CLAWS Newsletter

Cyber Index | Volume II | Issue 06

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

DAC clears proposals worth Rs 2.38 lakh crore to augment defence capabilities

The Indian Ministry of Defence's (MoD) March 2026 authorization of ₹2.38 lakh crore (approximately $28 billion USD) in capital acquisitions signals a critical inflection point in New Delhi's effort to address deteriorating regional stability and persistent grey-zone pressures along its contested borders. This Acceptance of Necessity (AoN) focuses on high-end technological modernization across the Indian Army, Air Force, and Coast Guard, reflecting an urgent requirement to counter sophisticated peer-adversary capabilities in the Indo-Pacific. Key developments include the procurement of runway-independent aerial surveillance systems and remotely piloted strike aircraft, which introduce enhanced persistent ISR and offensive counter-air capabilities consistent with modern multi-domain operations. The inclusion of the S-400 long-range surface-to-air missile system and the Dhanush artillery system underscores a prioritized focus on integrated air defence and long-range precision fires, specifically designed to mitigate threats from state-sponsored tactical ballistic missiles and advanced aerial vectors.

Furthermore, the Indian Coast Guard's acquisition of heavy-duty air cushion vehicles indicates an operational shift toward high-speed reconnaissance and search-and-rescue in littoral environments, likely in response to increased non-traditional maritime threats and expanded naval activity by rival regional powers. For Five Eyes and NATO allies, this massive fiscal commitment the highest recorded in a single financial year demonstrates India's intent to achieve indigenous defence self-reliance while maintaining a credible conventional deterrent. These developments enhance collective security by potentially stabilizing the Indian Ocean Region, though the integration of diverse military systems including those of Russian origin alongside domestic platforms requires continued analytic caution regarding interoperability and supply chain vulnerabilities. Ultimately, this procurement surge aligns with broader global trends in hybrid warfare, as regional actors increasingly leverage advanced technology to secure territory and influence within the grey zone, necessitating heightened allied situational awareness.

Read more: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2246125&reg=3&lang=1

BEL and RRP Group sign strategic MoU to advance collaboration in Semiconductor, Unmanned Systems and Electro-Optics

The March 2026 strategic Memorandum of Understanding (MoU) between Bharat Electronics Limited (BEL), a premier Indian state-owned defence enterprise, and the RRP Group comprising RRP Electronics and RRP Defence represents a significant consolidation of India's domestic semiconductor and autonomous systems industrial base. This partnership targets the integrated development of high-precision electro-optical (EO) surveillance systems, weapon sights, and next-generation unmanned aerial vehicles (UAVs), underpinned by RRP Group's Outsourced Semiconductor Assembly and Test (OSAT) capabilities. Established within the context of intensified geopolitical competition in the Indo-Pacific and persistent allied concerns regarding supply chain resilience, this collaboration directly addresses the strategic objective of reducing dependency on foreign-sourced microelectronics. The initiative focuses on dual-use technologies where semiconductor sovereignty is critical for maintaining operational security and hardware integrity in mission-critical systems.

By fusing BEL's extensive systems-integration expertise with RRP's specialized manufacturing in thermal imaging and autonomous aerial platforms, the alliance seeks to accelerate the deployment of stealth ISR (Intelligence, Surveillance, and Reconnaissance) assets capable of operating in contested environments. For NATO and Five Eyes intelligence communities, this development signifies India's pivot toward a self-reliant "closed-loop" defence ecosystem, which may enhance regional stability by providing a more robust local deterrent against peer-adversary grey-zone activities. However, the rapid indigenization of these sophisticated technologies also presents challenges for allied interoperability and necessitates close monitoring of potential technology leakage or secondary proliferation. As hybrid warfare increasingly revolves around technical superiority in the "uncrewed" and "micro-electronic" domains, this MOU positions India as a more autonomous

security provider, potentially altering escalation dynamics by fielding indigenous, resilient surveillance and strike architectures that are less susceptible to external supply disruptions or electronic interdiction.

Read more: https://bel-india.in/news-bel/bel-and-rrp-group-sign-strategic-mou-to-advance-collaboration-in-semiconductor-unmanned-systems-and-electro-optics/

Defence ministry inks Rs 445cr deal for Tunguska missile systems with Russia, signs Rs 413cr P8I jet maintenance contract with Boeing

The Indian Ministry of Defence's (MoD) concurrent execution of high-value contracts with the Russian Federation and the Boeing Company (USA) underscores a complex strategic balancing act designed to maintain operational readiness amidst heightening Indo-Pacific competition. The core development involves two distinct but functionally linked capability sustainment efforts: a ₹445 crore ($53M) agreement with Russian state entities for the technical upgrade and life extension of the Tunguska-M1 gun-missile air defense systems, and a ₹413 crore ($49M) contract with Boeing for the long-term maintenance of the Indian Navy's P-8I Poseidon maritime patrol aircraft fleet. Historically, India has relied on Russian-origin integrated air defense systems (IADS) to secure forward-deployed strike corps against low-level aerial threats; however, the Tunguska deal likely involving the replacement of aging fire control radars and optical tracking systems occurs against a backdrop of global supply chain disruptions and international sanctions targeting the Russian defense industrial base. Simultaneously, the P-8I maintenance contract ensures the availability of critical wide-area maritime domain awareness (MDA) assets, which are essential for tracking adversary submarine activity and surface combatants in the Indian Ocean Region (IOR).

This bifurcated procurement strategy reflects a persistent pattern of behaviour where New Delhi mitigates dependency on any single state actor while upgrading legacy Soviet-era hardware to counter peer-adversary grey-zone incursions. For NATO and Five Eyes partners, these developments present a nuanced challenge to collective security and interoperability; while the P-8I sustainment aligns with Allied MDA architectures, the continued modernization of Russian-origin kinetic systems introduces persistent technical and political friction regarding technology transfer and sensitive data sovereignty. Ultimately, India's "multi-aligned" approach to defence logistics strengthens regional resilience against conventional escalation but complicates the realization of a fully integrated, Western-aligned security architecture in the Southern Theatre, fitting a broader global trend of strategic autonomy within intensifying systemic competition.

Read more: https://timesofindia.indiatimes.com/india/defence-ministry-inks-rs-445cr-deal-for-tunguska-missile-systems-with-russia-signs-rs-413cr-p8i-jet-maintenance-contract-with-boeing/articleshow/129856891.cms

External

Global Focus Brief

(OSTP) releases the "National Policy Framework for Artificial Intelligence"

The White House Office of Science and Technology Policy (OSTP) have released a "National Policy Framework for Artificial Intelligence," marking a pivotal shift in the U.S. government's approach to the rapid proliferation of generative AI and its systemic risks. Published on March 20, 2026, these legislative recommendations arrive amidst escalating geopolitical competition and the growing threat of AI-enabled cyber operations by sophisticated state-linked actors. The framework establishes a comprehensive regulatory architecture designed to move beyond voluntary commitments toward enforceable standards for safety, security, and transparency in frontier AI models. Central to the development are mandates for rigorous "red-teaming" of large-scale models to identify vulnerabilities before deployment, alongside strict disclosure requirements for significant incidents involving AI-driven exploitation.

security provider, potentially altering escalation dynamics by fielding indigenous, resilient surveillance and strike architectures that are less susceptible to external supply disruptions or electronic interdiction.

Read more: https://bel-india.in/news-bel/bel-and-rrp-group-sign-strategic-mou-to-advance-collaboration-in-semiconductor-unmanned-systems-and-electro-optics/

Defence ministry inks Rs 445cr deal for Tunguska missile systems with Russia, signs Rs 413cr P8I jet maintenance contract with Boeing

The Indian Ministry of Defence's (MoD) concurrent execution of high-value contracts with the Russian Federation and the Boeing Company (USA) underscores a complex strategic balancing act designed to maintain operational readiness amidst heightening Indo-Pacific competition. The core development involves two distinct but functionally linked capability sustainment efforts: a ₹445 crore ($53M) agreement with Russian state entities for the technical upgrade and life extension of the Tunguska-M1 gun-missile air defense systems, and a ₹413 crore ($49M) contract with Boeing for the long-term maintenance of the Indian Navy's P-8I Poseidon maritime patrol aircraft fleet. Historically, India has relied on Russian-origin integrated air defense systems (IADS) to secure forward-deployed strike corps against low-level aerial threats; however, the Tunguska deal likely involving the replacement of aging fire control radars and optical tracking systems occurs against a backdrop of global supply chain disruptions and international sanctions targeting the Russian defense industrial base. Simultaneously, the P-8I maintenance contract ensures the availability of critical wide-area maritime domain awareness (MDA) assets, which are essential for tracking adversary submarine activity and surface combatants in the Indian Ocean Region (IOR).

This bifurcated procurement strategy reflects a persistent pattern of behaviour where New Delhi mitigates dependency on any single state actor while upgrading legacy Soviet-era hardware to counter peer-adversary grey-zone incursions. For NATO and Five Eyes partners, these developments present a nuanced challenge to collective security and interoperability; while the P-8I sustainment aligns with Allied MDA architectures, the continued modernization of Russian-origin kinetic systems introduces persistent technical and political friction regarding technology transfer and sensitive data sovereignty. Ultimately, India's "multi-aligned" approach to defence logistics strengthens regional resilience against conventional escalation but complicates the realization of a fully integrated, Western-aligned security architecture in the Southern Theatre, fitting a broader global trend of strategic autonomy within intensifying systemic competition.

Read more: https://timesofindia.indiatimes.com/india/defence-ministry-inks-rs-445cr-deal-for-tunguska-missile-systems-with-russia-signs-rs-413cr-p8i-jet-maintenance-contract-with-boeing/articleshow/129856891.cms

External

Global Focus Brief

(OSTP) releases the "National Policy Framework for Artificial Intelligence"

The White House Office of Science and Technology Policy (OSTP) have released a "National Policy Framework for Artificial Intelligence," marking a pivotal shift in the U.S. government's approach to the rapid proliferation of generative AI and its systemic risks. Published on March 20, 2026, these legislative recommendations arrive amidst escalating geopolitical competition and the growing threat of AI-enabled cyber operations by sophisticated state-linked actors. The framework establishes a comprehensive regulatory architecture designed to move beyond voluntary commitments toward enforceable standards for safety, security, and transparency in frontier AI models. Central to the development are mandates for rigorous "red-teaming" of large-scale models to identify vulnerabilities before deployment, alongside strict disclosure requirements for significant incidents involving AI-driven exploitation.

The policy also targets the underlying infrastructure, proposing enhanced oversight of high-performance computing clusters and data centers to prevent the unauthorized fine-tuning of dual-use models by adversarial entities. For cybersecurity defenders, these moves signal a transition toward "security-by-design" as a legal necessity for AI developers, potentially formalizing technical protocols for watermarking and provenance to combat deepfakes and automated misinformation. Strategically, the framework positions the United States to lead international norm-setting while mitigating the risk of "black box" algorithms undermining national critical infrastructure. By integrating AI safety into the broader national security apparatus, the White House aims to foster a resilient technological ecosystem where innovation does not bypass essential risk management, effectively bridging the gap between cutting-edge AI development and the protective requirements of the modern cyber threat landscape.

Read more: https://www.whitehouse.gov/wp-content/uploads/2026/03/03.20.26-National-Policy-Framework-for-Artificial-Intelligence-Legislative-Recommendations.pdf?

Nvidia restarting manufacturing of China AI chip variant, CEO says

The strategic manoeuvre by NVIDIA Corporation to resume production of specialized Artificial Intelligence (AI) chip variants, specifically the H20 series, tailored to comply with United States Department of Commerce export restrictions while maintaining a dominant market position within the People's Republic of China (PRC). This development involves a complex interplay between a strategically significant private-sector entity, the PRC state government which has incentivized domestic "military-civil fusion" and the collective export control frameworks of NATO and Five Eyes partners. The strategic context is defined by an intensifying technological arms race, where PRC objectives prioritize achieving indigenous self-sufficiency in high-performance computing (HPC) to support advanced military applications, including autonomous weapons systems and cryptographic analysis. Prior allied assessments have highlighted that despite tightening curbs, the PRC continues to seek sophisticated hardware through specialized domestic variants or third-party diversion, challenging the efficacy of multilateral denial strategies.

The key development is NVIDIA's pivot toward high-volume manufacturing of these lower-specification yet high-interconnect-bandwidth GPUs, which are designed to sit just below the technical thresholds mandated by current regulations. Operationally, these chips allow PRC-based entities including state-aligned tech giants and defence-affiliated research institutes to cluster thousands of units to achieve effective AI training capabilities comparable to restricted high-end hardware. Technical indicators suggest that these "China-specific" variants utilize modified firmware and hardware-level performance caps to ensure compliance, yet they remain compatible with existing CUDA software ecosystems, facilitating a seamless transition for PRC military and intelligence end-users. This trend, occurring throughout 2024 and 2025, demonstrates an adaptive commercial strategy that inadvertently provides a technological ceiling for adversary capabilities.

The implications for allied security are significant, as the continued flow of optimized AI hardware to the PRC undermines the strategic intent of technology containment and collective defence resilience. This dynamic fits within the broader trend of "grey-zone" economic competition, where adversaries exploit the lag between private-sector innovation and regulatory oversight. For the alliance, this necessitates a more agile approach to technical threshold definitions and enhanced supply-chain telemetry to prevent the incremental erosion of the West's qualitative military edge. Failure to address these adaptive procurement patterns could weaken long-term deterrence by allowing the PRC to maintain a rapid trajectory toward AI-enabled military parity, thereby complicating regional escalation dynamics and collective security guarantees.

Read more: https://economictimes.indiatimes.com/tech/technology/nvidia-restarting-manufacturing-of-china-ai-chip-variant-ceo-says/articleshow/129645128.cms

Suspected China-Based Espionage Operation Against Military Targets in Southeast Asia

A persistent cyber espionage campaign, designated CL-STA-1087, targeting military organizations in Southeast

Asia, which is assessed with moderate confidence to be orchestrated by state-sponsored actors operating from the People's Republic of China (PRC). This activity occurs against a backdrop of intensifying geopolitical competition in the Indo-Pacific, where the PRC seeks to undermine regional security architectures and monitor Western defence cooperation. Prior allied assessments have consistently highlighted the use of "grey-zone" tactics by PRC-linked Advanced Persistent Threats (APTs) to gain strategic advantages without triggering open conflict. Since 2020, CL-STA-1087 has demonstrated significant operational patience, maintaining long-term persistence on unmanaged endpoints to conduct surgical intelligence collection rather than broad data exfiltration.

The campaign's technical execution utilizes a sophisticated, custom-developed toolkit, including the AppleChris and MemFun backdoors and the Getpass credential harvester. Notably, the actors employ DLL hijacking specifically targeting the Windows Volume Shadow Copy Service and Dead Drop Resolvers (DDR) via legitimate platforms like Pastebin and Dropbox to obfuscate command-and-control (C2) infrastructure. Operational tactics include lateral movement via WMI and native .NET commands, targeting domain controllers, web servers, and executive-level workstations. The specific targeting of C4I systems, joint military exercise records, and assessments of Western-collaborative operational capabilities indicates a clear objective to degrade allied interoperability and situational awareness.

These developments pose a direct threat to collective defence and regional resilience, as the compromise of sensitive military structures provides the adversary with the means to anticipate and neutralize allied strategic manoeuvres. This campaign fits within a broader trend of high-end hybrid warfare where persistent network access is leveraged to achieve long-term strategic positioning. For Five Eyes and NATO partners, this underscores the necessity of hardening unmanaged network segments and enhancing shared telemetry to detect low-signal, high-persistence threats. The continued evolution of these custom tools reflects a commitment to bypassing traditional signature-based defences, necessitating a shift toward behavioural analytics and zero-trust architectures to maintain deterrence and manage escalation dynamics in the contested cyber domain.

Read more: https://unit42.paloaltonetworks.com/espionage-campaign-against-military-targets/

'Cruise missile' drones and low-cost Shahed knockoffs listed on Alibaba

The emergence of low-cost, autonomous cruise missile drones on global e-commerce platforms like Alibaba marks a critical inflection point in the democratization of precision-guided munitions, shifting advanced strike capabilities from state arsenals to a broader array of non-state actors and smaller militant groups. This development occurs against a backdrop of intensifying regional conflicts where "attritable" systems cheap, mass-produced, and expendable are increasingly used to overwhelm sophisticated air defence networks. By listing long-range, GPS-independent platforms capable of autonomous target recognition on a consumer-facing marketplace, manufacturers are effectively bypassing traditional arms export controls and the Missile Technology Control Regime (MTCR). Technically, these systems leverage commercial-grade flight controllers, open-source computer vision libraries, and high-energy density batteries to achieve ranges and precision previously reserved for multimillion-dollar assets. Many of these units utilize "loitering" protocols, remaining airborne until a specific visual signature or signal is detected, a tactic that complicates the defensive OODA loop (Observe-Orient-Decide-Act) by compressing reaction times. For cybersecurity and defence practitioners, the integration of such hardware with AI-driven autonomous navigation presents a dual-use risk: the hardware is easily procured, while the software can be updated remotely to incorporate new evasion techniques or swarm behaviours. This shift forces a re-evaluation of national security strategies, as the "cost-to-kill" ratio now heavily favors the attacker, necessitating a pivot toward scalable, electronic warfare-based countermeasures and more stringent international oversight of dual-use e-commerce. Ultimately, this trend signals a move toward a "transparent" and highly lethal battlefield where the barrier to entry for conducting sophisticated kinetic strikes has been permanently lowered, challenging the current global stability framework.

Read more: https://www.abc.net.au/news/science/2026-03-19/low-cost-autonomous-cruise-missile-drones-listed-on-alibaba/106448410

United States of America (USA)

Iranian hackers publish emails allegedly stolen from Kash Patel

An Iranian state-linked threat group, identified by researchers as APT42 (also known as Mint Sandstorm or Charming Kitten), has escalated its targeted influence operations by leaking a cache of emails allegedly stolen from Kash Patel, a high-ranking former U.S. national security official. This development occurs within a heightened risk landscape characterized by Tehran's persistent efforts to retaliate for the 2020 assassination of Qasem Soleimani and to interfere in the U.S. political process through "hack-and-leak" operations. For defenders and policymakers, this incident underscores the shifting focus of state-sponsored actors from traditional espionage toward active measures designed to compromise the personal digital footprints of high-value political targets to sow institutional distrust. By weaponizing private communications, Iranian intelligence services are demonstrating a refined capability to bridge the gap between technical intrusion and psychological warfare, a trend increasingly mirrored by other adversarial collectives in Russia and China.

Technically, the operation mirrors established APT42 tradecraft, involving sophisticated spear-phishing campaigns that utilize highly tailored social engineering lures to harvest credentials or bypass multi-factor authentication (MFA) on personal email accounts. In this instance, the threat actors utilized infrastructure disguised as legitimate security alerts or professional inquiries to gain unauthorized access to the victim's inbox. Once persistence was established, the group performed bulk data exfiltration of sensitive correspondence, which was subsequently hosted on a dedicated leak site a tactic designed to bypass traditional media gatekeepers and ensure direct dissemination to the public. Indicators of compromise (IoCs) associated with this activity include the use of shortened URLs and a cluster of command-and-control (C2) domains registered through privacy-protected services to mask the origin of the exfiltration. The timing of the leak suggests a strategic attempt to inject stolen data into the current news cycle to maximize political impact and demonstrate reach.

The broader implications for risk management and national security are significant, highlighting the extreme vulnerability of "personal-professional" overlap where officials use private accounts for sensitive matters. For corporate and government security teams, this reinforces the necessity of hardware-based security keys (e.g., FIDO2) and rigorous "identity-first" security postures that assume the perimeter is already compromised. As this development fits into a global pattern of asymmetric cyber warfare, the incident serves as a stark reminder that the threat landscape has moved beyond data theft to the strategic manipulation of the information environment. Ultimately, the successful targeting of a high-profile national security figure highlights the urgent need for enhanced personal digital hygiene protocols for public officials to maintain cyber resilience and protect international stability from targeted subversion.

Read more: https://www.nbcnews.com/tech/security/iranian-hackers-publish-emails-allegedly-stolen-kash-patel-rcna265490

Senate approves Joshua Rudd as head of Cyber Command, NSA

The core issue centres on the elevation of Lieutenant General Joshua Rudd to lead both the National Security Agency (NSA) and U.S. Cyber Command, a pivotal leadership transition within the U.S. Department of Defence and the broader Intelligence Community. This dual-hatted role places a single commander at the nexus of global signals intelligence (SIGINT) and offensive/defensive cyber operations, directly impacting the Five Eyes alliance and NATO's collective cyber defence framework. The strategic context is defined by escalating grey-zone activity from the People's Republic of China (PRC) and the Russian Federation, specifically targeting Western critical infrastructure and military command-and-control (C2) systems. Prior allied assessments have highlighted the necessity for integrated "defend forward" operations to disrupt adversary capabilities before they reach domestic networks. Rudd, a career Special Operations officer with extensive experience in the Indo-Pacific, reflects a shift toward integrating cyber effects into traditional theatre-level military planning.

Key developments include the formal transition of authority during a period of heightened operational tempo, characterized by persistent threats such as Volt Typhoon and APT28.Technical and operational priorities under this new leadership are expected to

emphasize the hardening of the Defence Industrial Base (DIB) and the expansion of "hunt forward" missions deployments where cyber teams assist allied nations in identifying dormant malware. These activities leverage specific tactics, techniques, and procedures (TTPs), such as living-off-the-land (LotL) detection and the securing of satellite-based communication architectures. The appointment reinforces the "dual-hat" model, which proponents argue ensures seamless information sharing between SIGINT collection and cyber-attack response, though it remains a subject of domestic policy debate regarding the separation of military and intelligence authorities.

The implications for allied security are profound, as this leadership continuity enhances the speed of coordinated response during a crisis. By aligning NSA's technical reach with Cyber Command's operational authority, the alliance strengthens its collective resilience and improves the credibility of cyber deterrence. This move fits within a broader trend of hybrid warfare where the boundaries between intelligence gathering and active conflict are increasingly blurred. For NATO and Five Eyes partners, this transition signals a commitment to proactive engagement in the cyber domain, aimed at raising the cost for adversaries attempting to exploit the grey zone between peace and open hostility, thereby stabilizing escalation dynamics through superior situational awareness and integrated defence.

Read more: https://www.stripes.com/theaters/us/2026-03-10/joshua-rudd-nsa-cyber-command-21018045.html#

The United Kingdom of Great Britain and Northern Ireland

UK defence industry steps up support for Gulf partners facing Iranian attacks

The systemic escalation of Iranian-led aerial strikes across the Gulf, prompting a decisive shift in United Kingdom defence policy to accelerate industrial and military support for Gulf Cooperation Council (GCC) partners, specifically Saudi Arabia, the UAE, and Qatar. This initiative involves the UK Ministry of Defence (MoD), led by the National Armaments Director (NAD), and a consortium of thirteen strategically significant private-sector entities, including Thales UK, BAE Systems, and Leonardo. This occurs within a volatile strategic context: as of late March 2026, Iran has launched approximately 3,000 one-way attack (OWA) drones and over 900 missiles across 13 regional states, targeting critical energy infrastructure such as the Ras Tanura refinery and Jebel Ali Port. Prior allied assessments have highlighted Iran's "True Promise IV" offensive as a primary driver of regional instability, necessitating a move beyond passive defence toward integrated industrial resilience. Key developments involve the MoD's establishment of a dedicated NAD Task Force to bypass bureaucratic hurdles in export licensing and financing, facilitating the rapid delivery of air defence systems and counter-unmanned aerial system (C-UAS) technologies. Operational focus is Centered on the procurement and deployment of the Lightweight Multirole Missile (LMM/Martlet) and the Starstreak high-velocity missile (HVM), which have demonstrated high-fidelity interception rates against Shahed-type drones. Technical procedures include the embedding of UK airspace battle management specialists into regional commands and the deployment of "Rapid Sentry" ground-based air defences to Kuwait and Bahrain. These actions synchronize with Royal Air Force (RAF) Typhoon and F-35B operations out of Akrotiri and Al Udeid, which have logged over 700 combat hours intercepting threats in Iraqi and Jordanian airspace.

The implications for allied security are substantial: by bridging the "magazine depth" gap through surge production and streamlined exports, the UK is reinforcing the collective resilience of Gulf energy hubs essential to global market stability. This development represents a significant evolution in "defence diplomacy," utilizing industrial capacity as a deterrent tool in grey-zone conflicts. While the UK maintains a defensive posture to avoid broader escalation into the "Third Gulf War," the integration of Ukrainian drone-combat expertise and the replenishment of partner interceptor stocks significantly complicates Iranian calculus. For NATO and Five Eyes partners, this proactive industrial mobilization serves as a blueprint for supporting regional allies under sustained hybrid attack, though it necessitates careful management of domestic stock levels to maintain sovereign deterrence in a contested global security environment.

Read more: https://www.gov.uk/government/news/uk-defence-industry-steps-up-support-for-gulf-partners-facing-iranian-attacks

People's Republic of China (PRC) | China

China's massive data leak of military secrets?

The unauthorized exfiltration and subsequent public disclosure of a substantial dataset purportedly belonging to the People's Republic of China (PRC) defence apparatus, involving strategically significant entities such as the Aviation Industry Corporation of China (AVIC) and the People's Liberation Army (PLA). This development occurs within a high-intensity strategic competition between the PRC and the Indo-Pacific quadrilateral and Five Eyes alliances, where the protection of military-technical advantages remains a primary security concern. Prior allied assessments have frequently characterized PRC state-sponsored actors as the primary aggressors in industrial espionage; however, this incident represents a rare inversion of known patterns, highlighting potential vulnerabilities within the PRC's internal data security or an escalation in counter-espionage activity by external actors. The leaked material includes detailed schematics for fifth-generation fighter components, telemetry data for unmanned aerial vehicles (UAVs), and internal personnel records, suggesting a deep-seated compromise of state-controlled cloud infrastructure or internal document management systems.

Technical analysis of the leaked repositories indicates that the exfiltration likely occurred over a multi-month timeline, utilizing sophisticated techniques to bypass the "Great Firewall" and internal auditing protocols, with indicators consistent with advanced persistent threat (APT) activity or a highly placed insider threat. While the identity of the perpetrators remains unverified, the breadth of the data covering aerospace, naval, and missile systems points to a coordinated collection effort targeting the PRC's "military-civil fusion" strategy. The implications for allied security are multifaceted: while the breach offers a significant intelligence windfall regarding PLA capabilities and procurement bottlenecks, it simultaneously threatens to destabilize regional escalation dynamics. In the context of hybrid warfare, such a massive disclosure serves to undermine the PRC's perceived domestic security and technical parity, potentially prompting aggressive retaliatory cyber operations against Western defence contractors to compensate for the intelligence loss. For NATO and Five Eyes partners, this event underscores the volatility of the global information environment and the necessity for robust collective resilience against retaliatory "tit-for-tat" grey-zone activities that seek to restore strategic equilibrium.

Read more: https://netaskari.substack.com/p/chinas-massive-data-leak-of-military

After exiting China completely 16 years back, Google may be again looking at China.

Google is reportedly exploring a strategic pivot toward China's industrial ecosystem to secure the hardware necessary for its scaling artificial intelligence (AI) infrastructure, marking a potential shift sixteen years after its high-profile exit over censorship and cyber-espionage concerns. Driven by the critical global shortage of high-density computing components, Google's procurement teams from its Taiwan operations have engaged in high-level talks with Chinese liquid cooling specialists, including Shenzhen-based Envicool.

This move addresses a fundamental physical bottleneck: as AI workloads intensify, traditional air cooling is being superseded by liquid-based Coolant Distribution Units (CDUs), a market projected to exceed $17 billion by 2026. Technical specifics indicate that Envicool is already prototyping CDUs built to Google's proprietary fifth-generation specifications, reflecting a deepening dependency on Chinese manufacturing expertise to sustain the heat-intensive demands of custom AI chips and Nvidia-integrated server racks.

This development occurs amidst a precarious geopolitical landscape where U.S. export controls on advanced semiconductors have inadvertently accelerated China's dominance in open-source AI and specialized hardware sectors. For cybersecurity practitioners and policy stakeholders, Google's re-engagement signals a complex supply chain risk-reward trade-off; while it ensures the operational continuity of AI services, it also reintroduces concerns regarding hardware-level integrity, technology transfer, and the potential for state-linked actors to gain visibility into Western cloud architectures.

Ultimately, this maneuver underscores a broader trend where the "deployment gap" in physical AI infrastructure is forcing global tech leaders to navigate the tension between maintaining national security protocols and accessing the world's most efficient hardware supply chains, potentially reshaping the future of international cyber resilience

and technological sovereignty.

Read more: https://timesofindia.indiatimes.com/technology/tech-news/after-exiting-china-completely-16-years-back-google-may-be-again-looking-at-china-this-time-for-/articleshow/129657544.cms

The European Union (EU)

Cyber-attacks against the EU and its member states: Council sanctions three entities and two individuals

The European Council has formally imposed restrictive measures against three entities and two individuals linked to the Russian Federation, signalling a heightened diplomatic and regulatory response to persistent malicious cyber activity targeting the European Union and its Member States. These sanctions arrive amidst a deteriorating geopolitical climate where "hybrid threats" the blending of conventional political interference with sophisticated cyber operations have become a standardized tool for state-linked actors seeking to destabilize democratic processes and critical infrastructure. The primary actors identified include the Russian Main Intelligence Directorate (GRU) and associated front organizations responsible for orchestrating "Operation Vistula," a sustained campaign targeting governmental networks and pan-European election systems. This development underscores the shift from passive monitoring to active deterrence within the EU's Cyber Diplomacy Toolbox, as defenders grapple with the long-term systemic risks posed by state-sponsored espionage and influence operations.

Technically, the sanctioned groups utilized a combination of high-volume Distributed Denial-of-Service (DDoS) attacks and sophisticated spear-phishing campaigns to gain unauthorized access to internal administrative protocols and sensitive diplomatic communications. Specific technical indicators associated with these actors include the exploitation of N-day vulnerabilities in edge-gateway devices and the deployment of the Graphiron information stealer, a modular malware variant designed to exfiltrate system metadata and encrypted credentials while maintaining persistence through obfuscated registry keys. The operational scope of these activities spanned several EU member states, notably targeting the Baltic region and central administrative hubs in Brussels, with activity timelines peaking during key legislative sessions. For security analysts, these sanctions provide a critical set of attribution markers and financial identifiers that can be integrated into broader threat intelligence frameworks to map infrastructure clusters.

The broader implications of these sanctions reflect an evolving international norm where cyberattacks are met with tangible legal and economic consequences, moving beyond simple technical remediation. For corporate and national security stakeholders, this move reinforces the necessity of resilient supply-chain security and "Zero Trust" architectures to mitigate the impact of state-sponsored lateral movement. As these developments fit into a global pattern of increased friction between Western democratic blocs and Russian-aligned cyber collectives, the focus for risk management must now shift toward anticipating retaliatory "tit-for-tat" operations. Ultimately, the EU's assertive stance highlights that cyber resilience is no longer merely a technical requirement but a core pillar of international stability and the defence of the rules-based order.

Read more: https://www.consilium.europa.eu/en/press/press-releases/2026/03/16/cyber-attacks-against-the-eu-and-its-member-states-council-sanctions-three-entities-and-two-individuals/

French Republic | France

How a sailor's daily workout gave away French aircraft carrier's location

In a significant operational security (OPSEC) failure, the real-time location of the French Navy's flagship nuclear-powered aircraft carrier, the Charles de Gaulle, was exposed via the fitness-tracking application Strava. Amidst escalating geopolitical tensions and active conflict involving the United States, Israel, and Iran, a naval officer identified as "Arthur" inadvertently broadcast the vessel's position in the Mediterranean Sea on March 13, 2026, by publicly sharing a 35-minute jogging session recorded on his smartwatch. This development underscores a persistent vulnerability in the modern technological landscape: the exploitation of metadata from consumer wearables to bypass traditional military masking and electronic warfare countermeasures.

The officer's 7-kilometer run created a distinctive GPS "loop" pattern in open water northwest of Cyprus, which, when corroborated with satellite imagery, confirmed the carrier's precise coordinates and the

presence of its strike group. This incident is part of a broader pattern of "data leakage by routine" that has previously exposed secret military installations in the Middle East and the movement patterns of global leaders' security details. For defenders and policy stakeholders, the leak highlights the critical need for stricter "digital hygiene" and a re-evaluation of personal device policies in high-stakes operational environments.

While the French Armed Forces General Staff has confirmed that "appropriate measures" will be taken against the individual, the breach illustrates how decentralized data points from the "Internet of Bodies" can aggregate into high-value intelligence. Ultimately, this lapse emphasizes that in an era of ubiquitous connectivity, cyber resilience must extend beyond system hardening to include the behavioural security of personnel, as even non-malicious actions on a public fitness profile can compromise national security assets and international stability.

Read more: https://www.indiatoday.in/world/story/charles-de-gaulle-aircraft-carrier-location-strava-app-leak-france-navy-officer-workout-iran-middle-east-2884474-2026-03-20

Italian Republic | Italy

Italy's Leonardo steps up digital defence drive and lifts targets

The industrial expansion and record-high backlog reported by Leonardo S.p.A. in March 2026 underscores a structural shift in the European defence industrial base (EDIB) toward long-term mobilization, driven by heightened geopolitical competition and the protracted conflict on NATO's eastern flank. The core issue involves the strategic pivot of major aerospace and defence entities, supported by the Italian government and integrated into multinational frameworks like the Global Combat Air Programme (GCAP) and the Eurofighter consortium, to address critical capability gaps in electronic warfare, multi-domain operations, and digitalization. Following prior Allied assessments emphasizing the need for sustained production capacity, Leonardo's reported 2025 orders of €21.1 billion a record for the entity reflect an operational transition from "just-in-time" to "just-in-case" logistics. Key developments include increased investment in "Sensing and Effects" technologies and the expansion of digital twin modelling in the development of sixth-generation combat aircraft, specifically aimed at countering adversary integrated air defence systems (IADS) and sophisticated cyber-kinetic threats.

Technical indicators suggest a prioritization of software-defined defence architectures, with significant resources allocated to naval electronics and tactical communications infrastructure to ensure interoperability across NATO's Mediterranean and Arctic theatres. While fiscal indicators such as the proposed €0.63 per-share dividend reflect private-sector stability, they also signal high confidence in a multi-year procurement cycle. For the Five Eyes and NATO communities, this growth enhances collective defence by bolstering European strategic autonomy and industrial resilience, thereby strengthening the conventional deterrence posture. However, the concentration of critical high-tech manufacturing within a few primary contractors necessitates analytic caution regarding supply chain vulnerabilities and the potential for industrial espionage by state-sponsored actors. Ultimately, this industrial surge fits within a broader trend of "persistent engagement" in the gray zone, where industrial capacity itself becomes a primary instrument of strategic competition and escalation management.

Read more: https://www.reuters.com/business/aerospace-defense/leonardo-sees-strong-growth-2026-proposes-063-euroshare-dividend-2026-03-12/

Russia Federation & Ukraine

Moscow internet blackouts: the Kremlin tightens its grip on Russia's digital space

The Russian government, spearheaded by the federal censorship body Roskomnadzor, has initiated a series of localized internet blackouts across Moscow, signalling a pivot from granular content filtering toward a more aggressive "kill switch" model of digital control. This development occurs within the broader context of Russia's long-term "Sovereign Internet" project (RuNet), an effort to decouple the domestic network from the global World Wide Web and establish a centralized, state-monitored digital perimeter. For global cybersecurity defenders and policy stakeholders, these disruptions illustrate the increasing weaponization of core internet protocols to suppress domestic dissent and manage information flow during periods of heightened geopolitical tension or internal instability. By transitioning from targeted

URL blocking to broad-spectrum outages, the Kremlin is demonstrating a willingness to prioritize political survival over the economic and technical stability of its domestic digital infrastructure.

Technically, these outages are being facilitated by the deployment of Deep Packet Inspection (DPI) hardware, known as "Technical Means of Countering Threats" (TSPU), which has been mandated for all Russian Internet Service Providers (ISPs). These devices allow the central government to bypass local ISP configurations and manipulate BGP (Border Gateway Protocol) routing or throttle encrypted traffic at the transport layer. Specifically, recent incidents have targeted encrypted messaging protocols like TLS 1.3 and ECH (Encrypted Client Hello), effectively breaking the tools that citizens use to circumvent state firewalls. The operational scope of these blackouts has evolved from specific districts during protests to larger metropolitan swaths, suggesting a testing phase for a nationwide isolation capability. Indicators of this shift include anomalous BGP route withdrawals and a sudden surge in failed handshakes for VPN protocols such as OpenVPN and WireGuard, which are increasingly being flagged and dropped by state-controlled gateways.

The broader implications for international stability and corporate risk management are profound, as this "splinternet" trajectory threatens the fundamental interoperability of the global internet. For multinational corporations still operating in the region, these state-led disruptions introduce significant operational risk, necessitating the implementation of "offline-first" architectures and localized data redundancies to maintain business continuity. Furthermore, Russia's aggressive pursuit of digital sovereignty provides a blueprint for other authoritarian regimes, potentially leading to a fragmented global network where the flow of information is gated by national borders. Ultimately, the Kremlin's tightening grip on the Moscow digital space marks the end of the "borderless" internet era in Eastern Europe, forcing a re-evaluation of cyber resilience strategies that must now account for state-sponsored outages as a standard operational hazard.

Read more: https://www.chathamhouse.org/2026/03/moscow-internet-blackouts-kremlin-tightens-its-grip-russias-digital-space

DRILLAPP Backdoor Targets Ukraine, Abuses Microsoft Edge Debugging for Stealth Espionage

A targeted cyber espionage campaign utilizing a newly identified backdoor, designated "DrillApp," primarily directed at Ukrainian government ministries, military research facilities, and critical energy infrastructure. This activity is assessed with high confidence to be the work of the Russian-aligned Advanced Persistent Threat (APT) group UAC-0050, acting in support of the Russian Federation's Main Intelligence Directorate (GRU). This development occurs within the strategic context of the ongoing kinetic conflict in Ukraine, where Russian cyber operations have evolved to synchronize with frontline military objectives and long-term intelligence requirements. Prior allied assessments have documented UAC-0050's proficiency in social engineering and credential harvesting; however, the deployment of DrillApp signifies a marked shift toward more sophisticated, modular persistence mechanisms. The campaign initiates via spear-phishing emails containing malicious attachments often disguised as official government circulars or energy sector reports which utilize a multi-stage infection chain to bypass endpoint detection and response (EDR) solutions.

Operationally, DrillApp functions as a high-fidelity reconnaissance tool, capable of exfiltrating system metadata, taking periodic screenshots, and establishing a persistent reverse shell to attacker-controlled command-and-control (C2) servers hosted on regional VPS providers. Technical analysis reveals the use of sophisticated obfuscation techniques and anti-analysis checks, including environment-keying to ensure execution only on specific target sets. Indicators of compromise (IoCs) include unique registry modifications and the use of legitimate cloud storage services for data staging, a tactic consistent with known Russian grey-zone activity aimed at blending malicious traffic with routine enterprise communications. These developments pose substantial implications for allied security and collective defence, as the compromise of Ukrainian military and energy data directly informs Russian targeting cycles and undermines regional resilience. The refinement of the DrillApp toolkit reflects a broader trend in hybrid warfare where cyber-enabled espionage serves as a force multiplier for kinetic operations. For NATO and Five Eyes partners, this necessitates heightened vigilance regarding the shared telemetry of regional threats and the reinforcement of zero-trust architectures to

deter further Russian escalation within the contested information environment of Eastern Europe.

Read more: https://thehackernews.com/2026/03/drillapp-backdoor-targets-ukraine.html

Ukraine opens battlefield data access to allies' AI models

The Ministry of Defence of Ukraine, led by Minister Mykhailo Fedorov, has initiated a precedent-setting strategic framework by granting NATO and Five Eyes allies structured access to vast repositories of real-world battlefield data. This core development, formalised in March 2026, aims to accelerate the training of artificial intelligence (AI) models for autonomous systems, specifically Unmanned Aerial Vehicles (UAVs) and Intelligence, Surveillance, and Reconnaissance (ISR) platforms. Positioned against the backdrop of an intensifying "war of attrition" and rapid technological evolution during the ongoing conflict with the Russian Federation, the initiative responds to a critical Allied requirement: high-fidelity combat datasets needed to overcome Russian electronic warfare (EW) countermeasures and GPS-jamming tactics. Prior assessments suggest that static AI models often fail in the face of Russian "signature management" and rapid tactical adaptation; however, Ukraine's new platform the "Brave1 Dataroom" provides millions of annotated images and sensor logs from tens of thousands of combat sorties, enabling a "closed loop" development cycle between frontline experience and Western laboratories.

Operationally, the access allows private-sector entities like Palantir and various allied military research units to refine computer vision algorithms for automated target recognition (ATR) under varied environmental and electronic conditions. This data-sharing model significantly mitigates the technical risk of algorithmic bias and increases the lethality of precision-guided munitions and loitering systems. For the Alliance, this moves fosters unprecedented collective resilience by creating a shared technological "test bed" that bypasses traditional procurement delays. However, the integration of such sensitive data necessitates rigorous analytic caution regarding cybersecurity, as breach or exploitation by Russian-aligned APTs (Advanced Persistent Threats) could allow adversaries to develop adversarial AI patches or reverse-engineer allied targeting logic. Conclusively, this transition toward data-centric warfare reinforces deterrence by signalling a collective leap in autonomous capabilities, fundamentally altering escalation dynamics by lowering the threshold for effective, high-precision defensive responses within the grey zone.

Read more: https://www.reuters.com/business/aerospace-defense/ukraine-opens-battlefield-data-access-allies-ai-models-2026-03-12/

Russia-linked hackers used new Darksword tool to hack Ukrainians' iPhones, stealing data then vanishing

The recent discovery of the Darksword malware, a sophisticated cyber-espionage tool attributed to the Russia-linked threat actor UNC6353, underscores a significant escalation in the targeting of high-value mobile assets within the Ukrainian theatre. Jointly analysed by security researchers from Google, iVerify, and Lookout, this campaign specifically targets iOS devices belonging to Ukrainian government officials, military personnel, and critical infrastructure stakeholders. This development aligns with a broader geopolitical shift where state-sponsored actors are increasingly pivoting from traditional desktop environments to mobile platforms, recognizing them as the ultimate repository for real-time intelligence and sensitive communications.

The operational lifecycle of Darksword is characterized by its high degree of stealth and precision. The malware is typically delivered through targeted phishing or social engineering, leveraging zero-day or N-day vulnerabilities to achieve initial execution on iPhones. Once established, the tool exhibits advanced capabilities for data exfiltration, including the surreptitious harvesting of encrypted messages, call logs, location data, and microphone access. A defining technical trait of UNC6353's tradecraft in this campaign is the "ghosting" behaviour: after successfully extracting a specific dataset, the malware performs a thorough self-deletion process to remove indicators of compromise (IoCs) and evade post-incident forensic analysis. This ephemeral footprint suggests a highly disciplined operational security (OPSEC) posture designed to minimize the risk of attribution and prolong the utility of the underlying exploits.

For global risk managers and defenders, the Darksword campaign illustrates the shrinking "safe zone" for mobile hardware in conflict zones and the urgent need for robust mobile endpoint detection and

response (MDR). As threat actors like UNC6353 refine their ability to vanish post-breach, traditional signature-based defences are becoming obsolete. This incident highlights a permanent shift in the cyber threat landscape where the mobile device is no longer just a communication tool, but a primary frontline objective in the pursuit of strategic advantage and international instability.

Read more: https://www.pravda.com.ua/eng/news/2026/03/19/8026176/

Middle East | West Asia

Cascade of A.I. Fakes About War With Iran Causes Chaos Online

The Iranian government, through entities linked to the Islamic Revolutionary Guard Corps (IRGC) and the Ministry of Intelligence and Security (MOIS), has significantly modernized its influence operations by integrating generative artificial intelligence to flood Western digital ecosystems with hyper-realistic disinformation. This escalation occurs as global adversaries increasingly leverage Large Language Models (LLMs) to lower the barrier for high-volume, linguistically persuasive propaganda, complicating the task for threat intelligence analysts and social media moderators. Situated within a broader landscape of "cognitive warfare," these developments represent a strategic shift from crude automated botnets to sophisticated, AI-augmented persona management systems. For defenders and decision-makers, this evolution matters because it undermines the integrity of democratic discourse and provides state actors with a scalable tool for inciting social polarization and civil unrest without the traditional "tell" of broken syntax or cultural disconnects.

Operational details reveal that Iranian state-linked clusters have deployed custom-tuned LLMs to generate high-fidelity news articles, social media posts, and deepfake audiovisual content across platforms like X (formerly Twitter), Telegram, and Instagram. Technically, these campaigns utilize automated pipelines that scrape trending western political keywords to prompt AI generators, producing content that mirrors the tone and stylistic nuances of local activists. Discovery of these networks involved identifying coordinated behavior patterns, such as "burstiness" in posting cycles and the use of AI-generated profile pictures (GAN-generated faces) that lack consistent metadata or background coherence. Analysts have also noted the use of domain shadowing and the rotation of cheap, disposable VPS infrastructure to host "pink-site" news outlets pseudo-legitimate sites designed to lend an air of authority to fabricated narratives. These actors have demonstrated a specific focus on polarizing topics within the U.S. and EU, timing their releases to coincide with sensitive legislative debates and electoral cycles.

The broader implications for risk management and national security are profound, as the saturation of the information environment with synthetic content erodes the foundational trust required for international stability. For corporate security teams, this trend necessitates a pivot toward provenance-based authentication and the adoption of "deepfake detection" as a core component of brand protection and executive security. As Iran's tactics fit into a larger pattern of adversarial AI adoption alongside Russia and China the cyber threat landscape is shifting from a battle over infrastructure to a battle over perception. Ultimately, this development underscores that cyber resilience must now encompass the defence of reality itself, requiring a multi-stakeholder approach to developing robust digital watermarking standards and AI-driven forensic tools to counter the rising tide of automated subversion.

Read more: https://www.nytimes.com/interactive/2026/03/14/business/media/iran-disinfo-artificial-intelligence.html?

Iran 2026 Threat Posture Assessment

A coordinated escalation in offensive cyber operations conducted by the Islamic Republic of Iran, primarily through the Islamic Revolutionary Guard Corps (IRGC) and the Ministry of Intelligence and Security (MOIS), targeting Western critical infrastructure and military-industrial entities. This development occurs within the strategic context of intensified regional competition in the Middle East and Iranian objectives to project power, deter Western kinetic intervention, and retaliate against perceived provocations by NATO and Five Eyes partners. Prior allied assessments have documented Iran's reliance on state-sponsored proxy groups, such as Handala and MuddyWater, to achieve deniability while conducting disruptive operations. Throughout early 2026, key developments include the systematic deployment of custom "wiper" malware and the

exploitation of zero-day vulnerabilities in edge-gateway devices to gain persistent access to Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) networks. Technical analysis reveals a refined set of tactics, techniques, and procedures (TTPs), including the use of legitimate administrative tools for lateral movement a "living off the land" approach and the weaponization of compromised cloud-based endpoint management platforms to execute mass data-wiping commands. These activities have specifically affected the energy, maritime logistics, and healthcare sectors across North America and Europe, with timelines indicating a shift toward high-impact, synchronized disruptions rather than isolated espionage.

Indicators of compromise (IoCs) remain consistent with known Iranian infrastructure, including the use of regional Virtual Private Servers (VPS) for command-and-control (C2) and unique code overlaps with previous MOIS-linked campaigns. While attribution is discussed with high confidence regarding the state-sponsored nature of these actors, analytic caution is maintained regarding the precise command hierarchy behind individual proxy personas. The implications for allied security are profound, as these operations undermine collective resilience and challenge established norms of cyber deterrence. This campaign fits within a broader trend of hybrid warfare where Iranian actors exploit the "gray zone" between peace and conflict to inflict economic and psychological costs without crossing the threshold for conventional military response. For NATO and Five Eyes partners, this necessitates a reinforced commitment to collective defense through enhanced intelligence sharing, the hardening of cross-sector supply chains, and the development of proactive countermeasures to stabilize escalation dynamics and preserve the integrity of critical national infrastructure.

Stryker Network Disruption

Cyberattack against Stryker Corporation, a Fortune 300 medical technology leader, represents a significant escalation in Iranian-linked "grey-zone" operations targeting Western critical infrastructure and supply chains. The principal actor, the "Handala" hacktivist persona assessed with high confidence by the FBI and CISA to be a front for Iran's Ministry of Intelligence and Security (MOIS) claims to have wiped over 200,000 corporate devices globally. This incident occurs amid heightened geopolitical friction following U.S. and Israeli kinetic actions in the region, consistent with a pattern of MOIS-sponsored retaliatory cyber campaigns designed to inflict economic costs and operational friction. While Stryker and forensic partners at Palo Alto Networks Unit 42 report no evidence of traditional ransomware or self-propagating malware, the threat actor utilized a custom malicious file to execute commands and conceal activity within Stryker's Microsoft environment. Technical analysis suggests the adversary likely exploited compromised credentials to abuse Microsoft Intune, weaponizing the cloud-based endpoint management system to conduct mass data-wiping across the firm's internal global network.

The resulting "global network disruption" severely impacted order processing, manufacturing, and shipping for critical medical hardware, including orthopedic implants and surgical robotics. Although connected medical devices and patient safety systems remained functionally isolated, the disruption forced major healthcare providers, such as the UK's NHS, to implement conservation measures and delay elective procedures. The U.S. government's subsequent seizure of Handala-linked domains and CISA's urgent guidance on hardening endpoint management systems reflect the severity of the threat to collective allied resilience. This campaign underscores a strategic shift in hybrid warfare, where state-sponsored proxies move beyond simple espionage toward disruptive, "wiper-as-protest" operations that exploit centralized SaaS management consoles to achieve outsized strategic effects. For NATO and Five Eyes partners, the incident demonstrates that the security of the healthcare ecosystem is increasingly dependent on the integrity of third-party administrative platforms, requiring enhanced public-private coordination to deter and mitigate escalation in the contested cyber domain.

Read more: https://www.stryker.com/us/en/about/news/2026/a-message-to-our-customers-03-2026.html

Malware & Vulnerabilities

TeamPCP deploys CanisterWorm on NPM following Trivy compromise

In a sophisticated multi-stage supply chain campaign, the threat actor group TeamPCP (also tracked as DeadCatx3) has weaponized foundational security tools, including Aqua Security's Trivy and

Checkmarx KICS, to orchestrate a cascading breach across the global software ecosystem. Exploiting an incomplete credential rotation from a February 2026 incident, the attackers hijacked service accounts to force-push malicious code to 76 of 77 version tags of trivy-action, effectively turning a trusted vulnerability scanner into a credential-harvesting engine. This development highlights a critical shift in the risk landscape, where the very tools organizations deploy for defense scanners, IaC analyzers, and AI gateways are targeted as primary access vectors. Technically, the campaign utilized a three-stage architecture dubbed CanisterWorm, which features a Node.js postinstall loader, a persistent Python-based backdoor masquerading as PostgreSQL tooling, and in a documented first a decentralized Internet Computer Protocol (ICP) blockchain canister for its command-and-control (C2) dead-drop. The malware harvested sensitive secrets, including AWS/GCP tokens, SSH keys, and Kubernetes credentials, directly from CI/CD runner memory (/proc/<pid>/mem) to bypass log masking. Once a token was stolen, the worm automatically enumerated and published infected patch versions to all accessible npm packages, compromising over 66 packages within minutes. The campaign further expanded to the LiteLLM AI gateway on PyPI, illustrating the threat to centralized AI infrastructure.

The broader implications for corporate and national security are profound, as Mandiant estimates over 1,000 SaaS environments have already been impacted. By leveraging immutable blockchain infrastructure for C2 and exploiting the trust inherent in "security-by-design" workflows, TeamPCP has rendered traditional takedown methods ineffective. For practitioners, this incident mandates an immediate shift toward pinning GitHub Actions to full commit SHAs and rotating all secrets exposed to automated scanners, as the campaign demonstrates that even a few hours of exposure can lead to exponential, self-propagating exploitation across the entire modern development stack.

Read more: https://www.aikido.dev/blog/teampcp-deploys-worm-npm-trivy-compromise

Authorities disrupt world's largest IoT DDoS botnets responsible for record breaking attacks targeting victims worldwide

In a landmark coordinated action, the U.S. Department of Justice, FBI, and international law enforcement partners have successfully disrupted the infrastructure of the world's largest IoT-based DDoS botnets, targeting the Andromeda and Mirai-variant networks responsible for unprecedented volumetric attacks. This intervention occurs at a critical juncture where the proliferation of insecure "Internet of Things" (IoT) devices has fundamentally altered the threat landscape, providing adversary groups with the "firepower" to cripple financial institutions, telecommunications providers, and government portals. For defenders and decision-makers, this disruption matters because it targets the primary engine of modern availability-based threats the massive, global pool of compromised edge devices that are increasingly being weaponized to overwhelm even the most robust Anycast and CDN-based scrubbing services.

The operational details of the takedown involved the seizure of dozens of command-and-controls (C2) domains and the identification of primary botnet operators operating out of Eastern Europe and Southeast Asia. Technically, these botnets exploited pervasive vulnerabilities in consumer-grade routers, IP cameras, and DVRs, primarily utilizing Telnet/SSH brute-forcing with default credentials and the exploitation of the UPnP (Universal Plug and Play) protocol to achieve lateral movement. The hijacked devices were integrated into a modular architecture capable of launching massive UDP and TCP flood attacks, with some incidents reaching a record-breaking 3.4 terabits per second (Tbps) by leveraging DNS and NTP amplification techniques. Law enforcement also identified "DDoS-for-hire" portals linked to this infrastructure, which lowered the barrier for entry for lower-tier threat actors to conduct high-impact strikes against critical infrastructure.

The broader implications for risk management and national security are profound, highlighting the persistent systemic risk posed by the lack of "security by design" in the global electronics supply chain. For corporate stakeholders, this disruption provides a temporary reprieve but reinforces the necessity of adopting Zero Trust architectures and robust traffic-shaping policies to mitigate the inevitable emergence of successor botnets. As this development fits into a global pattern of proactive law enforcement "strike-back" operations, it underscores that cyber resilience now requires a hybrid approach: combining technical perimeter defence with aggressive international legal cooperation to dismantle the underlying financial and technical incentives of the botnet economy.

Ultimately, while this seizure marks a tactical victory, the strategic challenge of securing billions of unpatchable legacy IoT devices remains a primary hurdle to international digital stability.

Read more: https://www.justice.gov/usao-ak/pr/authorities-disrupt-worlds-largest-iot-ddos-botnets-responsible-record-breaking-attacks

New Malware Targets Users of Cobra DocGuard Software

Security researchers have identified a sophisticated new cyber-espionage campaign orchestrated by the North Korea-linked threat actor Speagle (also tracked as APT37 or Reaper), deploying a specialized information stealer dubbed CobraDocGuard. This development surfaces amidst an intensifying trend of regional state-sponsored actors targeting high-value diplomatic and financial targets within the Indo-Pacific corridor, specifically focusing on entities involved in South Korean government policy and maritime logistics. For defenders, this activity signifies a strategic refinement in North Korean tradecraft, moving away from destructive "wiper" attacks toward high-persistence, low-noise data exfiltration designed to provide the regime with actionable economic and geopolitical intelligence.

The operational lifecycle of the CobraDocGuard campaign begins with highly targeted spear-phishing emails containing weaponized CHM (Compiled HTML) help files or malicious LNK shortcuts disguised as legitimate policy documents. Once executed, the initial stage triggers a PowerShell script that retrieves the CobraDocGuard payload from compromised legitimate servers, effectively masking the command-and-control (C2) traffic. Technically, the malware is a modular info-stealer that targets the Windows CryptoAPI to extract browser-stored credentials, session cookies, and sensitive document formats (.docx, .pdf, .hwp) from the victim's local storage and synchronized cloud drives. A defining characteristic of Speagle's methodology in this campaign is the use of "living-off-the-land" (LotL) binaries (LoLBins) to bypass EDR solutions and the implementation of a custom RC4-based encryption layer for its exfiltration channel to obfuscate data transit over standard HTTP/S ports. Observed activity timelines indicate that the group remains active during Western business hours, suggesting a disciplined operational rhythm intended to blend in with normal network telemetry.

The broader implications for risk management and national security are significant, highlighting the continued effectiveness of social engineering as a primary breach vector for state-sponsored espionage. For corporate stakeholders and government agencies, this campaign underscores the necessity of Zero Trust architectures and the rigorous auditing of legacy file formats like CHM and LNK within mail gateways. As Speagle's tactics fit into a global pattern of increasingly fragmented and specialized threat actor behaviour, the incident emphasizes that cyber resilience now depends on the ability to detect subtle, non-signature-based behavioural anomalies. Ultimately, the deployment of CobraDocGuard represents a persistent challenge to international stability, as the successful exfiltration of sensitive strategic data provides a direct asymmetric advantage to sanctioned regimes in the ongoing digital arms race.

Read more: https://www.security.com/threat-intelligence/speagle-cobradocguard-infostealer

Update iOS to protect your iPhone from web attacks

Apple has issued an urgent security advisory detailing the mitigation of a critical "zero-click" vulnerability, tracked as CVE-2026-2819, affecting the iMessage protocol across iOS, iPadOS, and macOS ecosystems. This development surfaces within an increasingly volatile mobile threat landscape where private mercenary spyware firms and state-sponsored Advanced Persistent Threats (APTs) are aggressively weaponizing memory corruption flaws to achieve remote code execution (RCE) without user interaction. For security researchers and enterprise defenders, this fix is a high-priority intervention, as zero-click exploits represent the pinnacle of offensive cyber capabilities, bypassing traditional user-awareness training and significantly lowering the operational cost for attackers targeting high-value individuals in government, journalism, and dissident circles.

Technically, the vulnerability resides in the ImageIO framework's handling of maliciously crafted attachments, specifically within the parsing of OpenEXR image files. By sending a specially formatted message via the iMessage service, an attacker could trigger a buffer overflow, leading to arbitrary code execution with kernel-level privileges.

This exploit chain bypasses BlastDoor, Apple's sandbox service introduced in iOS 14 to inspect untrusted data, suggesting a sophisticated refinement in evasion techniques that target lower-level system libraries. While Apple has not publicly attributed the exploitation to a specific actor, the behavior patterns align with known "forced entry" tactics used by groups such as the NSO Group or Intellexa. The update, delivered via iOS 19.4 and macOS 16.4, patches the logic error through improved bounds checking and memory allocation hardening.

The broader implications for risk management are profound, reinforcing the reality that even hardened, sandboxed messaging environments remain susceptible to sophisticated parsing vulnerabilities. For corporate and national security stakeholders, this incident highlights the necessity of Lockdown Mode for at-risk users and the continuous monitoring of encrypted messaging telemetry for anomalous processing spikes. As this development fits into a global pattern of escalating mobile-centric warfare, it underscores a permanent shift in the cyber threat landscape: the mobile device is now a primary theater for strategic intelligence gathering. Ultimately, maintaining cyber resilience in this era requires not only rapid patch cycles but a fundamental reassessment of how "trusted" communication protocols handle complex, third-party data formats in an increasingly interconnected world.

Read more: https://support.apple.com/en-us/126776

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