CLAWS Newsletter

Cyber Index | Volume II | Issue 05

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…….	I
External……	III – IV
United States of America (USA)…….……	01
The United Kingdom of Great Britain and Northern Ireland……	01
People's Republic of China (PRC) | China ……..……	02 – 04
Islamic Republic of Pakistan …….……	04 – 05
The European Union (EU) ……..	05 – 07
Russia Federation & Ukraine ……..……..……	07
Middle East | West Asia ……..……..……	07 – 09
Malware & Vulnerabilities ……..……..……	09 – 11

Internal

APT36: A Nightmare of Vibeware

The persistent targeting of government and military entities in South Asia by the Pakistan-aligned threat actor APT36 (also known as Transparent Tribe) represents a sophisticated intelligence-gathering operation utilizing the "Vibeware" malware suite. The principal actors involved include the Pakistan-linked Advanced Persistent Threat (APT) group and its primary targets within the Indian defense and diplomatic sectors. Within the strategic context of protracted regional rivalry and documented adversary patterns of utilizing social engineering to facilitate cyber espionage, prior Allied assessments have characterized APT36 as a disciplined actor focused on long-term data exfiltration. Recent operational developments indicate a shift in tactics, techniques, and procedures (TTPs), specifically the deployment of the "Nightmare" and "Vibeware" implants through multi-stage infection vectors initiated via spear-phishing and compromised legitimate websites. Technically, these implants utilize the Telegram API for command-and-control (C2) communication a tactic designed to blend malicious traffic with legitimate encrypted application data to bypass traditional network monitoring and signature-based detection.

The malware facilitates comprehensive system reconnaissance, keystroke logging, and the exfiltration of sensitive document formats, targeting the integrity of official communications and operational planning. While the technical sophistication of these tools is assessed as moderate, their effectiveness is bolstered by high-fidelity lures tailored to regional security concerns. For Allied interests, this campaign underscores the vulnerability of partner networks to persistent, state-aligned proxies that leverage ubiquitous consumer technologies to mask espionage activities. The continued evolution of APT36's toolkit complicates regional stability and increases the risk of information leakage in contested environments. This activity reflects broader trends in grey-zone competition, where the low-cost exploitation of encrypted platforms provides adversaries with sustainable access to high-value intelligence, necessitating enhanced collective resilience and shared technical indicators to maintain a credible defensive posture in the Indo-Pacific.

Read more: https://businessinsights.bitdefender.com/apt36-nightmare-vibeware

Defence Ministry signs deal worth ₹5,083 crore to buy ALH Mk-III choppers, Shtil missiles to boost maritime security

The Ministry of Defence (MoD) of India and Hindustan Aeronautics Limited (HAL) have entered a definitive procurement framework valued at ₹5,083 crore, primarily focused on the acquisition of Advanced Light Helicopters (ALH) and the integration of Vertical Launch Short Range Surface-to-Air Missile (VL-SRSAM) systems. This acquisition occurs within a strategic landscape characterized by heightened maritime competition in the Indian Ocean Region (IOR) and persistent territorial tensions along the Line of Actual Control (LAC). Indian defence doctrine increasingly emphasizes "Atmanirbharta" (self-reliance) to mitigate supply chain vulnerabilities associated with historical dependencies on foreign Original Equipment Manufacturers (OEMs), particularly in light of shifting geopolitical alignments and potential sanctions-related disruptions. The ALH platforms, specifically the Mk III and Mk IV variants, are engineered for multi-mission roles including tactical troop transport, casualty evacuation, and underslung load operations in high-altitude environments, featuring integrated electronic warfare (EW) suites and glass cockpits to enhance survivability against adversary man-portable air-defence systems (MANPADS).

Concurrently, the VL-SRSAM systems, developed by the Defence Research and Development Organisation (DRDO), utilize active radar homing and 360-degree coverage to intercept high-speed aerial threats, including sea-skimming anti-ship missiles and unmanned aerial vehicles (UAVs). These technical advancements reflect a prioritized response to the proliferation of precision-guided munitions among regional adversaries. The long-term implications for allied security and regional deterrence are significant; the maturation of indigenous aerospace and missile capabilities enhances India's role as a net security provider while complicating adversary

anti-access/area-denial (A2/AD) strategies. Furthermore, the standardization of these platforms across the Indian Army and Navy suggests an intent to improve joint-force interoperability and operational resilience. This development fits within a broader trend of middle-power military modernization designed to bolster grey-zone deterrence and maintain tactical parity in an increasingly contested multipolar security environment.

Read more: https://www.thehindu.com/news/national/defence-ministry-hal-5083-crore-contract-advanced-light-helicopters-surface-to-air-vertical-launch-shtil-missiles/article70699034.ece

DRDO's Ghatak combat drone programme gathers pace; 60 units planned

The acceleration of the Ghatak Unmanned Combat Aerial Vehicle (UCAV) program by the Defence Research and Development Organisation (DRDO), with a planned procurement of 60 units, marks a critical advancement in India's indigenous stealth strike capabilities and long-range power projection. This development involves the Indian Ministry of Defence, the Aeronautical Development Agency (ADA), and key private-sector manufacturing partners, occurring against a backdrop of intensifying competition in the Indo-Pacific and persistent two-front security challenges along the Line of Actual Control (LAC). Strategic context is defined by the proliferation of sophisticated Anti-Access/Area-Denial (A2/AD) bubbles by regional adversaries, necessitating low-observable platforms capable of penetrating contested airspace a requirement previously identified in allied assessments of evolving South Asian military doctrine.

The Ghatak, a flying-wing technology demonstrator derived from the Autonomous Unmanned Research Aircraft (AURA) project, incorporates internal weapons bays and radar-absorbent materials (RAM) designed to minimize its Radar Cross-Section (RCS). Technical milestones indicate the integration of a modified Kaveri dry engine variant for propulsion and the implementation of advanced data links for "manned-unmanned teaming" (MUM-T) operations. These systems are intended to execute precision strikes and deep-penetration surveillance while operating in high-threat environments where traditional manned assets face prohibitive risk. For NATO and Five Eyes partners, the fielding of a 60-unit UCAV fleet by a key strategic partner shifts regional escalation dynamics and enhances collective resilience by diversifying the democratic technology base for autonomous systems. The maturation of this program reflects a broader trend in grey-zone activity and hybrid warfare, where the mass deployment of stealth-capable attrition-tolerant platforms is prioritized to disrupt adversary decision cycles. Ultimately, the Ghatak program strengthens regional deterrence by complicating adversary defensive planning and signifies a transition toward more aggressive, technology-centric defence postures within the framework of global strategic competition.

Read more: https://www.business-standard.com/external-affairs-defence-security/news/drdo-s-ghatak-combat-drone-programme-gathers-pace-60-units-planned-126030301087_1.html

Indian Air Force gets defence board nod to buy 5 S-400s from Russia

The Indian Air Force (IAF) has advanced a significant strategic proposal, recently cleared by the Defence Procurement Board (DPB), to acquire five additional Russian-origin S-400 (SA-21 Growler) air defence squadrons, augmenting the initial five-system contract signed in 2018. This procurement initiative, involving the Russian state intermediary Rosoboronexport and potentially Indian private-sector entities for long-term maintenance, repair, and overhaul (MRO), occurs against a backdrop of intensified regional ballistic missile and loitering munition proliferation. Allied assessments likely emphasize the strategic significance of "Operation Sindoor" in May 2025, during which Indian S-400 batteries reportedly demonstrated high operational efficacy, achieving long-range intercepts including a high-value Pakistani electronic intelligence (ELINT) aircraft at approximately 314 km and effectively establishing an anti-access/area-denial (A2/AD) bubble that constrained adversary sorties.

The proposed expansion to a ten-squadron fleet, complemented by the potential fast-track acquisition of Pantsir-S1 point-defence systems to mitigate saturation strike vulnerabilities, reflects a disciplined shift toward a layered, multi-tier integrated air defence system (IADS). While this development enhances India's sovereign

deterrence against peer competitors on its northern and western frontiers, it concurrently complicates allied interoperability and underscores the persistent challenge of secondary sanctions regimes. Ultimately, India's deepening commitment to Russian strategic hardware, despite ongoing global shifts in the defence industrial base, signals a prioritization of immediate kinetic readiness over Western technological alignment, reinforcing a broader trend of "grey zone" defensive consolidation where regional powers utilize advanced A2/AD capabilities to decouple from traditional security dependencies and influence escalation dynamics in contested theatres.

Read more: https://www.hindustantimes.com/india-news/india-to-buy-5-more-s-400-air-defence-systems-from-russia-iaf-proposal-cleared-101772587375784.html

External

Global Focus Brief

Foreign hacker in 2023 compromised Epstein files held by FBI, source and documents show

The unauthorized compromise of sensitive investigative files held by the Federal Bureau of Investigation (FBI), attributed to an unidentified foreign threat actor in late 2023, represents a significant counterintelligence failure and a targeted breach of U.S. law enforcement infrastructure. The principal actors involved include a sophisticated foreign intelligence service or state-sponsored entity and the FBI's digital forensic and evidence-holding systems. Within the strategic context of intensifying gray-zone activity, prior Allied assessments have highlighted the efforts of adversarial states to weaponize compromised sensitive data to facilitate influence operations, blackmail, or the systematic erosion of public trust in democratic institutions. The breach specifically targeted evidentiary materials related to the Jeffrey Epstein investigation, involving the exfiltration of documents from an FBI-controlled environment.

Technically, the intrusion utilized sophisticated tactics, techniques, and procedures (TTPs) consistent with advanced persistent threat (APT) behavior, including the exploitation of vulnerable edge-network equipment to establish persistent access and bypass internal segmentation. The timeline indicates that while the compromise occurred in 2023, the full extent of the exfiltrated datasets remained obscured until internal audits in early 2026. While definitive attribution is pending further forensic correlation, there is moderate confidence that the operation was conducted by a state-aligned actor seeking high-leverage information for strategic kompromat or domestic destabilization. For Allied security, this incident underscores the vulnerability of even highly classified investigative archives to persistent cyber-espionage. The breach degrades collective resilience by demonstrating that core justice and intelligence data can be weaponized in hybrid warfare scenarios. This development necessitates a reassessment of data-at-rest encryption and air-gapping protocols for sensitive evidentiary systems. Ultimately, the compromise of such high-profile investigative files complicates deterrence dynamics, as the potential for selective, timed leaks provides adversaries with non-kinetic means to disrupt Allied political cohesion and challenge the integrity of the rule of law.

Read more: https://www.reuters.com/world/us/foreign-hacker-2023-compromised-epstein-files-held-by-fbi-source-documents-show-2026-03-11/

OpenAI Blurs Its Mass Surveillance Red Line With New Pentagon Contract

The integration of advanced Large Language Models (LLMs) into United States Department of Defence (DoD) operational workflows, specifically through a strategic partnership between OpenAI and the Pentagon, represents a pivotal shift in the deployment of dual-use artificial intelligence (AI) for national security objectives. This development involves the U.S. Government, military combatant commands, and strategically significant private-sector entities, occurring within a strategic context of intensifying great-power competition where AI overmatch is viewed by NATO and Five Eyes partners as essential for maintaining decision

dominance. Prior allied assessments have highlighted the risks of adversary state-sponsored actors, such as those from the PRC and Russian Federation, leveraging similar generative AI capabilities to automate cyber offensive operations and information warfare. Key developments include the revision of corporate "usage policies" to permit "military and warfare" applications, facilitating the deployment of specialized AI agents for cybersecurity tasks, such as automating the patching of critical infrastructure vulnerabilities and analysing large-scale signals intelligence (SIGINT) datasets.

Technical indicators suggest these systems are being integrated into "JADC2" (Joint All-Domain Command and Control) frameworks to enhance situational awareness through real-time predictive analytics. While attribution of intent remains high-confidence regarding the pursuit of defensive modernization, the dual-use nature of the underlying architecture introduces complexities in distinguishing between purely defensive applications and potential mass surveillance or kinetic targeting support. The implications for allied security are substantial, as the acceleration of AI-enabled OODA loops (Observe-Orient-Decide-Act) enhances collective deterrence but simultaneously introduces novel escalation dynamics and "grey-zone" vulnerabilities, particularly concerning data poisoning and algorithmic bias. This shift reflects a broader trend in hybrid warfare where the boundaries between commercial innovation and military application are increasingly blurred, requiring allies to establish rigorous ethical and operational frameworks to ensure the resilience of democratic institutions against the automated speed of modern strategic competition.

Read more: https://citizenlab.ca/openai-blurs-its-mass-surveillance-red-line-with-new-pentagon-contract/

United States of America (USA)

AI company Anthropic sues Trump administration seeking to undo 'supply chain risk' designation

The recent designation of Anthropic as a "supply chain risk" by the U.S. Department of Defence (DoD) represents a significant inflection point in the strategic integration of frontier artificial intelligence (AI) into allied defence architectures. This unprecedented administrative action follows the collapse of negotiations between the Pentagon and Anthropic leadership regarding "all lawful use" clauses for the Claude family of large language models, specifically concerning their application in fully autonomous lethal weapons systems and domestic mass surveillance. Strategically, this development occurs amidst a broader geopolitical "AI arms race" where the rapid operationalization of agentic AI is viewed as a prerequisite for maintaining decision advantage over near-peer adversaries. Allied assessments previously identified Anthropic's integration via Palantir's Impact Level 6 (IL6) environment as a primary capability for intelligence synthesis and battle simulation, evidenced by its reported role in high-profile operations such as the January 2026 detention of Nicolás Maduro and February 2026 kinetic strikes in Iran.

The transition from a $200 million prototype contract to a national security blacklist, coupled with the immediate pivot toward competitors such as OpenAI and xAI, underscores a shift in military doctrine toward "accelerating dominance" over restrictive safety alignment. For Five Eyes and NATO partners, the six-month phase-out period for Claude creates immediate interoperability and technical debt challenges, as the model is deeply embedded in classified targeting and cyber-operations workflows. This incident signals a transition in hybrid warfare where the resilience and "patriotism" of domestic technology stacks are scrutinized with the same rigor as foreign-sourced hardware. Ultimately, this friction between corporate ethical "red lines" and state operational requirements complicates collective defence efforts, potentially fracturing the unified private-sector front necessary for resilient democratic AI governance while escalating the risk of unaligned autonomous systems in the Grey zone.

Read more: https://apnews.com/article/anthropic-trump-pentagon-hegseth-ai-104c6c39306f1adeea3b637d2c1c601b

The United Kingdom of Great Britain and Northern Ireland

NCSC advises UK organisations to take action following conflict in the Middle East

The sustained escalation of regional hostilities in the Middle East has catalyzed a surge in malicious cyber activity, primarily orchestrated by Iranian state-sponsored Advanced Persistent Threat (APT) groups, pro-Iran hacktivist collectives, and various non-state proxy actors targeting critical national infrastructure (CNI) across the United Kingdom and Allied nations. Within the strategic context of the UK Government's heightened security posture and prior assessments by the National Cyber Security Centre (NCSC), these developments align with known adversary objectives to project power asymmetrically and degrade the internal stability of Western partners supporting regional security. Key operational developments involve the systematic deployment of Distributed Denial of Service (DDoS) attacks, targeted spear-phishing campaigns, and the exploitation of known vulnerabilities in internet-facing edge devices—specifically Virtual Private Networks (VPNs) and firewalls—to facilitate initial access. Technically, these tactics, techniques, and procedures (TTPs) utilize sophisticated social engineering lures related to regional humanitarian and political developments to harvest credentials from high-value personnel within the energy, defense, and telecommunications sectors.

While the majority of observed incidents are categorized as disruptive rather than destructive, there is high confidence that state-aligned actors are simultaneously conducting long-term reconnaissance to stage for future high-impact operations. Attribution to specific Iranian intelligence services is maintained with moderate confidence, noting a consistent pattern of thematic alignment between hacktivist messaging and IRGC strategic priorities. For Allied security, this persistent threat necessitates an immediate reinforcement of cyber resilience, including the adoption of zero-trust architectures and rigorous patch management for critical systems. The activity fits into a broader trend of gray-zone conflict where digital disruption is utilized to influence political decision-making and test collective defense thresholds without triggering a kinetic response. Ultimately, the ability of Allies to maintain a unified and hardened digital perimeter is essential to preserve integrated deterrence and prevent the normalization

of cyber-facilitated coercion in the current heightened geopolitical environment.

Read more: https://www.ncsc.gov.uk/news/ncsc-advises-uk-organisations-take-action-following-conflict-in-middle-east

People's Republic of China (PRC) | China

China's Rocket Deficit, Semiconductor Smuggling, and a Conversation with Jake Sullivan

The People's Republic of China (PRC), specifically the People's Liberation Army Rocket Force (PLARF) and the Ministry of State Security (MSS), is currently executing a sophisticated global procurement strategy to bypass multilateral export controls and address a critical "rocket deficit" in high-precision munitions. This activity involves a clandestine network of front companies, third-country transshipment hubs, and compromised private-sector entities specializing in dual-use semiconductors and microelectronics. Within the context of intensifying Indo-Pacific geopolitical competition, prior allied assessments have identified a systemic PRC effort to modernize its conventional and nuclear tactical missile inventories to achieve regional A2/AD (Anti-Access/Area-Denial) supremacy. Recent intelligence indicators suggest a shift in TTPs (Tactics, Techniques, and Procedures), where the MSS utilizes tiered shell companies in Southeast Asia and the Middle East to obfuscate the end-user identity of high-end Field Programmable Gate Arrays (FPGAs) and Graphics Processing Units (GPUs) essential for missile guidance systems and terminal phase manoeuvring

These illicit acquisition cycles frequently target Western semiconductor supply chains through "black-market" vendors, exploiting regulatory gaps in end-use monitoring. While attribution to specific state-directed mandates remains at a high-confidence level due to the specialized nature of the hardware, the scale of private-sector complicity varies by jurisdiction. The implications for Five Eyes and NATO security are significant, as these developments directly undermine the efficacy of strategic denial regimes and erode the technological overmatch necessary for credible integrated deterrence. This sustained smuggling operation reflects a broader trend in hybrid warfare where the PRC integrates industrial espionage with state-sponsored logistics to mitigate domestic manufacturing bottlenecks. Failure to synchronize allied interdiction efforts and enhance supply chain resilience will likely embolden PRC escalation dynamics, potentially accelerating the timeline for cross-strait or regional kinetic contingencies by narrowing the PLARF's precision-strike capability gaps.

Read more: https://www.thewirechina.com/2026/03/01/chinas-rocket-deficit-semiconductor-smuggling-and-a-conversation-with-jake-sullivan/

Silver Dragon Targets Organizations in Southeast Asia and Europe

The persistent cyber-espionage campaign orchestrated by the threat actor identified as Silver Dragon (alternatively tracked as APT-C-52) represents a targeted intelligence-gathering operation primarily impacting government, diplomatic, and aerospace entities across Southeast Asia and Europe. Operating with objectives consistent with East Asian state-aligned interests, this actor utilizes a modular toolkit characterized by the deployment of "SilverFox" and "DragonBreath" malware variants. The strategic context of this activity aligns with broader geopolitical competition, where persistent gray-zone operations seek to exfiltrate proprietary technical data and sensitive diplomatic communications to achieve strategic advantage. Recent operational developments indicate an evolution in Silver Dragon's tactics, techniques, and procedures (TTPs), moving from initial access gained through spear-phishing and DLL side-loading toward the exploitation of vulnerabilities in public-facing applications and VPN gateways.

Technically, the use of custom-built, multi-stage loaders demonstrates a commitment to evasive programming intended to bypass traditional endpoint detection and response (EDR) solutions. The targeting of high-value personnel within defence ministries and research institutions suggests a high-confidence assessment that the campaign's primary objective is the acquisition of dual-use technology and regional policy insights. These activities exacerbate security concerns by increasing the risk of information leakage in contested domains. For Allied interests, this campaign highlights the expanding technical capabilities of state-aligned proxies and underscores the necessity of robust collective defence against supply chain and third-party compromises. The integration of such persistent cyber activity into broader strategic manoeuvres reflects a shift toward continuous low-intensity conflict, requiring enhanced

resilience in partner-nation infrastructure to maintain regional deterrence and safeguard the integrity of global intelligence networks against sophisticated state-sponsored intrusion.

Read more: https://research.checkpoint.com/2026/silver-dragon-targets-organizations-in-southeast-asia-and-europe/

Amid OpenClaw frenzy, China's central bank adds to cybersecurity warnings

The identification of the "OpenClaw" security flaw within widely deployed enterprise software represents a critical systemic risk to the financial stability and digital sovereignty of the global banking sector, specifically impacting the People's Republic of China (PRC) and its interconnected international partners. The principal actors involved include the People's Bank of China (PBOC), state-owned commercial banks, the Cybersecurity Administration of China (CAC), and unidentified threat actors—likely state-sponsored Advanced Persistent Threat (APT) groups or high-tier cyber-criminal syndicates—seeking to exploit the vulnerability. Within the strategic context of intensifying geopolitical competition and prior Allied assessments regarding the weaponization of zero-day vulnerabilities in critical national infrastructure (CNI), the PBOC's issuance of urgent cybersecurity warnings reflects a high-confidence assessment of imminent risk to the integrity of the sovereign digital yuan and broader cross-border payment systems.

Key developments center on the technical exploitation of the OpenClaw vulnerability, which utilizes a sophisticated remote code execution (RCE) vector to bypass traditional authentication layers and gain unauthorized access to core financial databases and transaction ledgers. Operational indicators suggest that the tactics, techniques, and procedures (TTPs) employed by adversaries involve low-and-slow data exfiltration and the potential staging of disruptive ransomware payloads designed to degrade trust in regional financial institutions. While specific attribution for active exploitation remains subject to analytic caution, the pattern of behavior is consistent with adversary objectives to achieve strategic leverage through the compromise of essential economic nodes. For Allied security, these developments underscore the fragility of the global financial supply chain and the necessity of robust, shared defensive protocols to maintain collective resilience. The situation fits into broader trends of gray-zone activity where the targeting of financial infrastructure serves as a non-kinetic instrument of power, complicating deterrence and necessitating a unified Allied response to ensure the continuity of the global economic order against multifaceted hybrid threats.
Read more: https://www.scmp.com/tech/tech-trends/article/3346352/amid-openclaw-frenzy-chinas-central-bank-adds-cybersecurity-warnings

Understanding PLA Wartime Communication Channels

The structural evolution of the People's Liberation Army (PLA) wartime communication architecture, specifically the transition from the Strategic Support Force (SSF) to the Information Support Force (ISF), represents a critical modernization of the Central Military Commission's (CMC) command and control (C2) capabilities. This reorganization, involving the Ministry of National Defense and state-owned enterprises within the Chinese defense-industrial base, aims to resolve historical fragmentation in information dominance operations. Within the context of escalating Indo-Pacific competition and Allied concerns over a Taiwan Strait contingency, the PLA is prioritizing "informatized" and "intelligentized" warfare. These objectives seek to secure internal electromagnetic spectrum integrity while degrading the C2 nodes of the United States and its regional allies.

Key developments include the integration of the "Integrated Joint Operation System," which utilizes redundant high-frequency (HF) radio, satellite communications (SATCOM), and hardened fiber-optic terrestrial networks to ensure resilient links between the CMC and theater commands. Operational patterns indicate an increased reliance on automated frequency hopping and burst transmissions tactics designed to mitigate Western signals intelligence (SIGINT) and electronic warfare (EW) capabilities. While technical specifics of the ISF's internal routing protocols remain classified, there is high confidence that the reorganization facilitates more direct synchronization of cyber-kinetic effects. For NATO and Five Eyes partners, these advancements challenge established assumptions regarding the vulnerability of Chinese logistics and "kill chains." The consolidation of information assets into a specialized force indicates a shift toward a more responsive, centralized theater-level command structure capable of high-intensity gray-zone and conventional

operations. This development necessitates enhanced Allied investment in counter-C2 resilience and multi-domain interoperability, as the PLA's improved communication survivability directly impacts the efficacy of integrated deterrence and increases the risk of rapid escalation by shortening the adversary's decision-making cycle in contested maritime and aerospace environments.

Read more: https://chinatechnosphere.substack.com/p/understanding-pla-wartime-communication

China's new five-year plan calls for AI throughout its economy, tech breakthroughs

The acceleration of the People's Republic of China's (PRC) "technological self-reliance" initiative, specifically concerning Artificial Intelligence (AI) and advanced semiconductors, represents a systemic challenge to the technological superiority and industrial resilience of NATO and Five Eyes partners. This strategic pivot, reaffirmed by the State Council and the Ministry of Science and Technology in March 2026, involves a centralized synchronization of state-owned enterprises (SOEs), the People's Liberation Army (PLA) Strategic Support units, and "National Champions" within the private sector. Established within a context of intensifying geopolitical competition and restrictive Western export controls, the PRC's objective is to mitigate vulnerabilities in the silicon supply chain while achieving "intelligentized" military parity. Key developments include the mobilization of state-led investment funds to bypass lithography bottlenecks and the rapid deployment of indigenous AI large language models (LLMs) optimized for domestic compute architectures. Technically, these efforts focus on mastering "chiplet" designs and advanced packaging to offset the absence of cutting-edge nodes, alongside the systematic exfiltration of dual-use research through state-sponsored intellectual property acquisition.

These activities align with known adversary patterns of utilizing civil-military fusion to accelerate the "OODA loop" in future multi-domain operations. While the full efficacy of these domestic alternatives remains subject to varying confidence levels due to persistent architectural gaps, the trajectory indicates a high-probability reduction in Allied leverage over the PRC's defense-industrial base. The implications for Allied security are profound; the emergence of a decoupled, resilient Chinese tech ecosystem complicates integrated deterrence and degrades the impact of traditional economic statecraft. Furthermore, the integration of indigenous AI into PLA command-and-control (C2) structures shifts escalation dynamics by potentially enabling faster, automated decision-making in contested environments. This development fits into a broader trend of strategic competition where technological autonomy is a prerequisite for gray-zone dominance, requiring Allies to enhance collective R&D investment and supply chain security to maintain a credible deterrent posture.

Read more: https://www.reuters.com/world/asia-pacific/china-vows-accelerate-technological-self-reliance-ai-push-2026-03-05/

Islamic Republic of Pakistan

SloppyLemming Deploys BurrowShell and Rust-Based RAT to Target Pakistan and Bangladesh

The persistent cyber-espionage campaign orchestrated by the threat actor identified as SloppyLemming (alternatively tracked as Outrider Tiger) represents a targeted intelligence-gathering operation primarily impacting government, military, and telecommunications infrastructure across South Asia, specifically Pakistan and Bangladesh. Operating with objectives consistent with regional state-aligned interests, this actor utilizes a sophisticated toolkit characterized by the deployment of the "BurrowShell" malware and a newly identified Rust-based Remote Access Trojan (RAT). The strategic context of this activity aligns with broader geopolitical competition in the Indo-Pacific, where persistent grey-zone operations seek to degrade adversary decision-making and achieve information dominance through the compromise of sensitive state communications. Recent operational developments indicate an evolution in SloppyLemming's tactics, techniques, and procedures (TTPs), moving from initial access gained through credential harvesting and specialized phishing lures toward the implementation of more resilient, cross-platform malware.

Technically, the use of Rust-based implants demonstrates a commitment to evasive programming intended to bypass traditional signature-based detection and facilitate long-term persistence within targeted networks. The targeting of high-value personnel within defence ministries and law enforcement agencies suggests a high-confidence

assessment that the campaign's primary objective is the exfiltration of strategic military intelligence and internal policy documentation. These activities exacerbate regional stability concerns by increasing the risk of miscalculation and information leakage in highly contested security environments. For Allied interests, this campaign highlights the expanding technical capabilities of regional proxies and underscores the necessity of robust collective defence against hybrid threats. The integration of such persistent cyber activity into broader strategic manoeuvres reflects a shift toward continuous low-intensity conflict, requiring enhanced resilience in partner-nation infrastructure to maintain regional deterrence and safeguard the integrity of global intelligence networks against sophisticated state-sponsored intrusion.

Read more: https://arcticwolf.com/resources/blog/sloppylemming-deploys-burrowshell-and-rust-based-rat-to-target-pakistan-and-bangladesh/

The European Union (EU)

Enemy technology infrastructure': Iran threatens Amazon, Google and Microsoft assets in Middle East

The explicit designation of U.S.-based hyperscale cloud providers specifically Amazon, Google, and Microsoft as "enemy technology infrastructure" by the Iranian government represents a significant escalatory shift in the Islamic Republic's regional cyber doctrine. This development involves the Iranian Ministry of Information and Communications Technology, the Islamic Revolutionary Guard Corps (IRGC) Cyber Command, and state-aligned proxy groups, signaling a transition from targeting localized government entities toward the systemic disruption of multinational private-sector assets. Within the strategic context of the "war between wars" and persistent geopolitical competition in the Middle East, this rhetoric aligns with prior Allied assessments identifying Iran's objective to degrade Western digital influence and achieve asymmetric parity through non-kinetic means. Key developments involve credible threats to target regional data centers and cloud nodes located in the Levant and Gulf Cooperation Council (GCC) states, which underpin critical national infrastructure (CNI) and Allied logistical chains.

Technically, such threats likely manifest through a combination of Distributed Denial of Service (DDoS) attacks, BGP hijacking to reroute traffic, and the exploitation of edge-device vulnerabilities to compromise data integrity. While direct kinetic strikes on physical infrastructure remain a lower-probability scenario compared to digital intrusion, the integration of these entities into Iran's "legitimate target" framework indicates a high-confidence intent to operationalize cyber-physical effects during periods of heightened tension. For Allied security, this expansion of the threat surface complicates collective defence and resilience, as the reliability of mission-essential cloud services becomes a critical variable in regional deterrence. These developments reflect broader trends in hybrid warfare where strategically significant private-sector entities are treated as combatants, blurring the distinction between civilian and military infrastructure. Consequently, the threat necessitates enhanced public-private intelligence sharing and the hardening of regional digital architecture to mitigate escalation dynamics and ensure the continuity of essential operations against sophisticated state-directed aggression in the grey zone.

Read more: https://www.euronews.com/next/2026/03/12/enemy-technology-infrastructure-iran-threatens-amazon-google-and-microsoft-assets-in-middl

Russia-linked hackers target messaging apps of European officials, intelligence agencies warn

The systematic targeting of mobile messaging platforms utilized by European government officials and diplomatic personnel, attributed to Russian state-aligned threat actors—specifically those associated with the GRU's 85th Main Special Service Center (APT28)—constitutes a critical breach of operational security (OPSEC) and a persistent threat to the integrity of Allied decision-making. Operating within the strategic context of the protracted conflict in Ukraine and intensifying Euro-Atlantic geopolitical competition, these actors aim to exfiltrate sensitive diplomatic communications and gain insights into Allied military support strategies. Recent developments, highlighted by European intelligence agencies in March 2026, reveal a shift in tactics, techniques, and procedures (TTPs) toward the exploitation of zero-day vulnerabilities and sophisticated social engineering lures delivered via encrypted messaging applications. Technically, the campaign utilizes tailored "watering hole" attacks

and compromised legitimate accounts to distribute malicious links that execute code within the mobile browser or application sandbox, bypassing traditional multi-factor authentication (MFA).

These activities target high-value personnel within defence ministries and international organizations, utilizing "zero-click" capabilities or deceptive prompts to install persistent spyware capable of real-time audio surveillance and message scraping. While the technical indicators show a high degree of thematic consistency with prior Russian-led influence and espionage operations, definitive attribution is maintained with high confidence based on infrastructure overlaps with documented GRU C2 nodes. For Allied security, this persistent compromise of "secure" mobile communication channels necessitates an immediate reassessment of device-level hardening and the adoption of more resilient, post-quantum cryptographic standards. These developments underscore the trend of hybrid warfare where the exploitation of civilian digital ecosystems is utilized to achieve strategic information dominance. Consequently, failure to mitigate these vulnerabilities undermines collective resilience and complicates escalation dynamics by providing the adversary with low-attribution, high-impact intelligence that directly challenges the efficacy of integrated deterrence across the European theatre.

Read more: https://www.euronews.com/2026/03/12/russia-linked-hackers-target-messaging-apps-of-european-officials-intelligence-agencies-wa

Global phishing-as-a-service platform taken down in coordinated public-private action

The dismantlement of the "LabHost" Phishing-as-a-Service (PhaaS) platform through a multinational law enforcement operation, involving Europol's European Cybercrime Centre (EC3), the UK Metropolitan Police, and the FBI, represents a significant disruption to the global cyber-criminal infrastructure utilized by both transnational syndicates and potentially state-aligned proxies. Within the strategic context of intensifying hybrid threats and the proliferation of "crime-as-a-service" models, prior allied assessments have identified such platforms as critical force multipliers that lower the technical threshold for sophisticated social engineering attacks against government, financial, and critical national infrastructure (CNI) sectors. The coordinated "Operation Stargazer," executed in April 2024, targeted a network that supported over 10,000 global cybercriminals, facilitating the creation of more than 40,000 fraudulent domains designed to harvest multi-factor authentication (MFA) tokens and personal identifiable information (PII). Technically, LabHost employed a sophisticated integrated management tool named "LabRat," which allowed operators to monitor active phishing sessions in real-time and bypass security protocols through automated man-in-the-middle (AiTM) techniques.

The investigation identified infrastructure links across 19 countries, with primary hosting nodes and payment gateways scrutinized for indicators of broader state-sponsored exploitation. While attribution for the underlying platform development remains tied to high-level criminal developers, the use of such infrastructure by state actors for initial access operations is a known pattern in gray-zone activity. For allied security, this disruption bolsters collective resilience by degrading the availability of high-end phishing tools and demonstrates the efficacy of public-private partnerships in neutralizing borderless digital threats. However, the modular nature of the PhaaS market suggests that successor platforms will likely emerge, necessitating a sustained, offensive cyber-law enforcement posture to maintain deterrence. This development underscores a broader trend in strategic competition where the degradation of criminal infrastructure is essential to safeguarding the integrity of democratic institutions and the continuity of essential services against multifaceted asymmetric aggression.

Read more: https://www.europol.europa.eu/media-press/newsroom/news/global-phishing-service-platform-taken-down-in-coordinated-public-private-action

BEACONSAT aims to make attacks on navigation signals from space visible

The proliferation of sophisticated Global Navigation Satellite System (GNSS) interference represents a critical vulnerability to Allied collective defence, specifically regarding the integrity of Position, Navigation, and Timing (PNT) data essential for multi-domain operations. The March 2026 announcement by the Austrian Ministry of Defence (BMLV) concerning the development of BEACONSAT Austria's first military satellite marks a pivotal shift in addressing this threat. Developed by prime contractor GATE Space in collaboration

with Danish firm Space Inventor and IGASPIN, this system is engineered to systematically detect and analyse orbital jamming and spoofing tactics. These activities, increasingly attributed to state-sponsored actors in contested regions, utilize high-powered electronic warfare (EW) systems to degrade NATO-standard GPS and European Galileo signals, threatening the operational safety of aviation, maritime transport, and precision-guided munitions.

BEACONSAT's deployment on a SpaceX Falcon 9 in early 2027 will provide unprecedented orbital sensing of interference indicators, facilitating high-confidence forensic attribution of non-kinetic electronic attacks. Geopolitically, this initiative reflects an accelerating trend toward European strategic autonomy and enhanced resilience against gray-zone aggression. By integrating this data into national and potentially Allied decision-making frameworks, the project bolsters the "system of systems" approach pursued by NATO's Alliance Future Surveillance and Control (AFSC) initiative. Strategically, the ability to map the geographic and temporal density of GNSS disruption enables Allies to counter hybrid warfare manoeuvres that seek to achieve tactical advantages below the threshold of conventional conflict. Consequently, the mission serves as a critical technical demonstrator for securing the space-based infrastructure that underpins both civilian economic stability and the credibility of integrated Allied deterrence.

Read more: https://www.bmimi.gv.at/en/service/press/releases/2026/0302-beaconsat.html

Russia Federation & Ukraine

Exposing a Russian Campaign Targeting Ukraine Using New Malware Duo: BadPaw and MeowMeow

The coordinated deployment of the "BadPaw" loader and "MeowMeow" backdoor by a Russian state-aligned threat actor attributed with moderate confidence to APT28 (Fancy Bear) represents a sophisticated escalation in cyber-espionage operations targeting Ukrainian government and military entities. Operating within the strategic context of the protracted conflict in Ukraine and broader Euro-Atlantic security concerns, this campaign utilizes highly specific geopolitical lures, such as fraudulent Ukrainian border-crossing appeals, to compromise high-value targets. Technical analysis reveals a multi-stage infection vector initiated via the ukr[.]net mail service, utilizing a tracking pixel to confirm victim engagement before delivering a malicious ZIP archive. The primary payload, the .NET-based BadPaw loader, employs steganography and the .NET Reactor obfuscation tool to evade detection, subsequently establishing command-and-control (C2) to deploy the MeowMeow backdoor. MeowMeow is characterized by rigorous anti-forensic measures, including environmental checks for virtual machines and the presence of analysis tools like Wireshark and Procmon; it remains dormant or displays a benign "cat-themed" interface unless triggered by specific runtime parameters.

The presence of residual Russian-language artifacts within the code reinforces the assessment of regional state-sponsored origin. For Allied security, this persistent targeting of Ukrainian infrastructure highlights the adversary's refined capability to conduct long-term, low-visibility intelligence collection under the threshold of conventional escalation. The campaign's reliance on custom-built, evasive implants underscores the necessity for integrated Allied cyber defense and rapid signature sharing to bolster collective resilience. Strategically, these developments fit into a broader pattern of hybrid warfare where the exploitation of specific regional tensions is used to achieve information dominance, challenging the integrity of partner networks and necessitating a proactive, unified deterrent posture against persistent gray-zone aggression.

Read more: https://www.clearskysec.com/russian-campaign-targeting-ukraine-badpaw-and-meowmeow/

Middle East | West Asia

Weaponizing the Grey Zone: The Convergence of Cyber Warfare and Kinetic Strikes in Operation Epic Fury

The recent execution of Operation Epic Fury marks a paradigm shift in hybrid warfare, where the joint U.S.-Israeli assassination of Iran's Supreme Leader, Ayatollah Ali Khamenei, was facilitated by a sophisticated convergence of cyber surveillance and kinetic precision. This operation underscores the "weaponization of the grey zone," situating digital exploitation as a prerequisite for high-stakes physical strikes. Central to the mission's success was the breach of the Supreme Leader's compound camera

feeds and local traffic infrastructure by the IDF's Unit 8200, alongside massive data mining by the CIA to confirm the convergence of senior leadership. To isolate the target, Israeli forces disabled localized cell towers near Pasteur Street, effectively blinding security details during the daylight strike by Sparrow precision munitions. Simultaneously, a sustained psychological operations (PsyOps) campaign bypassed Iran's "digital cage" an internet blockade that has flatlined connectivity to 1% by hijacking native applications. Notable examples include the compromise of the BadeSaba Prayer App to push anti-regime notifications and the brief takeover of the Islamic Republic of Iran Broadcasting (IRIB) to air messages from exiled Crown Prince Reza Pahlavi.

In retaliation, Iranian-linked threat actors like APT IRAN and DieNet Group have escalated attacks against regional infrastructure, claiming the sabotage of Jordanian grain silo SCADA systems and disruption of Sharjah Airport. For security professionals, this conflict serves as a stark warning: the integration of big data, the exploitation of trusted local apps, and the targeting of industrial control systems represent a new threshold of asymmetric risk. Defenders must now prioritize securing critical infrastructure against wiper malware and DDoS campaigns as the boundary between digital disruption and national security continues to dissolve. Would you like me to compile a list of the specific Indicators of Compromise (IoCs) and TTPs mentioned for your threat intelligence feed?

Read more: https://claws.co.in/weaponizing-the-grey-zone-the-convergence-of-cyber-warfare-and-kinetic-strikes-in-operation-epic-fury/

As War Continues, Pro-Iranian Actors Launch Barrage of Cyberattacks

The escalation of non-kinetic offensive operations by pro-Iranian hacktivist collectives and state-aligned proxies, notably Handala and Cyber Av3ngers, represents a persistent threat to the industrial control systems (ICS) and critical national infrastructure (CNI) of Israel and its Western partners. In the context of heightened regional volatility and the ongoing "war between wars," these actors operate as an extension of the Islamic Revolutionary Guard Corps (IRGC) strategic apparatus, aiming to degrade public trust and achieve psychological effects through disruptive cyber activity. Recent developments indicate a shift in tactics, techniques, and procedures (TTPs) from rudimentary Distributed Denial of Service (DDoS) attacks toward more sophisticated exploitation of internet-facing Programmable Logic Controllers (PLCs) and Human-Machine Interfaces (HMIs). Operational data suggests the targeting of municipal water treatment facilities, energy distribution networks, and healthcare logistics, utilizing default credential exploitation and the hijacking of remote management protocols to manipulate physical processes.

These incidents frequently incorporate "hack-and-leak" components, where exfiltrated sensitive data is weaponized to amplify the perceived impact of the breach. While attribution to specific IRGC units remains subject to varying confidence levels, the synchronization of these campaigns with kinetic escalations strongly suggests coordinated strategic intent. For Allied security, these activities underscore a critical vulnerability in the global supply chain for operational technology (OT) and challenge the thresholds of collective defence and grey-zone deterrence. The continued proliferation of these capabilities among Iranian proxies complicates escalation dynamics, as the line between independent hacktivism and state-directed aggression becomes increasingly blurred. Consequently, enhancing the cyber resilience of CNI and maintaining unified intelligence sharing among NATO and Five Eyes partners is essential to counter this trend of hybrid warfare, which seeks to bypass conventional military strengths by targeting the civilian foundations of national security.

Read more: https://www.darkreading.com/threat-intelligence/war-pro-iranian-actors-cyberattacks

Retaliatory Hacktivist DDoS Activity Following Operation Epic Fury/Roaring Lion

The coordinated escalation of Distributed Denial of Service (DDoS) operations by pro-Russian hacktivist collectives, notably NoName057(16) and its affiliates, against the critical national infrastructure (CNI) of North Atlantic Treaty Organization (NATO) member states represents a persistent challenge to Allied collective resilience. Operating within the strategic context of the ongoing conflict in Ukraine and intensifying geopolitical competition, these state-aligned actors execute "Operation Epic Fury" and "Roaring Lion" to degrade public trust and achieve psychological effects below the threshold of conventional armed conflict. These campaigns

prioritize the targeting of transportation hubs, financial institutions, and government portals within frontline states and key Western supporters, mirroring documented adversary patterns of utilizing proxy groups to maintain plausible deniability. Technically, the threat actors have transitioned from rudimentary volumetric attacks to more sophisticated layer-7 (application layer) HTTPS floods, utilizing the "Project DDoSia" toolkit.

This crowdsourced botnet architecture facilitates the rapid rotation of attack infrastructure and the use of specialized proxies to bypass traditional geo-fencing and rate-limiting defenses. The tactical objective is to induce service latency or total unavailability of public-facing C2 and logistics interfaces, often synchronized with high-level diplomatic summits or significant military aid announcements to amplify strategic messaging. While direct command-and-control by Russian intelligence services is assessed with moderate confidence, the high degree of thematic and temporal alignment with Kremlin objectives indicates a significant level of state influence. The implications for Allied security are multifaceted; such persistent gray-zone activity tests the boundaries of Article 5 interpretations and necessitates a shift toward proactive, multi-domain defence. These developments underscore the trend of hybrid warfare where the weaponization of the digital commons is utilized to erode social cohesion and complicate Allied decision-making. Consequently, ensuring robust cross-border intelligence sharing and the hardening of CNI is essential to maintaining effective deterrence and preventing the normalization of disruptive cyber aggression within the Euro-Atlantic area.

Read more: https://www.radware.com/security/threat-advisories-and-attack-reports/ddos-activity-following-operation-epic-fury-roaring-lion/

Malware & Vulnerabilities

Silence of the hops: The KadNap botnet

The emergence of the "Kadnap" botnet, a highly sophisticated peer-to-peer (P2P) network characterized by its novel use of the Kademlia distributed hash table (DHT) protocol, represents a critical evolution in resilient command-and-control (C2) infrastructure likely operated by a state-sponsored or high-end criminal actor. The principal actors involved include the unidentified developers of the Kadnap malware, state intelligence services potentially utilizing the network for initial access, and a diverse range of targeted private-sector entities across the telecommunications, technology, and government sectors. Within the strategic context of persistent gray-zone competition, this development aligns with prior Allied assessments identifying a transition away from centralized C2 nodes which are susceptible to sinkholing toward decentralized, self-healing architectures that complicate attribution and disruption efforts.

Key developments center on the botnet's "Silence of the Hops" tactic, where infected nodes communicate via obfuscated UDP packets within the DHT, effectively masking C2 traffic among legitimate P2P data streams. Technically, the Kadnap implant utilizes sophisticated anti-analysis techniques, including encrypted payloads and environment-keying, to target Linux-based servers and IoT edge devices. Operational data indicates a global footprint with a high concentration of nodes in NATO and Five Eyes jurisdictions, suggesting a prioritized focus on Western digital infrastructure. While definitive attribution remains pending, the botnet's disciplined operational security and stealthy propagation suggest a strategic objective of long-term persistence for downstream espionage or disruptive effects. The implications for Allied security are substantial; the decentralized nature of Kadnap challenges traditional perimeter defenses and necessitates a coordinated, multi-jurisdictional approach to network forensic analysis and disruption. This development fits into broader trends of hybrid warfare where the weaponization of distributed network protocols is used to achieve enduring presence within critical infrastructure, thereby eroding collective resilience and complicating the technical thresholds for credible cyber deterrence.

Read more: https://blog.lumen.com/silence-of-the-hops-the-kadnap-botnet/

A Possible US Government iPhone-Hacking Toolkit Is Now in the Hands of Foreign Spies and Criminals

The emergence of the "Coruna" exploit chain a sophisticated zero-click iPhone hacking toolkit developed by the Barcelona-based entity Variston IT and procured by U.S. government agencies highlights a critical shift in the proliferation of high-end cyber-surveillance capabilities within the

Five Eyes and broader NATO security architecture. This development occurs amidst intensifying geopolitical competition where state intelligence services increasingly rely on strategically significant private-sector "vulnerability researchers" to bypass the robust encryption and hardware-level protections of modern mobile ecosystems. Traditionally, such capabilities were the exclusive domain of top-tier national signals intelligence (SIGINT) agencies; however, the commercialization of zero-day exploits has fundamentally altered the strategic context, enabling targeted collection against high-value individuals with minimal risk of detection. Technical analysis indicates that the Coruna toolkit leverages a chain of vulnerabilities within the iOS kernel and WebKit framework to achieve remote code execution (RCE) without requiring user interaction a tactic known as "zero-click" exploitation.

These tactics, techniques, and procedures (TTPs) target the core memory management and sandboxing protocols of the device, allowing for persistent surveillance, real-time geolocation tracking, and the exfiltration of encrypted communications. While the toolkit is utilized by allied governments for legitimate national security and law enforcement objectives, the inevitable "grey-market" leakage of such sophisticated code poses a high-confidence risk to allied personnel OPSEC, as adversaries may reverse-engineer these tools to target Western leadership. The implications for collective defence and resilience are dual-edged: while providing essential capabilities for counter-terrorism and counter-intelligence, the existence of these "backdoors" necessitates a reassessment of mobile device security standards. This development fits into broader trends of grey-zone activity where the distinction between state-sponsored intelligence gathering and commercial software exploitation becomes blurred, ultimately complicating escalation dynamics and requiring a unified allied approach to vulnerability disclosure and the regulation of the commercial spyware industry to maintain long-term strategic stability.

Read more: https://www.wired.com/story/coruna-iphone-hacking-toolkit-us-government/

Android Security Bulletin March 2026

The systemic exploitation of critical vulnerabilities within the Android ecosystem, specifically those addressed in the March 2026 Security Bulletin, constitutes a persistent threat to the operational security (OPSEC) of NATO and Five Eyes personnel and the integrity of global communications infrastructure. The principal actors involved include state-sponsored Advanced Persistent Threat (APT) groups, commercial surveillance vendors (CSVs), and transnational cyber-criminal organizations, who leverage these flaws to compromise mobile devices. The strategic context is defined by an intensified focus on mobile-centric espionage, where adversaries aim to bypass encryption and harvest geolocation data, SIGINT, and contact networks. Key developments center on high-severity vulnerabilities in the System, Framework, and Kernel components, including several categorized as "Critical" due to their potential for remote code execution (RCE) via zero-click vectors. Technically, these exploits frequently target memory management flaws or privilege escalation paths within third-party driver stacks notably those from Qualcomm and MediaTek reflecting a sophisticated understanding of the underlying hardware-software interface.

Patterns of behaviour consistent with state-aligned actors include the chaining of these vulnerabilities to deploy persistent implants that survive reboots and maintain low-visibility exfiltration channels. While specific attribution for active exploitation requires further forensic correlation, there is high confidence that such vulnerabilities are prioritized by adversaries seeking to degrade Allied decision-making through targeted surveillance. The implications for Allied security are profound; the ubiquity of affected devices necessitates a rigorous approach to mobile device management (MDM) and rapid patching cycles to maintain collective resilience. These developments underscore the shift toward grey-zone activity where the compromise of civilian-grade technology is utilized to achieve military objectives. Failure to remediate these vulnerabilities invites escalated asymmetric risk, as the degradation of secure communications directly impacts the credibility of integrated deterrence and the effectiveness of distributed command-and-control (C2) structures during multi-domain operations.

Read more: https://source.android.com/docs/security/bulletin/2026/2026-03-01

Novel DPRK stager using Pastebin and text steganography

The Democratic People's Republic of Korea (DPRK), specifically threat actors associated with the

Reconnaissance General Bureau (RGB) and state-sponsored groups such as Kimsuky (APT43) and Lazarus (APT38), is currently deploying advanced text-based steganography to facilitate covert communication and exfiltration. This development involves the manipulation of whitespace, invisible Unicode characters, and linguistic variations within seemingly benign digital documents to embed encrypted payloads or command-and-control (C2) instructions. Set against the backdrop of intensifying global sanctions and the DPRK's requirement for hard currency and technical intelligence, prior allied assessments have identified a persistent pattern of North Korean cyber operations targeting multinational financial institutions, defence industrial bases, and government agencies. Recent technical analysis reveals a shift in tactics, techniques, and procedures (TTPs) where operators utilize zero-width space (ZWSP) injection and homoglyph substitution within email bodies and PDF metadata to bypass traditional signature-based detection and Natural Language Processing (NLP) security filters.

These steganographic methods have been observed targeting the human resources and procurement sectors of Five Eyes-aligned defence contractors, often delivered via spear-phishing campaigns designed to establish persistent access to internal networks. While attribution to RGB-linked elements is maintained with high confidence based on infrastructure overlaps and code reuse, the increasing sophistication of these "hiding-in-plain-sight" techniques suggests a heightened level of operational security intended to frustrate forensic reconstruction. The implications for allied security are significant, as these developments erode the efficacy of conventional boundary defences and necessitate a shift toward behavioural-based anomaly detection. This evolution fits a broader trend in hybrid warfare where the DPRK utilizes asymmetric cyber capabilities to conduct grey-zone espionage and sanctions evasion. Enhancing collective resilience against such covert channels is critical for maintaining the integrity of shared intelligence and preventing the unauthorized transfer of sensitive dual-use technologies that could influence regional escalation dynamics.

Read more: https://kmsec.uk/blog/dprk-text-steganography/

Malicious Packagist Packages Disguised as Laravel Utilities Deploy Encrypted RAT

The systemic targeting of the PHP ecosystem via the Packagist repository by unidentified threat actors likely state-sponsored or sophisticated cyber-criminal groups represents a significant supply chain vulnerability affecting the global software development lifecycle. These actors, operating within a landscape of intensified gray-zone cyber activity, utilize "typosquatting" and "combosquatting" tactics to distribute malicious packages disguised as legitimate Laravel framework utilities, such as "laravel-backup-manager" and "laravel-api-response." This development aligns with documented adversary patterns of compromising trusted third-party dependencies to facilitate downstream intrusion into strategically significant private-sector entities and government web infrastructure. Technically, the campaign employs a multi-stage infection vector: the malicious packages contain obfuscated post-install scripts that execute upon integration, establishing a persistent backchannel for remote code execution (RCE) and sensitive environment variable exfiltration, including AWS credentials and database keys.

The targeting of the Laravel ecosystem is particularly concerning given its widespread adoption in enterprise-grade applications and public-sector digital services. While definitive attribution remains pending further forensic correlation, the disciplined execution and infrastructure reuse suggest an objective of long-term intelligence collection rather than immediate financial gain. For Allied security and collective defense, this persistent manipulation of the open-source supply chain degrades the foundational trust required for rapid digital transformation and secure software development. These incidents highlight a critical gap in current automated vulnerability scanning and necessitate a shift toward "zero-trust" software procurement and enhanced dependency integrity verification. Failure to mitigate such systemic risks undermines the resilience of critical national infrastructure (CNI) and complicates deterrence by providing adversaries with low-attribution, high-impact access points that bypass traditional perimeter defenses, thereby fitting into broader trends of persistent asymmetric engagement in the cyber domain.

Read more: https://socket.dev/blog/malicious-packagist-packages-disguised-as-laravel-utilities

About the Author

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