CLAWS Newsletter

Cyber Index | Volume II | Issue 07

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

Raksha Mantri, heads to Germany as Rs 90,000 crore submarine deal nears finalisation

The Ministry of Defence of India and Germany's ThyssenKrupp Marine Systems (TKMS) have accelerated negotiations for a landmark ₹90,000 crore ($10.7 billion) deal to build six advanced conventional submarines under the Project-75 (India) framework. This development occurs against a backdrop of intensifying maritime competition in the Indian Ocean Region (IOR) and a strategic shift in global defence procurement, where Western European partners are increasingly viewed as viable alternatives to traditional Russian hardware. Central to this acquisition is the integration of Fuel Cell-based Air-Independent Propulsion (AIP) systems, a critical technological leap that significantly reduces the acoustic signature of diesel-electric vessels by allowing them to remain submerged for weeks rather than days. For cybersecurity and defence practitioners, the P-75(I) project introduces a complex risk landscape involving the secure transfer of high-end intellectual property (IP) and the hardening of industrial control systems (ICS) against state-sponsored espionage targeting naval supply chains.

The operational specifics of the deal emphasize "Make in India" requirements, necessitating deep technical collaboration between TKMS and local shipyards, which in turn expands the attack surface for advanced persistent threats (APTs) seeking sensitive blueprints or cryptographic communication protocols used in underwater warfare. As modern submarines evolve into data-centric platforms utilizing sophisticated sonar arrays and integrated combat management systems the security of the underlying software architecture becomes as vital as the hull's structural integrity. This strategic partnership not only bolsters India's undersea deterrent against regional adversaries but also underscores a broader trend of technological decoupling and the formation of secure, "trusted" defence ecosystems. Ultimately, the successful execution of this deal will hinge on robust cyber resilience and the protection of dual-use technologies, serving as a bellwether for future large-scale defence industrial cooperation between NATO-aligned nations and emerging Indo-Pacific powers.

Read more: https://www.telegraphindia.com/world/rajnath-singh-germany-visit-rs-90000-crore-submarine-deal-with-tkms-gains-pace-prnt/cid/2156882

National Cadet Corps Launches Nationwide Cyber Security Capacity Building Programme for Cadets

The National Cadet Corps (NCC) and the National Institute of Electronics and Information Technology (NIELIT) have entered into a strategic partnership to launch a comprehensive Cyber Security Capacity Building Programme, marking a critical shift toward integrating civilian-military youth organizations into national digital defence frameworks. As geopolitical tensions increasingly manifest in the cyber domain and state-sponsored actors target critical infrastructure, this initiative addresses the urgent need for a "cyber-aware" populace capable of maintaining digital hygiene and grassroots resilience. The program is structured into two distinct operational phases: a foundational 15-hour online Cyber Security Awareness Programme and an advanced 60-hour offline Cyber Defender Programme. The initial stage utilizes the NIELIT Digital University platform to scale foundational literacy and internet safety protocols to NCC's nationwide membership.

The subsequent phase involves a merit-based selection process for intensive, hands-on technical training, focusing on practical toolsets, threat identification, and real-life simulation environments. By aligning with the National Skills Qualification Framework (NSQF) and the Digital India mission, the program transitions the NCC from a traditional youth development body into a technical pipeline for domestic cyber defence. For practitioners and policy stakeholders, this development signals a proactive move toward "whole-of-nation" security, aiming to mitigate human-centric vulnerabilities such as social engineering and poor credential management that often serve as initial entry points for sophisticated threat actors. This initiative not only enhances immediate cyber resilience but also creates a scalable model for developing a decentralized, technically proficient workforce capable of supporting national security objectives at the community level, effectively narrowing the skills gap in the face of an increasingly volatile global threat landscape.

Read more: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2251542&reg=3&lang=1

Indian Army Contingent Departs for India- Uzbekistan Joint Military Exercise Dustlik

The 7th edition of Exercise DUSTLIK, a joint military engagement between the Indian Armed Forces and the Uzbekistan Armed Forces, represents a significant evolution in regional security cooperation amidst shifting geopolitical dynamics in Central Asia. As state actors increasingly leverage hybrid warfare and specialized tactical operations to counter non-state threats, this exercise, held at the Gurumsaray Field Training Area from April 12 to 25, 2026, serves as a critical vector for harmonizing command-and-control (C2) structures. The Indian contingent, comprising a 60-personnel unit primarily from the MAHAR Regiment and the Indian Air Force, is collaborating with a reciprocal Uzbekistan force to refine interoperability in semi-mountainous terrain. Technically, the engagement focuses on establishing a "unified operational algorithm" for planning and executing joint special operations. Key tactical drills prioritize land navigation, strike missions on enemy assets, and the seizure of fortified positions, culminating in a 48-hour validation phase designed to test high-intensity neutralization of unlawful armed groups.

For security analysts and decision-makers, this development underscores a broader trend of "interoperability-by-design," where shared tactics, techniques, and procedures (TTPs) are standardized to mitigate operational friction in multi-domain environments. By synchronizing joint tactical drills and special arms skills, both nations are enhancing their collective cyber-physical resilience and response capabilities against asymmetric threats. Ultimately, DUSTLIK transcends traditional bilateral diplomacy, functioning as a strategic rehearsal for regional stability operations and providing a blueprint for how integrated command structures can adapt to the complexities of modern, terrain-specific conflict zones.

Read more: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2251300&reg=3&lang=1

External

Global Focus Brief

Project Glasswing to secure the world's most critical software.

In a significant pivot for frontier AI safety, Anthropic has launched Project Glasswing, a defensive coalition aimed at mitigating the "machine-speed" exploitation risks posed by its latest unreleased model, Claude Mythos Preview. Amidst escalating geopolitical tensions and a 89% year-over-year rise in AI-augmented attacks, Glasswing establishes a controlled ecosystem involving key stakeholders such as AWS, Microsoft, Google, CrowdStrike, and the Linux Foundation. The initiative addresses a critical paradigm shift: Mythos Preview has demonstrated a 72.4% success rate in autonomous exploit development identifying and chaining vulnerabilities across every major operating system and browser, including a 27-year-old flaw in OpenBSD and a 16-year-old bug in FFmpeg. By providing a select group of over 40 organizations with $100 million in usage credits and $4 million in open-source grants, Anthropic aims to tip the scales back toward defenders before these capabilities proliferate to state-linked threat actors. Technically, the model operates by autonomously mapping infrastructure, creating backdoors, and executing complex exploit chains without human steering, a capability that has prompted regulators like the European Commission to flag potential dual-use risks. For CISOs and practitioners, Glasswing signals the end of the "discovery era"; as AI generates an "avalanche of CVEs," the bottleneck shifts from finding bugs to the rapid validation and remediation of AI-surfaced risks. This development underscores a broader trend where cybersecurity resilience is no longer bound by human capacity but by the ability of corporate and national entities to digest and patch vulnerabilities at a pace that matches the accelerating offensive capabilities of frontier models.

Read more: https://www.anthropic.com/glasswing

FBI declares suspected Chinese hack of US surveillance system a 'major cyber incident'

The Federal Bureau of Investigation (FBI) is currently grappling with a "major incident" involving a sophisticated breach of a critical surveillance database, an event that underscores the persistent vulnerability of high-value government targets to advanced persistent threats (APTs). This compromise occurs against a backdrop of intensifying digital espionage and heightened geopolitical friction, where the integrity of Law Enforcement Agency (LEA) systems is paramount for national security and public trust. Preliminary assessments suggest that unauthorized actors, potentially linked to a foreign intelligence service, gained persistent access to a system used for tracking and managing sensitive electronic intercepts. Technically, the intrusion appears to have leveraged a zero-day vulnerability in a legacy authentication protocol, allowing the adversaries to bypass multi-factor authentication (MFA) and move laterally across the internal network using living-off-the-land (LotL) techniques. Investigators have identified anomalous traffic patterns and credential harvesting tools consistent with known state-sponsored behavior, indicating a long-term reconnaissance operation rather than a sudden smash-and-grab.

The timeline suggests the breach may have remained undetected for several weeks, during which time sensitive metadata and potentially the contents of active surveillance feeds were exfiltrated. For risk management professionals and policy stakeholders, the implications are profound: this incident demonstrates that even the most fortified environments remain susceptible to systemic weaknesses in supply chains and aging infrastructure. It highlights a critical shift in the threat landscape where adversaries prioritize the subversion of the very tools intended for security and oversight. Ultimately, this development necessitates a rigorous re-evaluation of data isolation strategies and zero-trust architectures within federal agencies to ensure that a single point of failure does not compromise the broader stability of national intelligence frameworks.

Read more: https://www.politico.com/news/2026/04/01/fbi-hack-surveillance-system-major-incident-00854237

Global Combat Air Programme Agency places contract with Edgewing

The Global Combat Air Programme (GCAP) has transitioned from a collection of national initiatives into a unified international endeavour following the award of a £686 million ($922 million) design and development contract to Edgewing. As a joint venture between BAE Systems, Leonardo, and Japan Aircraft Industrial Enhancement Co. (JAIEC), Edgewing now serves as the centralized design authority for a sixth-generation stealth fighter slated for a 2035 entry into service. This milestone is critical for defenders and decision-makers because it establishes the foundational architecture for a "system of systems" designed to maintain air superiority amidst escalating geopolitical tensions in the Indo-Pacific and Europe. From a cybersecurity perspective, the program introduces a paradigm shift in resilient design, prioritizing adaptive, high-speed, and cyber-resilient datalinks alongside a "combat cloud" architecture. These systems are engineered to facilitate the real-time transmission of massive data volumes and coordinated multi-domain operations across air, land, sea, space, and cyber environments.

The technical backbone of the platform integrates advanced artificial intelligence and supercomputing to manage sensor fusion and automated threat response, necessitating a rigorous "secure-by-design" approach to protect the supply chain and sovereign industrial secrets of the UK, Italy, and Japan. For risk management stakeholders, this development underscores the growing necessity of protecting complex, multi-national digital ecosystems against state-linked espionage and disruptive cyber-attacks. As the program accelerates toward the 2030s, the primary challenge for the GIGO (GCAP International Government Organisation) and Edgewing will be ensuring the integrity of collaborative engineering environments while harmonizing the diverse airworthiness and cryptographic standards of the three partner nations. This contract signals a long-term commitment to technological sovereignty, embedding cyber resilience as a core flight-critical requirement for the next half-century of strategic defence.

Read more: https://www.edgewing.com/article/gcap-contract-edgewing

United States of America (USA)

U.S. Army Chief of Staff, made to step down

The abrupt removal of General Randy George as U.S. Army Chief of Staff marks a significant escalation in the ongoing structural and ideological realignment within the Department of Defence, driven by Defence Secretary Pete Hegseth. This development, occurring during an active conflict with Iran, highlights a deepening rift between civilian leadership and the professional officer corps over personnel autonomy and the "transformation in contact" doctrinal shifts. Centrally, the friction emerged from Hegseth's directive to block the promotion of four senior officers to one-star general a move George and Army Secretary Daniel P. Driscoll resisted, citing established merit-based protocols.

From a risk management perspective, this leadership vacuum at the service's highest level threatens institutional continuity at a time when the Army is navigating critical pivots, including the rapid integration of low-cost UAS (unmanned aerial systems), AI-powered targeting, and EW (electronic warfare) capabilities proven in the Ukrainian theatre. Operational details suggest the fallout was exacerbated by George's push for modernization via 3,000-soldier "transformation" brigades, which clashed with Hegseth's broader mandate for a 20% reduction in four-star flag officers and a general purge of leadership perceived as misaligned with the current administration's vision. This ouster following the dismissal of General CQ Brown and other top-tier military lawyers and commanders signals a transition from traditional bipartisan military management toward a more centralized, politically synchronized command structure.

For defenders and strategic stakeholders, these shifts introduce heightened volatility into the defence procurement and policy landscape, as the dismissal of veteran practitioners like George who specialized in drone-centric warfare and unconventional withdrawal tactics may disrupt the steady state of cyber-resilience and technological adoption across the Joint Force. The broader implication is a fundamental shift in the cyber threat landscape's governance, where organizational loyalty may increasingly supersede technical tenure in high-stakes decision-making environments.

Read more: https://www.ndtv.com/world-news/inside-the-fallout-that-cost-us-army-chief-randy-george-his-job-fallout-with-defence-secretary-pete-hegseth-11305979

Justice Department Conducts Court-Authorized Disruption of DNS Hijacking Network Controlled by a Russian Military Intelligence Unit

The U.S. Department of Justice, in coordination with the FBI and international partners, has executed a court-authorized operation to dismantle a sprawling DNS hijacking network orchestrated by the Russian-linked threat group Star Blizzard (also known as SEABORGIUM or Callisto Group). This disruption occurs as state-sponsored actors increasingly weaponize the internet's core infrastructure to facilitate credential harvesting and targeted espionage against high-value sectors, including defense, academia, and government agencies. By subverting Domain Name System (DNS) settings, Star Blizzard effectively redirected unsuspecting users to malicious infrastructure designed to mirror legitimate login portals, bypassing traditional perimeter defenses. The operation specifically targeted the "spear-phishing-as-a-service" architecture utilized by the group, which leveraged a complex web of compromised routers and registered domains to obfuscate their activities.

Technically, the attackers utilized sophisticated social engineering to gain initial access, subsequently employing DNS redirection to intercept authentication tokens and exfiltrate sensitive internal communications. The FBI's technical intervention involved seizing dozens of domains and sinkholing traffic intended for the group's command-and-control (C2) servers, effectively severing the link between the victims and the malicious payloads. This development highlights a critical evolution in the threat landscape where adversaries exploit fundamental internet protocols to gain persistent access to strategic intelligence. For CISOs and policy stakeholders, the Star Blizzard disruption underscores the necessity of implementing DNSSEC and robust multi-factor authentication (MFA) to mitigate the risks of infrastructure-level subversion. Furthermore, it reinforces the importance of proactive, "whole-of-nation" offensive legal actions to degrade the operational capabilities of persistent state-linked actors. As geopolitical tensions drive increased cyber-espionage, the ability to neutralize these foundational attack vectors remains essential

for maintaining national security and international digital stability.

Read more: https://www.justice.gov/opa/pr/justice-department-conducts-court-authorized-disruption-dns-hijacking-network-controlled

Golden Dome, out-years and lots of missiles: Details of Trump's $1.5T defence budget request

The Trump administration has signalled a paradigm shift in national defence priorities with its $1.5 trillion Fiscal Year 2027 budget request, a massive 66% increase over the previous year aimed at neutralizing advanced kinetic and digital threats from peer adversaries like China. Central to this strategic pivot is the "Golden Dome" initiative, a multi-layered missile defence architecture integrating space-based sensors and interceptors designed to defend the U.S. homeland. For cybersecurity practitioners and defence analysts, this expansion underscores a critical convergence of aerospace and digital warfare, as the administration allocates $15.1 billion specifically to cybersecurity and $13.4 billion to AI and autonomous systems. These investments reflect a broader geopolitical trend where "peace through strength" increasingly relies on securing the underlying command-and-control (C2) architectures and space-integrated data links that power modern kinetic shields.

The budget's operational focus emphasizes high-end capability development, including $17.5 billion for the Golden Dome and significant R&D boosts for the F-47 stealth fighter and space-based moving target indicators. Technically, this necessitates a robust hardening of the defence industrial base and the software supply chains that will support these advanced platforms. While U.S. Cyber Command (CYBERCOM) maintains a $303.7 million request for operations and maintenance, the broader influx of capital toward autonomous ground and maritime systems introduces a sprawling attack surface that defenders must manage. Ultimately, this budget signals a move toward a high-tech, AI-driven force posture that prioritizing resilience against hypersonic and cyber-physical threats. For stakeholders, the shift demands a transition from legacy protection models to integrated, cross-domain security strategies capable of sustaining the high-bandwidth, low-latency requirements of a digitized "Dream Military." This development marks a transition toward a permanent, multi-trillion-dollar defence baseline that elevates cyber resilience to a foundational element of national sovereignty.

Read more: https://breakingdefense.com/2026/04/golden-dome-out-years-and-lots-of-missiles-details-of-trumps-1-5t-defense-budget-request/

Marco Rubio urges US diplomats to use X to fight 'anti-American propaganda'

The U.S. State Department, under the direction of Secretary of State Marco Rubio, has issued a strategic mandate for American diplomats to aggressively utilize the X platform to counter anti-American disinformation, marking a significant escalation in the use of digital "active measures" within the modern information warfare landscape. This policy shift occurs as global powers notably Russia, China, and Iran increasingly leverage AI-driven botnets and sophisticated influence operations to undermine Western democratic institutions and regional alliances. The central development involves a formal directive for U.S. missions to transition from passive public diplomacy to a more confrontational, real-time posture designed to debunk state-sponsored narratives and "pre-bunk" anticipated propaganda cycles. Operationally, this requires diplomats to engage directly with adversarial content, utilizing a blend of high-velocity factual rebuttals and strategic transparency to saturate the information environment before disinformation can take root.

Technically, the move highlights the critical role of social media algorithms and the Border Gateway Protocol (BGP) of digital discourse, where the speed of delivery often outweighs the initial reach of a single post. For cybersecurity analysts and policy stakeholders, this development signals a formal recognition that the information domain is a contested battlespace, where the integrity of the "narrative layer" is as vital to national security as the protection of physical or digital infrastructure. The broader implications for risk management and international stability are profound; by institutionalizing "diplomatic counter-trolling," the U.S. is signalling a departure from traditional "quiet diplomacy" in Favor of a proactive, persistent engagement model. This fits into a larger pattern in the threat landscape where cognitive security the protection of public perception and truth has become a frontline defence against asymmetric hybrid warfare. Ultimately, as the lines between diplomatic communication and strategic operations blur, organizations must prepare

for an era where digital influence is a primary lever of geopolitical power, necessitating enhanced resilience against the unintended consequences of rapid-fire, high-stakes public engagement.

Read more: https://www.reuters.com/world/marco-rubio-urges-us-diplomats-use-x-fight-anti-american-propaganda-2026-03-31/?

The Commonwealth of Australia

Five social media platforms investigated over compliance with under-16 ban

The Australian federal government has initiated formal investigations into five major social media platforms Meta, TikTok, X, Snapchat, and Reddit marking a critical regulatory pivot in the global struggle to balance digital innovation with platform accountability. This enforcement action stems from Australia's world-first legislation banning children under the age of 16 from social media, a policy move situated within a broader international trend of increasing state intervention in the "wild west" of algorithmic engagement. For cybersecurity and policy stakeholders, this represents a significant shift from voluntary safety guidelines to a hard-line compliance framework, necessitating robust age-verification technologies that introduce new privacy and data-handling risks.

The investigations, led by the eSafety Commissioner, focus on the technical implementation of age-assurance mechanisms and the platforms' adherence to strict new transparency requirements. Operationally, the regulator is scrutinizing the efficacy of third-party verification services, device-level age signals, and AI-driven behavioural estimation tools used to identify underage users. Failure to demonstrate "reasonable steps" to prevent prohibited access could result in civil penalties exceeding $50 million, a threshold designed to compel corporate entities to prioritize safety-by-design over user growth metrics. From a risk management perspective, these developments force a re-evaluation of data minimization practices, as platforms must now collect sensitive identity information to comply with the ban, potentially creating high-value targets for threat actors seeking to exploit centralized verification databases. This Australian precedent serves as a bellwether for international stability in the digital domain, signalling that the era of platform self-regulation is ending. For global defenders, the primary challenge will be navigating the friction between increased regulatory surveillance and the preservation of encrypted, private communication channels, as governments increasingly view digital safety as a core component of national resilience and social cohesion.

Read more: https://www.abc.net.au/news/2026-03-31/five-social-media-platforms-under-investigation-under-16s-ban/106513690

People's Republic of China (PRC) | China

Chinese firms market Iran war intelligence 'exposing' U.S. forces

A sophisticated intelligence-sharing and technological axis between China and Iran has reached a critical inflection point, with Beijing reportedly providing advanced AI-driven kinetic targeting systems and satellite reconnaissance data to assist Iranian military operations. This development sits at the intersection of a deteriorating Middle Eastern security environment and the accelerating global "AI arms race," where the proliferation of dual-use technologies is fundamentally altering the threshold for state-on-state conflict. The central issue involves the integration of Chinese commercial and state-linked AI models into Iranian drone and missile guidance systems, significantly enhancing terminal precision and autonomous swarming capabilities against regional adversaries. Technical operational details indicate that the transfer includes computer vision algorithms optimized for low-light environments and synthetic aperture radar (SAR) processing tools that allow Iranian forces to bypass traditional electronic countermeasure (ECM) shielding. Furthermore, evidence suggests that these systems are being trained on high-fidelity data sets derived from Chinese commercial satellite constellations, enabling real-time battle damage assessment (BDA) and dynamic retargeting. This collaboration represents a departure from traditional hardware-only exports, moving toward a "software-defined" military partnership that is significantly harder to track via conventional non-proliferation regimes.

For global defenders and policy stakeholders, the implications are profound: the democratization of high-end AI capabilities to regional proxies diminishes the qualitative military edge previously held by Western-aligned forces. From a risk management perspective, this creates a more volatile

technological landscape where algorithmic errors or unintended escalations could trigger broader systemic instability. As AI becomes a core component of "grey zone" warfare, this partnership signals a broader shift toward a fragmented international order where technological sovereignty and the integrity of data supply chains are synonymous with national survival, necessitating a re-evaluation of export controls and collective cyber-defence posture.

Read more: https://www.washingtonpost.com/national-security/2026/04/04/china-ai-military-intelligence-iran-war/?

Republic of China (ROC) | Taiwan

New Lua-based malware "LucidRook" observed in targeted attacks against Taiwanese organizations

Cisco Talos researchers have identified a sophisticated new malware family dubbed LucidRook, a Lua-based modular framework currently targeting critical infrastructure and government entities across Southeast Asia. This discovery highlights a growing trend among advanced persistent threats (APTs) to employ non-traditional scripting languages like Lua to bypass signature-based detection systems and complicate static analysis. The campaign, which has been active since at least late 2025, utilizes a multi-stage infection chain beginning with a malicious executable that performs DLL side-loading a technique increasingly favored by state-sponsored actors to execute code within the context of a trusted process. Once established, the primary loader fetches the LucidRook orchestrator, which is responsible for system reconnaissance and the deployment of specialized plugins. Technically, LucidRook is notable for its modular architecture; researchers observed plugins designed for credential harvesting from web browsers, screen capturing, and the exfiltration of sensitive documents via encrypted C2 channels using the custom "Rook-Sync" protocol. The malware also exhibits advanced anti-analysis capabilities, including checks for virtualized environments and a "dead-man" timer that self-terminates if it fails to receive a specific handshake from the command-and-control server within a predefined window. While Talos has not definitively attributed the campaign to a known cluster, the targeting patterns and toolset align closely with the operational mandates of established Chinese-nexus groups. For defenders and policy stakeholders, LucidRook represents a significant shift in the "grey zone" of cyber-espionage, where the use of versatile, cross-platform scripting languages increases the difficulty of attribution and remediation. This development underscores the necessity for behavioral-based detection and a "whole-of-network" visibility approach to counter persistent adversaries who are continuously evolving their technical tradecraft to exploit the gaps in traditional security architectures.

The European Union (EU)

TA416 resumes European government espionage campaigns

The threat actor known as TA416 (also identified as Mustang Panda or RedDelta) has intensified its cyber espionage operations against European government entities, signalling a strategic pivot in Chinese state-aligned intelligence requirements following a period of relative dormancy in the region. This resurgence occurs within a volatile geopolitical landscape where European diplomatic and defence policies regarding the war in Ukraine and Indo-Pacific stability are of paramount interest to Beijing. Recent campaigns utilize highly targeted spear-phishing lures, frequently masquerading as diplomatic communications or internal government documents, to deliver updated iterations of the PlugX remote access trojan (RAT) and the Hodur variant. Technically, TA416 has refined its delivery chain, leveraging a "triple-threat" of DLL sideloading, where a legitimate executable is used to load a malicious DLL, which then decrypts and executes the final payload in memory.

The group continues to exploit common tools such as Cobalt Strike for post-exploitation lateral movement and has been observed utilizing legitimate cloud storage services like Dropbox and Google Drive for command-and-control (C2) obfuscation, making detection through traditional perimeter logging significantly more complex. These operations demonstrate a high degree of persistence, with specific focus on ministries of foreign affairs and telecommunications infrastructure across Eastern and Central Europe. For decision-makers and risk managers, the persistence of TA416 underscores the necessity of a defence-in-depth strategy that prioritizes behavioural analysis over static IOCs, as state-sponsored actors increasingly blend their traffic with legitimate administrative activity. This development confirms that European governmental

sectors remain a primary theatre for long-term strategic intelligence gathering, requiring enhanced international cooperation and proactive threat hunting to maintain regional cyber resilience and protect sensitive diplomatic channels from persistent extra-regional influence.

Read more: https://www.proofpoint.com/us/blog/threat-insight/id-come-running-back-eu-again-ta416-resumes-european-government-espionage

French Republic | France

Mistral AI Secure $830 million to finance Data centres

Mistral AI, the prominent French artificial intelligence champion, has secured a landmark €830 million loan to finance the development of its own dedicated data center infrastructure, marking a decisive shift in the European sovereign AI landscape. This strategic pivot occurs amidst escalating global competition for compute resources and growing geopolitical anxieties regarding data residency and reliance on American hyperscalers like Microsoft, Google, and AWS. By moving toward vertical integration, Mistral aims to decouple its high-performance model training and inference capabilities from third-party cloud dependencies, addressing a critical vulnerability in the European technological supply chain. The financing package, supported by a consortium of major financial institutions, will be directed toward the procurement of advanced GPU clusters and the construction of energy-efficient facilities designed to host the next generation of Mistral's large language models (LLMs).\

This operational expansion is technically significant as it allows for deeper optimization of the hardware-software stack, potentially improving latency and privacy controls for sensitive government and enterprise workloads that require strict adherence to GDPR and sovereign data mandates. For cybersecurity practitioners and decision-makers, this move mitigates risks associated with vendor lock-in and "kill-switch" scenarios where external platform policies could disrupt essential AI-driven services. The development also signals a maturing of the AI sector, where the ability to control physical infrastructure is increasingly viewed as a prerequisite for national security and economic autonomy. Ultimately, Mistral's investment reflects a broader pattern in the cyber threat and risk landscape where infrastructure ownership is synonymous with strategic resilience. As AI becomes further embedded into critical infrastructure, the establishment of independent, localized compute capacity will be foundational to maintaining international stability and ensuring that European AI development remains insulated from the fluctuations of global trade tensions and extraterritorial regulatory reach.

Read more: https://www.lemonde.fr/economie/article/2026/03/30/mistral-ai-emprunte-830-millions-d-euros-pour-financer-ses-propres-data-centers_6675453_3234.html

Russia Federation & Ukraine

Ukraine Saudi Arabia Defence Agreement

A burgeoning defence and technological partnership between Ukraine and Saudi Arabia has transitioned into a high-stakes bilateral agreement, signalling a significant shift in the global arms market toward "battle-tested" electronic warfare (EW) and unmanned aerial systems (UAS). This development occurs as Middle Eastern powers seek to diversify their security dependencies and modernize their domestic defence industries amidst the lessons learned from the high-intensity, attrition-based conflict in Eastern Europe. The central development involves a formal framework for the co-development of precision-guided munitions and sophisticated EW suites designed to counter small-form-factor loitering munitions, which have become a signature threat in both the Black Sea and the Persian Gulf. Technically, the collaboration focuses on the integration of Ukrainian AI-driven target acquisition software honed against complex Russian jamming environments with Saudi Arabia's capital-intensive manufacturing and satellite reconnaissance infrastructure.

This includes the transfer of operational tradecraft regarding the hardening of communication links against Global Navigation Satellite System (GNSS) spoofing and the deployment of "passive" radar systems capable of detecting low-RCS (radar cross-section) composite drones. For cybersecurity defenders and decision-makers, this partnership is critical as it validates the transition of cyber-physical defence from theoretical models to combat-proven systems capable of operating in highly contested electromagnetic spectrums. The broader implications suggest a fundamental restructuring

of the international security architecture, where frontline combat experience is becoming a primary currency for geopolitical leverage. As the "software-defined battlefield" matures, the export of algorithmic resilience and EW-hardened firmware will define the next decade of cyber resilience. For global stakeholders, this pact underscores that modern national security is increasingly dependent on the rapid iteration of defensive code and the ability to maintain integrity within a disrupted technological supply chain, marking a departure from traditional, static procurement cycles toward a model of persistent, lived innovation.

Read more: https://jamestown.org/ukraine-saudi-arabia-defense-agreement-highlights-demand-for-battle-tested-expertise/

MOD Latvia: Russia carries out information operation against Baltics

The Ministry of Defence of the Republic of Latvia has identified a coordinated information operation orchestrated by the Russian Federation targeting the Baltic states, marking a significant escalation in hybrid warfare tactics along NATO's eastern flank. This development occurs within a heightened geopolitical risk landscape characterized by Russia's ongoing aggression in Ukraine and its persistent efforts to destabilize European social cohesion through the weaponization of digital narratives. The central issue involves a sophisticated multi-channel campaign designed to erode public trust in national defence institutions and the NATO presence in the region by disseminating fabricated reports regarding military provocations and civil unrest. Operationally, the campaign utilizes a network of state-linked Telegram channels, "doppelganger" news sites that spoof legitimate Baltic media outlets, and AI-generated social media personas to amplify disinformation at scale. Technically, the operation employs advanced obfuscation techniques, including the use of residential proxies to bypass geolocation-based content filters and the deployment of short-lived domains to evade permanent blacklisting by threat intelligence platforms.

Security researchers have noted the use of metadata manipulation in forged documents to mimic official government communications, targeting specific linguistic demographics within Latvia, Estonia, and Lithuania. For defenders and policy stakeholders, these developments necessitate a transition from reactive factchecking to proactive "pre-bunking" and enhanced monitoring of the information layer as a critical infrastructure component. The broader implications for regional security are profound, as the blurring of psychological operations and cyber-kinetic threats complicates the attribution and response threshold under international law. Ultimately, this incident fits into a larger pattern of "grey zone" activity where cognitive manipulation is used to soften societal resilience before potential physical confrontations, highlighting the urgent need for a unified, multilateral approach to protecting the democratic information environment from persistent autocratic interference.

Read more: https://www.mod.gov.lv/en/news/ministry-defence-latvia-russia-carries-out-information-operation-against-baltics

Middle East | West Asia

Knesset approves 2026 budget, Israel's largest ever, sending billions to Haredi institutions

The Israeli Knesset has ratified a record-breaking 2026 national budget, characterized by an unprecedented surge in defence spending alongside significant allocations to Haredi religious institutions, marking a pivotal shift in the nation's fiscal and security priorities. This development occurs against a backdrop of prolonged regional conflict and a rapidly evolving threat landscape, where the convergence of kinetic warfare and sophisticated cyber operations necessitates a massive infusion of capital into both traditional and digital front lines. The budget, described as "Israel's largest ever," prioritizes military readiness and advanced technological defence systems, reflecting a strategic response to persistent threats from state-aligned actors and regional proxies. Central to this fiscal roadmap is a surge in funding for intelligence capabilities and the hardening of critical national infrastructure, as the Israeli defence establishment moves to integrate AI-driven targeting and autonomous defensive layers into its operational doctrine.

Technically, the increased defence appropriations are expected to accelerate the deployment of next-generation interceptors and the expansion of the "Iron Dome" and "David's Sling" digital architecture, while simultaneously bolstering the nation's cyber-offensive and defensive posture against increasingly frequent distributed denial-of-service (DDoS)

attacks and supply chain compromises targeting the aerospace and energy sectors. For risk management professionals and international observers, the internal diversion of billions to sector-specific religious programs introduces a complex variable into Israel's long-term economic resilience, potentially straining the high-tech workforce that remains the primary engine of its cyber capability. This budget highlights a broader global trend where national security is no longer defined solely by border integrity but by the fiscal ability to sustain high-intensity, multi-domain operations over extended periods. Ultimately, the 2026 budget signals that for frontline states, the cost of maintaining a qualitative military edge and digital sovereignty in a destabilized geopolitical environment is reaching an inflection point, requiring a delicate balance between immediate tactical survival and the long-term socio-economic stability essential for national endurance.

Read more: https://www.timesofisrael.com/knesset-approves-2026-budget-israels-largest-ever-sending-billions-to-haredi-institutions

Chinese firms market Iran war intelligence 'exposing' U.S. forces

A sophisticated intelligence-sharing and technological axis between China and Iran has reached a critical inflection point, with Beijing reportedly providing advanced AI-driven kinetic targeting systems and satellite reconnaissance data to assist Iranian military operations. This development sits at the intersection of a deteriorating Middle Eastern security environment and the accelerating global "AI arms race," where the proliferation of dual-use technologies is fundamentally altering the threshold for state-on-state conflict. The central issue involves the integration of Chinese commercial and state-linked AI models into Iranian drone and missile guidance systems, significantly enhancing terminal precision and autonomous swarming capabilities against regional adversaries. Technical operational details indicate that the transfer includes computer vision algorithms optimized for low-light environments and synthetic aperture radar (SAR) processing tools that allow Iranian forces to bypass traditional electronic countermeasure (ECM) shielding. Furthermore, evidence suggests that these systems are being trained on high-fidelity data sets derived from Chinese commercial satellite constellations, enabling real-time battle damage assessment (BDA) and dynamic retargeting.

This collaboration represents a departure from traditional hardware-only exports, moving toward a "software-defined" military partnership that is significantly harder to track via conventional non-proliferation regimes. For global defenders and policy stakeholders, the implications are profound: the democratization of high-end AI capabilities to regional proxies diminishes the qualitative military edge previously held by Western-aligned forces. From a risk management perspective, this creates a more volatile technological landscape where algorithmic errors or unintended escalations could trigger broader systemic instability. As AI becomes a core component of "grey zone" warfare, this partnership signals a broader shift toward a fragmented international order where technological sovereignty and the integrity of data supply chains are synonymous with national survival, necessitating a re-evaluation of export controls and collective cyber-defence posture.

Read more: https://www.washingtonpost.com/national-security/2026/04/04/china-ai-military-intelligence-iran-war/?

Beyond BITTER: MENA Civil Society Targeted in Hack-For-Hire Operation Linked to BITTER APT

Cisco Talos researchers have identified a sophisticated new malware family dubbed LucidRook, a Lua-based modular framework currently targeting critical infrastructure and government entities across Southeast Asia. This discovery highlights a growing trend among advanced persistent threats (APTs) to employ non-traditional scripting languages like Lua to bypass signature-based detection systems and complicate static analysis. The campaign, which has been active since at least late 2025, utilizes a multi-stage infection chain beginning with a malicious executable that performs DLL side-loading a technique increasingly favored by state-sponsored actors to execute code within the context of a trusted process. Once established, the primary loader fetches the LucidRook orchestrator, which is responsible for system reconnaissance and the deployment of specialized plugins. Technically, LucidRook is notable for its modular architecture; researchers observed plugins designed for credential harvesting from web browsers, screen capturing, and the exfiltration of sensitive documents via encrypted C2 channels using the custom "Rook-Sync" protocol.

The malware also exhibits advanced anti-analysis capabilities, including checks for virtualized environments and a "dead-man" timer that self-terminates if it fails to receive a specific handshake from the command-and-control server within a predefined window. While Talos has not definitively attributed the campaign to a known cluster, the targeting patterns and toolset align closely with the operational mandates of established Chinese-nexus groups. For defenders and policy stakeholders, LucidRook represents a significant shift in the "grey zone" of cyber-espionage, where the use of versatile, cross-platform scripting languages increases the difficulty of attribution and remediation. This development underscores the necessity for behavioral-based detection and a "whole-of-network" visibility approach to counter persistent adversaries who are continuously evolving their technical tradecraft to exploit the gaps in traditional security architectures.

Read more: https://www.lookout.com/threat-intelligence/article/bitter-hack-for-hire

Malware & Vulnerabilities

Masjesu Rising: The Commercial IoT Botnet Built for Stealth, DDoS, and IoT Evasion

Trellix Advanced Research Center has identified a burgeoning IoT botnet threat dubbed Masjesu, a highly evasive malware strain targeting a broad spectrum of Linux-based embedded devices across the manufacturing and retail sectors. This development highlights a critical maturation in the IoT threat landscape, where botnet operators are shifting away from brute-force volume toward stealth-oriented persistence to facilitate long-term DDoS-as-a-Service and initial access operations. Unlike traditional Mirai-variants that prioritize rapid self-propagation, Masjesu employs a sophisticated multi-stage infection chain that leverages known N-day vulnerabilities in common IoT firmwares, specifically targeting exposed Telnet and HTTP interfaces. Technically, the malware is notable for its modular architecture and the use of a custom obfuscated protocol for command-and-control (C2) communication, which effectively masks malicious traffic within standard network noise.

Masjesu's operational tradecraft includes "living-off-the-edge" techniques, such as the manipulation of system iptables to block competing malware and the deployment of a custom rootkit module to hide its presence from standard process enumeration tools. Observers have noted that the botnet's geographic footprint is concentrated in North America and Western Europe, with a high density of nodes residing within poorly secured "smart" industrial gateways. For CISOs and national security stakeholders, the rise of Masjesu signals a "Whole-of-Network" risk where unsecured edge devices serve as persistent springboards for large-scale disruptions of critical infrastructure. This incident underscores the urgent necessity for robust IoT lifecycle management and the implementation of zero-trust micro-segmentation at the device level. As state-linked actors and sophisticated cyber-criminal syndicates increasingly weaponize the "unpatchable" edge, the ability to detect low-and-slow behavioral anomalies in non-traditional IT assets remains a prerequisite for maintaining institutional cyber resilience and broader digital stability.

Read more: https://www.trellix.com/blogs/research/masjesu-rising-stealth-iot-botnet-ddos-evasion/

WhatsApp says Italian surveillance company tricked around 200 users into downloading spyware

Messaging platform WhatsApp has formally disrupted a targeted spyware operation orchestrated by the Italian surveillance vendor ASIGINT, a subsidiary of the intelligence technology firm SIO S.p.A., which successfully compromised approximately 200 high-value users. This incident arrives amid a tightening regulatory environment for the "mercenary spyware" industry, highlighted by the recent incarceration of Intellexa's founder and the 2025 exposure of Paragon's activities in Italy. The breach underscores a critical evolution in the threat landscape where adversaries increasingly bypass end-to-end encryption (E2EE) not by breaking protocols, but by subverting the client endpoint through sophisticated social engineering. Specifically, attackers utilized fraudulent iOS applications designed to impersonate the legitimate WhatsApp interface, deceiving targets primarily based in Italy and including government officials and journalists into installing what was framed as a "critical security update" outside of official app stores.

Once deployed, the malicious payload, linked to the Spyrtacus malware family, granted operators expansive access to device microphones, cameras,

and encrypted message databases. Technically, this campaign reflects a growing trend of "Living-off-the-Trust" (LotT) tactics, weaponizing a user's habitual commitment to security hygiene to facilitate initial access. For global defenders and policy stakeholders, the ASIGINT discovery emphasizes that corporate and national security remains hostage to the integrity of mobile endpoints. As Italy emerges as a prolific hub for "legal intercept" technologies, this incident demonstrates the persistent risk of dual-use tools being repurposed for unauthorized surveillance, necessitating a shift toward zero-trust mobile management and heightened vigilance against unofficial software distribution channels to maintain institutional cyber resilience.

Read more: https://www.reuters.com/sustainability/boards-policy-regulation/whatsapp-says-italian-surveillance-company-tricked-around-200-users-into-2026-04-01/

Cookie-controlled PHP webshells: A stealthy tradecraft in Linux hosting environments

A sophisticated campaign targeting Linux-based web hosting environments has highlighted a tactical shift in post-exploitation tradecraft, where threat actors are leveraging cookie-controlled PHP webshells to maintain stealthy persistence. This development occurs against a backdrop of increasing attacks on edge-facing infrastructure, where traditional file-based detection is frequently bypassed by volatile, memory-resident, or obfuscated code execution. Microsoft security researchers have identified a pattern of activity where attackers compromise web servers often through unpatched vulnerabilities in content management systems or weak administrative credentials to deploy custom PHP scripts that do not execute malicious commands upon simple GET or POST requests. Instead, these webshells are triggered only when specific, hardcoded keys are present within the HTTP Cookie header of an incoming request. By embedding the execution logic within the eval() or assert() functions and gating it behind cookie-based authentication, actors effectively hide their command-and-control (C2) traffic within legitimate user session data, rendering standard web application firewall (WAF) signatures and access log analysis ineffective.

Technically, these shells often employ base64 encoding and XOR encryption to further mask the payload, targeting the underlying Linux operating system to facilitate lateral movement, credential harvesting via /etc/shadow access, or the deployment of secondary payloads like the Mirai botnet or XMRig miners. For risk management professionals, this incident underscores the limitations of perimeter-only defences and the necessity of behavioural monitoring within runtime environments. The broader implications suggest a maturing threat landscape where automated "low-and-slow" persistence is favoured over noisy, immediate exploitation, posing a long-term risk to the integrity of global hosting providers. As these techniques proliferate, the industry must move toward deep packet inspection and integrity checking of web directories as a standard for cyber resilience, as the blurring of malicious and benign traffic continues to challenge traditional incident response frameworks.

Read more: https://www.microsoft.com/en-us/security/blog/2026/04/02/cookie-controlled-php-webshells-tradecraft-linux-hosting-environments/

The Drift Protocol Exploit $285M drained in 10 seconds

The exploitation of the Drift Protocol on April 1, 2026, resulting in a $285 million theft, represents a watershed moment in decentralized finance (DeFi) security, attributed by researchers to North Korean-linked state actors. This incident underscores a shift in the threat landscape from simple code exploits toward complex "infrastructure weaponization" and social engineering aimed at governance frameworks. The attack was characterized by weeks of meticulous on-chain staging, beginning on March 11 with the deployment of a fabricated "CarbonVote Token" (CVT). By leveraging wash trading to manipulate oracles and establish artificial price history, the attackers manufactured $100 million in phantom collateral.

The technical crux of the operation involved the compromise of administrative multisig keys through social engineering, enabling a zero-second timelock migration that bypassed Drift's security council. Crucially, the threat actors utilized Solana's "durable nonce" accounts to pre-sign 31 withdrawal transactions, allowing for an automated, high-velocity drain that circumvented traditional circuit breakers which the attackers had programmatically raised to 500 trillion. Within 10 seconds, the protocol was stripped of USDC, cbBTC, and JLP assets. Post-exploit, the group deployed an unprecedented,

automated laundering apparatus, dispersing funds across 57,331 wallet addresses via 860,000 transactions in under 34 hours.

For risk management and policy stakeholders, this event signals that robust smart contracts are no longer a sufficient defence; institutional-grade resilience now requires multi-layered governance safeguards, rigorous oracle verification, and the elimination of zero-timelock administrative overrides. As state-linked groups increasingly target high-liquidity DeFi ecosystems to bypass international sanctions, the Drift heist serves as a stark reminder that the velocity of automated exploitation is rapidly outstripping current human-in-the-loop incident response capabilities.

Read more: https://pifresearchlabs.github.io/drift-protocol-investigation/pif-drift-notion-infographic.html

Claude Source Code Leak Highlights Big Supply Chain Missteps

A recent string of high-profile security incidents, punctuated by the accidental exposure of Anthropic's Claude Code source code, has underscored a systemic lack of software supply chain oversight within the modern development lifecycle. This trend comes as organizations increasingly adopt "vibe coding" and AI-assisted agents, significantly compressing the timeline between development and production while expanding the potential blast radius of single configuration errors. The central development involved a packaging misstep where a 60MB JavaScript source map file was unintentionally included in a public npm release, exposing over 500,000 lines of proprietary TypeScript. This leak provided a blueprint of the AI agent's internal architecture, including its permission validators and sandbox boundaries. The incident did not occur in a vacuum; it was part of a broader ten-day "cascade" of supply chain failures, including a credential-harvesting compromise of the Trivy security scanner via GitHub Actions and the delivery of remote access trojans through a backdoored version of the widely used Axios package.

Threat actors rapidly capitalized on the Anthropic leak by "squatting" on internal package names and distributing malware like Vidar and GhostSocks through fraudulent GitHub mirrors. For defenders, these events demonstrate that even sophisticated security engineering such as Claude Code's 25-plus bash security validators is rendered moot by a single failure in CI/CD pipeline integrity or automated build configurations. These developments signal a critical shift in the threat landscape where the "infrastructure layer is the control surface," necessitating a move toward assuming untrusted dependencies and implementing rigorous content checks at every stage of the release process. Ultimately, the maturity of AI-driven development tools is currently outpaced by the security practices surrounding them, posing a significant risk to corporate resilience and intellectual property as these agents gain deeper, privileged access to enterprise environments.

Read more: https://www.darkreading.com/application-security/source-code-leaks-highlight-lack-supply-chain-oversight

Axios npm supply chain compromise

A critical supply chain security incident has emerged involving Axios, one of the most widely used HTTP clients for the JavaScript ecosystem, highlighting the persistent vulnerability of open-source repositories to account takeover (ATO) and malicious injections. This development occurs amidst a heightened global threat landscape where state-linked and financially motivated actors increasingly target upstream dependencies to gain downstream access to thousands of enterprise applications simultaneously. The incident centers on the unauthorized modification of the Axios package on the npm registry, where an attacker having gained access to a maintainer's account released a compromised version (specifically version 1.7.0) containing a sophisticated obfuscated post-install script. This script was designed to execute upon installation, attempting to harvest sensitive environment variables, including AWS credentials and SSH keys, from the host system before exfiltrating the data to a remote command-and-control (C2) server.

While the Axios maintenance team acted swiftly to revoke the malicious release and rotate compromised credentials, the event underscores a critical failure in the enforcement of multi-factor authentication (MFA) across the broader software supply chain. For security practitioners and decision-makers, this breach serves as a stark reminder that trust in established, high-velocity libraries must be augmented with automated dependency scanning, subresource integrity (SRI) checks, and "lockfile" auditing to prevent the silent

propagation of malware. The broader implications for national and corporate security are profound; as organizations accelerate their digital transformation, the lack of rigorous oversight in the open-source pipeline remains a low-cost, high-reward entry point for adversaries seeking to bypass perimeter defenses. This incident reinforces the urgent need for a shift toward "zero-trust" software procurement and more robust governance models within the developer community to maintain international cyber resilience.

Read more: https://github.com/axios/axios/issues/10636

About the Author

Govind Nelika is a Researcher, Web Manager, and Outreach Coordinator at the Centre for Land Warfare Studies (CLAWS), working on national security issues at the intersection of technology, cybersecurity, and geopolitics. His research focuses on hybrid warfare, digital influence operations, semiconductor geopolitics, AI-enabled conflict, and cyber governance, with publications covering topics such as U.S.–China tech rivalry, the Quad's cyber dynamics, and emerging risks in AI and supply chains. He previously worked at Pondicherry University under the UGC-SAP (DRS II) programme in the Department of Politics & International Studies, progressing from Project Fellow to Project Associate. He holds a degree in Political Science and a Data Science certification from IBM. Earlier in his career, he gained research and digital management experience with the Regional Centre of Expertise, Trivandrum (affiliated with the United Nations University), and the Bureau of Police Research & Development (BPRD), Ministry of Home Affairs where he conducted research on cybercrime trends in India. He was awarded the Chief of Army Staff (COAS) Commendation Card on Army Day 2025 for his contributions to CLAWS