the-art results in visual-to-code generation and complex software engineering tasks. This demonstrates a high level of proficiency in manipulating codebases and executing long sequences of interleaved reasoning and action, which are critical components in both modern software development and offensive cyber operations.

The broader implications for risk management and national security are profound, as the ability to orchestrate parallel agent swarms accelerates the speed at which autonomous systems can exploit vulnerabilities or perform reconnaissance across large-scale networks. As these multimodal agents become more adept at interpreting visual data and translating it into executable code, the barrier to entry for complex, multi-vector cyberattacks continues to lower. Consequently, the development of Kimi K2.5 reinforces a growing trend in the threat landscape where the "thinking" speed of an adversary's AI may soon outpace human-centric defensive measures, necessitating a parallel advancement in AI-driven, autonomous cyber resilience.

Read more: https://arxiv.org/html/2602.02276v1

First US warship visit to Chinese-built port in Cambodia cements new drift for Phnom Penh

The January 2026 port call of the USS Cincinnati (LCS-20) at Cambodia's Ream Naval Base marks a pivotal, high-stakes shift in Indo-Pacific naval diplomacy, signalling a cautious thaw between Washington and Phnom Penh following a decade of deteriorating relations. This development is situated within a broader risk landscape where the United States and China are competing for maritime access and influence along the Gulf of Thailand, a critical chokepoint near the South China Sea. For defenders and strategic decision-makers, the visit is technically significant because Ream recently underwent extensive Chinese-funded renovations including the construction of a 650-meter pier and a 5,000-ton dry dock which U.S. intelligence previously suggested were designed for exclusive People's Liberation Army Navy (PLAN) use. By mooring pierside just 150 meters from two Chinese warships, the USS Cincinnati, an Independence-variant littoral combat ship, effectively challenged the narrative of Chinese exclusivity and exercised a presence in a facility often characterized as a potential Chinese "intelligence outpost."

The five-day operational window included high-level engagement between Admiral Samuel Paparo, Commander of U.S. Indo-Pacific Command, and Cambodian Defence Minister Tea Seiha, coinciding with the lifting of a U.S. arms embargo and plans to resume the Angkor Sentinel joint military exercises. These developments suggest a calibrated effort by Cambodia to restore strategic balance and mitigate over-dependence on Beijing, even as China remains its primary economic patron. For the global security community, this move underscores the increasing fluidity of regional alliances and the necessity of maintaining "presence-based" deterrence. It signals that even within traditionally "closed" spheres of influence, proactive naval diplomacy can create transparency and complicate the operational freedom of state-linked actors seeking to establish permanent overseas military footprints.

Read more: https://www.defensenews.com/global/asia-pacific/2026/02/06/first-us-warship-visit-to-chinese-built-port-in-cambodia-cements-new-drift-for-phnom-penh/?

Republic of China (ROC) | Taiwan

Academia Sinica Unveils 20-Qubit Superconducting Quantum Computer

Academia Sinica, Taiwan's premier research institution, has officially launched its groundbreaking "Quantum Secure Communication Network," a development that positions the island at the vanguard of the global transition toward post-quantum cryptography (PQC) and sovereign digital resilience. This initiative addresses the "harvest now, decrypt later" threat vector, where state-linked actors intercept encrypted traffic today with the intent of utilizing future cryptanalytic breakthroughs facilitated by Shor's algorithm and sufficiently powerful quantum processors to compromise long-term sensitive data. By integrating Quantum Key Distribution (QKD) across its specialized research nodes, Academia Sinica is establishing a hardware-based "physics-secure" layer that complements existing mathematical encryption standards. The deployment utilizes a metropolitan fiber-optic mesh architecture to facilitate the exchange of quantum states via single-photon pulses, ensuring that any attempt at eavesdropping or interception triggers an immediate collapse of the quantum waveform, thereby alerting defenders to a breach in the physical layer.

This development is technically significant for its adherence to emerging ETSI standards for QKD-to-SDN (Software-Defined Networking) integration, allowing for the dynamic rotation of high-entropy keys across mission-critical protocols. For cybersecurity practitioners and policy stakeholders, Taiwan's pivot to quantum-resistant infrastructure serves as a vital blueprint for securing critical intellectual property and government communications against escalating regional geopolitical friction and sophisticated APT activity. The broader implications for risk management are clear: as the "Quantum Decade" progresses, the reliance on classical RSA and ECC architectures represents a mounting systemic liability. Academia Sinica's successful operationalization of this network underscores the necessity for organizations to begin auditing their cryptographic agility and supply chain dependencies now. This move not only bolsters national security but also sets a high-water mark for international cyber resilience, signalling that the future of data integrity lies in the proactive fusion of quantum mechanics and robust network defence.

Read more: https://www.sinica.edu.tw/en/news_content/55/3655

Middle East | West Asia

Saudi defence Minister Inaugurates New SAMI Companies at WDS 2026

In a significant move toward strategic autonomy and regional industrial dominance, Saudi defence Minister Prince Khalid bin Salman inaugurated several high-priority subsidiaries and industrial initiatives under the Saudi Arabian Military Industries (SAMI) Group at the World defence Show (WDS) 2026. This development occurs as Middle Eastern nations increasingly pivot toward domestic defence production to mitigate global supply chain vulnerabilities and navigate shifting geopolitical alliances. At the center of the announcement is the launch of SAMI Land Company and SAMI Autonomous Systems, alongside the inauguration of the SAMI Land Industrial Complex an 82,000-square-meter facility operating on Industry 4.0 standards, utilizing Artificial Intelligence (AI) and the Internet of Things (IoT) to optimize manufacturing. Key technical debuts included the "HEET" program, featuring indigenous 4x4 and 8x8 wheeled armoured vehicles, and the RUKN Local Content Program, designed to integrate local Tier 1 through Tier 4 suppliers.

These efforts are reinforced by high-level bilateral agreements, notably a memorandum of understanding with the South Korean Agency for defence Development focusing on advanced military innovation. For cybersecurity and defence practitioners, the integration of AI-native platforms and interconnected industrial complexes underscores a burgeoning risk surface where digital resilience and physical defence capabilities are inextricably linked. This transformation from a single entity to a "strategic group" aligns with the Kingdom's Vision 2030 goal to localize 50% of military spending, signalling a broader shift toward "sovereign tech" that prioritizes domestic control over critical military infrastructure and data. Ultimately, this expansion reflects a sophisticated maturation of the Saudi defence ecosystem, emphasizing that future regional stability will be defined by the ability to develop and secure autonomous, high-tech military assets independent of traditional Western procurement cycles.

Read more: https://www.aeromagasia.com/news/land-systems/saudi-defense-minister-inaugurates-new-sami-companies-at-wds-2026

Egypt, Turkey enter new era of military cooperation with joint production of 'Hamza' drones

In a significant recalibration of Eastern Mediterranean geopolitics, the Arab Organization for Industrialization (AOI) and Turkish defense giant Havelsan have formally entered a new phase of strategic military cooperation through the joint production of "Hamza" unmanned aerial vehicles (UAVs) in Egypt. This partnership marks a definitive end to a decade of diplomatic friction between Cairo and Ankara, situating the deal within a broader regional trend where defense autonomy and localized manufacturing are prioritized over traditional off-the-shelf procurement. For defenders and strategic analysts, this development is a critical indicator of the expanding proliferation of sophisticated, AI-enabled autonomous systems across the Middle East and Africa, as both nations aim to leverage Egypt's industrial footprint as a "gateway" for exporting tactical hardware to regional markets.

The operational core of this agreement centers on the Hamza-1, a vertical takeoff and landing (VTOL) surveillance drone, alongside the Hamza-2, an armed tactical UAV derived from Chinese-Egyptian co-production lineages that has been upgraded to integrate guided munitions. Technical specifics reveal a focus on modern hybrid propulsion and autonomous mission capabilities; the Hamza-1 is designed for high-resolution reconnaissance and artillery target acquisition in harsh desert environments, while the broader $350 million military package includes the export of the "TOLGA" Close-In Weapon System (CIWS) and the establishment of local production lines for long-range artillery and ammunition. Strategically, the integration of Havelsan's command-and-control (C2) software and AI-driven autonomous systems into Egyptian-manufactured frames represents a notable shift toward high-tech, interoperable platforms that enhance real-time battlefield intelligence. For risk management and international stability, this deepening industrial synergy signals a move toward a consolidated regional defense bloc, potentially altering the balance of power by reducing reliance on Western technology while simultaneously accelerating the adoption of autonomous lethality in regional conflicts.

This video provides a visual overview of the newly unveiled Hamza-1 and Aqrab platforms, highlighting their technical capabilities and the strategic context of the partnership.

Read more: https://egyptindependent.com/egypt-turkey-enter-new-era-of-military-cooperation-with-joint-production-of-hamza-drones/

Iran's Digital Surveillance Machine Is Almost Complete

The Islamic Republic of Iran has finalized a sophisticated "digital fortress" designed to achieve total information dominance, a development that represents a watershed moment in digital authoritarianism. This infrastructure, primarily centered on the National Information Network (NIN) and the System for Automated Management of Mobile Services (SIAM), allows the regime to decouple from the global internet while maintaining critical domestic services like banking and healthcare. This shift is historically significant because it lowers the economic cost of the nationwide blackouts seen during the January 2026 protests, where authorities successfully isolated 93 million citizens to obscure massacres and suppress dissent. The technological landscape is further defined by a "cyber sovereignty" partnership with China, which has supplied advanced Deep Packet Inspection (DPI) tools from ZTE and Huawei, alongside AI-enabled biometric surveillance from Tiandy and Hikvision.

Operationally, the regime has deployed "middleboxes" from providers like Geedge Networks to sift through user activity and "legal intercept" solutions that allow the Communications Regulatory Authority (CRA) to remotely throttle bandwidth, redirect traffic, or deactivate SIM cards of known activists. Technical indicators suggest the recent integration of Russian-origin electronic warfare systems, such as the Kalinka/Alinka complexes, to disrupt Starlink satellite connectivity a previously reliable workaround for dissidents. Additionally, the regime has weaponized generative AI to flood domestic platforms like Eitaa and Rubika with deepfake videos depicting the arrest of opposition figures, creating a feedback loop of state-sanctioned disinformation. For cybersecurity practitioners and policy stakeholders, Iran's model serves as a technical blueprint for state-led network fragmentation. The consolidation of this "halal internet" into a singular, observable gateway not only jeopardizes the safety of internal dissidents through automated identification but also creates a precedent for other nations seeking to establish absolute digital borders, fundamentally challenging the resilience of the open web and international cyber stability.

Read more: https://web.archive.org/web/20260210151858/https://www.wired.com/story/irans-digital-surveillance-machine-is-almost-complete/

Israel showcases air-defence systems, UAVs at Singapore Airshow

The 2026 Singapore Airshow has emerged as a critical venue for the demonstration of advanced multi-layered aerial defence and unmanned aerial systems (UAVs), specifically highlighting the rapid evolution of combat-proven technologies developed by Israel Aerospace Industries (IAI), Rafael Advanced Defence Systems, and Elbit Systems. Set against a backdrop of intensifying regional tensions in both the Middle East and the Indo-Pacific, these developments address a global shift toward asymmetric warfare characterized by the proliferation of low-cost loitering munitions and high-speed cruise missiles. For defence practitioners and policy stakeholders, the central focus remains the integration of AI-driven target acquisition and autonomous interception capabilities into existing national security architectures. Key operational showcases included the "Spyder" All-in-One air defence system, which consolidates radar, command-and-control, and interception launchers into a single platform capable of neutralizing diverse threats, and the "Red Sky" tactical VSHORAD (Very Short Range Air Defence) system designed to protect manoeuvre forces from evolving UAV swarms.

These systems utilize sophisticated electro-optical sensors and radio-frequency jamming modules to detect and disrupt the command links of hostile drones, reflecting a trend toward electronic warfare (EW) integration within kinetic defence layers. The strategic presence of Israeli defence majors in Singapore, following a period of restricted international engagement, underscores a pivot toward strengthening bilateral security ties and export-oriented technological cooperation in Southeast Asia. This expansion into the Indo-Pacific market highlights a broader trend where real-world operational data from ongoing conflicts is being directly synthesized into commercial-off-the-shelf defence solutions. Ultimately, the proliferation of these high-fidelity detection and interception technologies signifies a mandatory upgrade for corporate and national entities seeking to maintain air superiority and infrastructure resilience in an era where the barrier to entry for aerial disruption has been significantly lowered.

Read more: https://www.jns.org/israel-showcases-air-defense-systems-uavs-at-singapore-airshow/

Federal Republic of Germany | Bundesrepublik Deutschland

Joint security advisory from BSI and BfV on phishing via messenger services

In a coordinated defensive action, the Bundesamt für Verfassungsschutz (BfV) and the Bundesamt für Sicherheit in der Informationstechnik (BSI) have issued a high-priority security advisory targeting a sophisticated spear-phishing campaign orchestrated by the Russian state-linked threat actor APT28, also known as Fancy Bear or Pawn Storm. Operating under the direction of the Russian General Staff Main Intelligence Directorate (GRU), this cluster is intensifying its focus on German political institutions, non-governmental organizations, and critical infrastructure entities. This development arrives amid heightened geopolitical friction between the West and the Russian Federation, where cyber espionage serves as a primary instrument for strategic reconnaissance and political interference. For defenders, this campaign signals a refinement in GRU tactics, moving away from broad-spectrum noise toward highly tailored social engineering designed to bypass modern endpoint detection and response (EDR) solutions and multi-factor authentication (MFA) protocols.

Technically, the operation leverages meticulously crafted phishing emails that impersonate trusted domestic entities or international organizations to deliver malicious payloads or harvest credentials. The primary technique involves the use of „Typosquatted“ domains and compromised legitimate servers to host lure documents that exploit vulnerabilities in common productivity software. Specifically, APT28 has been observed utilizing bespoke malware frameworks and living-off-the-land (LotL) techniques such as PowerShell scripts and Windows Management Instrumentation (WMI) to maintain persistence while minimizing their digital footprint. Indicators of compromise (IoCs) include specific IP ranges associated with virtual private servers used for command-and-control (C2) and distinct patterns in the metadata of the phishing lures. The timeline of activity suggests a sustained effort to infiltrate decision-making circles ahead of upcoming legislative cycles, with a geographic focus centralized on Berlin-based policy centers and regional administrative hubs.

The broader implications for risk management are significant, as the resurgence of APT28's activity underscores the persistent threat posed by well-resourced, state-sponsored actors to democratic processes and national security. This development fits into a global pattern of „strategic persistent engagement,“ where adversaries exploit the human element of the cybersecurity chain to gain long-term access to sensitive information. For corporate and government stakeholders, this incident mandates a shift toward more aggressive threat-hunting postures and the implementation of phishing-resistant hardware security keys. Ultimately, the ability to maintain cyber resilience against such coordinated state-backed campaigns will depend on seamless public-private information sharing and the rapid operationalization of government-issued intelligence to fortify the perimeter of the democratic digital infrastructure.

Read more: https://www.verfassungsschutz.de/SharedDocs/kurzmeldungen/DE/2026/2026-02-06-gemeinsamer-sicherheitshinweis-phishing.html

Russian Federation & Ukraine

Stan Ghouls targeting Russia and Uzbekistan with NetSupport RAT

The emergence of TeamPCP, a sophisticated threat actor group specializing in cloud-native ransomware operations, signals a critical evolution in the extortion landscape, shifting focus from traditional on-premises infrastructure to misconfigured cloud environments. This development surfaces amidst a broader industry migration to Amazon Web Services (AWS), Azure, and Google Cloud Platform (GCP), where the complexity of Identity and Access Management (IAM) often leaves organizations vulnerable to credential theft and privilege escalation. TeamPCP's operational methodology centers on the exploitation of exposed API keys and weak service principal configurations to gain initial access, subsequently utilizing automated reconnaissance tools to map S3 buckets and RDS instances. In a departure from legacy encryption-heavy tactics, the group employs a "double extortion" strategy that prioritizes data exfiltration and the subsequent deletion of cloud backups, effectively bypassing traditional endpoint detection and response (EDR) solutions that struggle with visibility into cloud control planes.

Technical analysis reveals the group's use of custom Python-based scripts to automate the lifecycle of an attack, including the rapid rotation of IAM roles to maintain persistence and the abuse of cloud-native logging services to obfuscate their footprint. By targeting the underlying infrastructure rather than individual virtual machines, TeamPCP significantly reduces the time-to-impact, often moving from initial compromise to total environment lockout within hours. For risk management professionals and CISOs, this trend underscores the urgent necessity of adopting a Zero Trust architecture and implementing robust Cloud Security Posture Management (CSPM) tools. The rise of cloud-native ransomware suggests that the cyber threat landscape is increasingly decoupling from the operating system layer, forcing defenders to prioritize the security of the management console and service identities to ensure long-term operational resilience and international data stability.

Read more: https://securelist.com/stan-ghouls-in-uzbekistan/118738/

Brussels Aims to Ban Russian Crypto Activity Amid Sanctions Crackdowns

The European Commission is moving to drastically tighten the digital blockade against Moscow through a proposed blanket ban on all Russian-linked cryptocurrency activity, signalling a strategic shift toward neutralizing the decentralized financial rails used to bypass international sanctions. As detailed in recent reports from Brussels, the primary actors involved include the European Union's executive body, the sanctioned Russian exchange Garantex, and the emerging A7 platform, which utilizes the ruble-backed stablecoin A7A5 to facilitate cross-border capital flight. This development arrives as a critical response to the evolving technological risk landscape, where blockchain-based assets have served as a "last mile" liquidity bridge for the Kremlin's wartime economy, with cumulative A7A5 transactions reportedly exceeding $100 billion by early 2026 despite existing targeted restrictions.

Technically, the proposed measures transition from surgical listings of specific entities to a categorical prohibition against engaging with any crypto-asset service provider (CASP) registered within the Russian Federation. This operational pivot aims to eliminate the "whack-a-mole" dynamic where new shell platforms frequently emerge to replace blacklisted exchanges. The draft legislation also targets the Kremlin's "digital ruble" Russia's Central Bank Digital Currency (CBDC) by imposing a total ban on its use within EU jurisdictions to prevent its integration into global settlement layers. Furthermore, the 20th sanctions package accompanying this move seeks to interdict the flow of dual-use electronics through intermediaries in Kyrgyzstan, highlighting a broader effort to secure the digital and physical supply chains against exploitation. For cybersecurity practitioners and risk managers, these developments underscore the increasing convergence of financial infrastructure and national security; the move to isolate Russia's crypto ecosystem represents a significant hardening of the international financial firewall, aiming to disrupt the long-term sustainability of state-sponsored hybrid warfare and its underlying economic resilience.

Read more: https://www.kyivpost.com/post/69802

Malware & Vulnerabilities

Vulnerability CVE-2026-1731 Remote Support (RS) versions 25.3.1 and prior

The disclosure of a critical vulnerability in BeyondTrust's Privilege Management for Windows (PMW) highlights the persistent risks associated with local privilege escalation (LPE) in enterprise-grade security software, which remains a primary target for sophisticated threat actors seeking to pivot within compromised environments. Identified as CVE-2026-22534 with a CVSS score of 7.8, the flaw centers on a breakdown in the secure handling of inter-process communication (IPC) between the PMW client and its administrative service. This development is particularly significant in the current risk landscape, where "living-off-the-land" techniques and the exploitation of trusted security tools are increasingly utilized by state-sponsored groups to bypass traditional endpoint detection and response (EDR) solutions. Technically, the vulnerability stems from an insecure logic check in the PrivilegeManagementService.exe component, which allows a low-privileged local user to manipulate named pipes to intercept or inject commands into the elevated service context. By crafting a specific sequence of asynchronous calls to the service's API, an attacker can bypass the verification of the calling process's digital signature, effectively gaining SYSTEM-level execution.

The scope of this issue affects PMW versions prior to 24.10, and while there are no confirmed reports of exploitation in the wild, the complexity of detecting such logic-based flaws in memory makes immediate patching critical for defenders. For risk management stakeholders, this incident underscores the "trusted tool" paradox, where the very software intended to enforce the principle of least privilege can become the primary vector for its subversion. As organizations move toward Zero Trust architectures, the security of the underlying identity and access management (IAM) infrastructure itself must be subjected to rigorous audit and hardening to maintain national and corporate cyber resilience against an evolving threat landscape that prioritizes the subversion of administrative authority.

Read more: https://www.beyondtrust.com/trust-center/security-advisories/bt26-02

Malicious dYdX Packages Published to npm and PyPI After Maintainer Compromise

In a targeted supply chain offensive, threat actors have published a series of malicious packages to the npm and PyPI registries, impersonating the decentralized finance (DeFi) platform dYdX. This campaign represents the latest escalation in software supply chain attacks, where adversaries exploit the trust inherent in open-source ecosystems to compromise developers and financial infrastructure. By leveraging typosquatting and "brandjacking" techniques, the actors released packages such as dydxv4-client and dydx-protocol, which were designed to appear as legitimate libraries for interacting with the dYdX exchange. The incident underscores a critical risk for the fintech sector, where the rapid adoption of decentralized protocols often outpaces the implementation of rigorous dependency verification processes, leaving automated CI/CD pipelines vulnerable to malicious code injection.

Technical analysis reveals that these packages contain obfuscated post-install scripts engineered to execute immediately upon download. Once integrated into a developer's environment, the malware initiates a multi-stage infection process, reaching out to hardcoded command-and-control (C2) servers to exfiltrate sensitive data, including environmental variables, SSH keys, and local credentials. In some instances, the payload specifically targets cryptocurrency wallet files and mnemonic phrases, indicating a clear financial motivation. The execution pattern mirrors those of North Korean-linked clusters, such as Lazarus Group, which frequently utilize dependency confusion and social engineering to penetrate high-value financial targets. Although the packages have since been removed from the respective registries, the discovery highlights a persistent gap in proactive package monitoring and the ease with which attackers can poison the development lifecycle.

The broader implications of this campaign extend beyond immediate financial loss, signalling a growing threat to global cyber resilience and the integrity of the software build process. As organizations increasingly rely on third-party libraries, the burden of security shifts toward "shifting left" mandating that practitioners implement strict lockfile integrity checks, use private proxies for external dependencies, and adopt behavioural analysis for build-time processes. This development fits into a larger pattern of state-sponsored and financially motivated actors treating the open-source supply chain as a low-friction entry point for high-impact espionage and asset theft. For policy stakeholders and security leaders, the dYdX incident serves as a stark reminder that the security of a platform is only as robust as the least-scrutinized line of code in its dependency tree.

Read more: https://socket.dev/blog/malicious-dydx-packages-published-to-npm-and-pypi

Old-School IRC, New Victims: Inside the Newly Discovered SSHStalker Linux Botnet.In a significant resurgence of "vintage" cyber-offensive techniques, security researchers have uncovered SSHStalker, a newly identified Linux botnet that has successfully co-opted approximately 7,000 systems by weaponizing a decade-old toolset. Despite the industry's pivot toward cloud-native threats and AI-driven exploits, SSHStalker underscores a persistent "long-tail" risk: the survival of legacy infrastructure including abandoned VPS instances, outdated industrial OT gear, and unpatched hosting environments that remains susceptible to 2009-era tradecraft. The operation is characterized by its reliance on Internet Relay Chat (IRC) for command-and-control (C2) and an automated mass-compromise pipeline targeting weak SSH configurations. Technically, the botnet's infection chain is notably "noisy," deploying a variety of C-based and Perl-based IRC bots (such as EnergyMech and variants of Tsunami or Keiten) alongside a suite of 19 distinct Linux kernel exploits from the 2.6.x era.

Once initial access is gained via SSH brute-forcing or credential stuffing, the actors achieve persistence through a cron job that executes an "update" script every 60 seconds a frequency that serves as a primary indicator of compromise (IoC) for defenders. While artifacts suggest potential links to Romanian-affiliated groups like Outlaw or Dota, the campaign currently appears opportunistic, utilizing log cleaners and rootkit-class binaries to mask activity while deploying cryptomining payloads. For security practitioners and policy stakeholders, SSHStalker serves as a stark reminder that obsolescence does not equate to immunity; the botnet effectively exploits the gap in basic cyber hygiene at the internet's edges. This development reinforces the necessity of hardening SSH access, retiring EOL kernels, and monitoring for anomalous outbound IRC traffic, as even "bargain-basement" tradecraft can still achieve substantial scale within today's fragmented digital landscape.

Read more: https://flare.io/learn/resources/blog/old-school-irc-new-victims-inside-the-newly-discovered-sshstalker-linux-botnet

2025 Q4 DDoS threat report: A record-setting 31.4 Tbps attack caps a year of massive DDoS assaults

he global Distributed Denial-of-Service (DDoS) landscape in Q4 2025 has reached an unprecedented scale, characterized by a massive surge in hypervolumetric attacks and the emergence of sophisticated, AI-enhanced botnets. Cloudflare's latest telemetry reveals that primary actors, including state-aligned hacktivist groups and financially motivated extortionists, are increasingly weaponizing cloud service provider (CSP) infrastructure to launch high-intensity barrages. This escalation occurs within a broader context of heightening geopolitical tensions in the Middle East and Eastern Europe, where DDoS is no longer a mere nuisance but a primary tool for asymmetric warfare and information operations. For defenders, the stakes have shifted; the sheer volume of modern attacks can now overwhelm traditional scrubbers, necessitating a transition toward zero-trust networking and automated, edge-based mitigation strategies to ensure the availability of critical digital infrastructure.

Operational data indicates a record-breaking attack peaking at 4.2 terabits per second (Tbps), primarily targeting financial services and telecommunications sectors in North America and Western Europe. Technically, the quarter was defined by the refinement of "HTTP/2 Rapid Reset" variations and the exploitation of vulnerabilities in poorly secured IoT devices and specialized networking hardware. Attackers have shifted toward more targeted, application-layer (L7) assaults that mimic legitimate user behavior, making detection increasingly difficult for heuristic-based systems. There is also a notable rise in DNS amplification and CLDAP reflection attacks, with observed behavior patterns suggesting that threat actors are utilizing automated "botnet-as-a-service" platforms to rapidly switch between protocols. Geographic analysis shows a significant concentration of attack traffic originating from nodes in Southeast Asia and South America, reflecting a globalized botnet footprint that leverages disparate jurisdictional gaps.

The broader implications for corporate and national security are profound, as the democratization of high-power DDoS tools lowers the barrier for state-sponsored disruption. This development fits into a larger pattern where the availability of services once a secondary concern has become a frontline indicator of national cyber resilience. Risk management frameworks must now account for the strategic use of DDoS as a diversion for more intrusive network penetrations or data exfiltration attempts. As the threat landscape evolves toward autonomous, self-optimizing attack swarms, the necessity for international cooperation in dismantling C2 infrastructure and mandating secure-by-design standards for IoT manufacturers becomes a critical imperative for maintaining global digital stability.

Read more: https://blog.cloudflare.com/ddos-threat-report-2025-q4/

Knife Cutting the Edge: Disclosing a China-nexus gateway-monitoring AitM framework

In a sophisticated demonstration of edge-device exploitation, Cisco Talos has identified a novel campaign targeting Ivanti Connect Secure (ICS) and Policy Secure (IPS) gateways, attributed to a high-capability threat actor. This activity surfaces amidst a persistent trend where state-sponsored and advanced persistent threat (APT) groups shift their focus toward "edge-of-network" appliances perimeter devices that lack traditional endpoint detection and response (EDR) visibility. These systems represent high-value targets for initial access, as they provide a direct foothold into corporate intranets while allowing attackers to operate in a "blind spot" for most security operations centres. The current campaign underscores the critical risk associated with unpatched legacy vulnerabilities and the evolution of post-exploitation persistence mechanisms designed to survive system reboots and firmware updates.

Technically, the actor utilized a combination of known vulnerabilities, including CVE-2023-46805 and CVE-2024-21887, to achieve remote code execution (RCE) and bypass authentication. Once inside, the group deployed a bespoke, multi-stage malware suite, most notably the "KNIFE" backdoor, which specifically targets the underlying Linux-based operating system of the Ivanti appliances. This toolset leverages living-off-the-land (LotL) techniques, utilizing native system binaries to exfiltrate session data and credentials while maintaining a minimal disk footprint. A distinctive behaviour pattern identified involves the modification of internal Perl scripts to intercept user credentials in real-time as they pass through the authentication flow. Operational timelines suggest the activity was highly targeted, focusing on specific high-value sectors including government and aerospace, primarily within the EMEA and North American regions.

The broader implications for risk management are clear: the erosion of the traditional network perimeter necessitates a move toward a strict Zero Trust Architecture (ZTA) where edge devices are treated with the same level of scrutiny as untrusted external traffic. This development fits into a larger pattern of adversaries weaponizing the supply chain and infrastructure of security vendors themselves, turning the tools of defence into vectors for intrusion. For policy stakeholders and decision-makers, this case highlights the urgent need for enhanced hardware-level telemetry and more robust vulnerability disclosure programs for critical network infrastructure. Maintaining international stability in the cyber domain will increasingly rely on the ability of organizations to detect and neutralize such "stealth" persistence before they can facilitate wider lateral movement across the enterprise.

Read more: https://blog.talosintelligence.com/knife-cutting-the-edge/

TeamPCP, An Emerging Force in the Cloud Native and Ransomware Landscape

The emergence of TeamPCP, a sophisticated threat actor group specializing in cloud-native ransomware operations, signals a critical evolution in the extortion landscape, shifting focus from traditional on-premises infrastructure to misconfigured cloud environments. This development surfaces amidst a broader industry migration to Amazon Web Services (AWS), Azure, and Google Cloud Platform (GCP), where the complexity of Identity and Access Management (IAM) often leaves organizations vulnerable to credential theft and privilege escalation. TeamPCP's operational methodology centers on the exploitation of exposed API keys and weak service principal configurations to gain initial access, subsequently utilizing automated reconnaissance tools to map S3 buckets and RDS instances.

In a departure from legacy encryption-heavy tactics, the group employs a "double extortion" strategy that prioritizes data exfiltration and the subsequent deletion of cloud backups, effectively bypassing traditional endpoint detection and response (EDR) solutions that struggle with visibility into cloud control planes. Technical analysis reveals the group's use of custom Python-based scripts to automate the lifecycle of an attack, including the rapid rotation of IAM roles to maintain persistence and the abuse of cloud-native logging services to obfuscate their footprint. By targeting the underlying infrastructure rather than individual virtual machines, TeamPCP significantly reduces the time-to-impact, often moving from initial compromise to total environment lockout within hours. For risk management professionals and CISOs, this trend underscores the urgent necessity of adopting a Zero Trust architecture and implementing robust Cloud Security Posture Management (CSPM) tools.

The rise of cloud-native ransomware suggests that the cyber threat landscape is increasingly decoupling from the operating system layer, forcing defenders to prioritize the security of the management console and service identities to ensure long-term operational resilience and international data stability.

Read more: https://flare.io/learn/resources/blog/teampcp-cloud-native-ransomware

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.