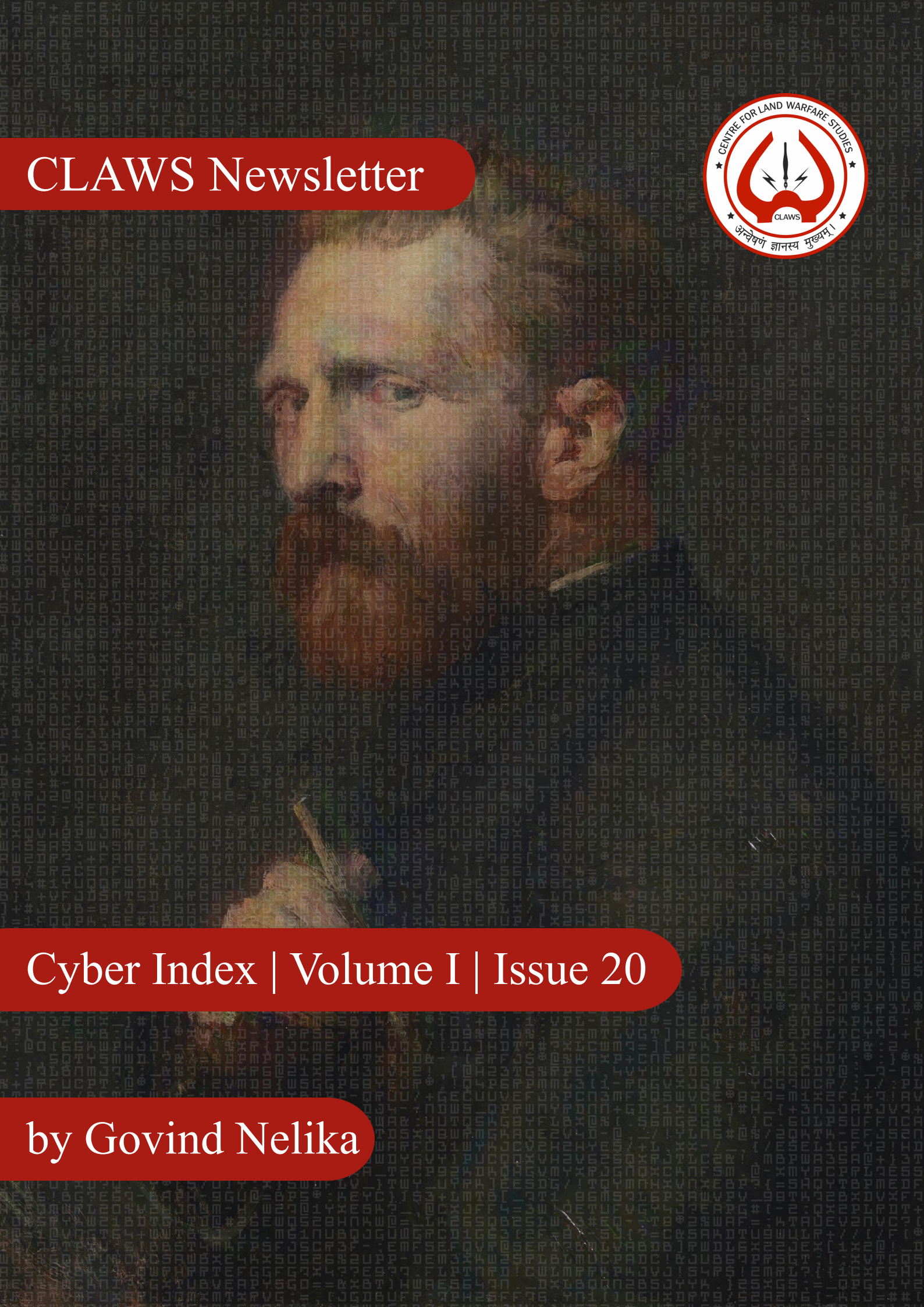
CLAWS Newsletter



Cyber Index | Volume I | Issue 20

by Govind Nelika

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

Global Brief

China's UK Investment Spree Granted Access to Military-Grade Technology

China's recent surge in UK investment, especially by state-linked funds, has allowed Beijing via opaque acquisitions to obtain advanced semiconductor and dual-use technologies with potential military applications. A key example is Imagination Technologies, a UK-based chip-design firm, whose 2017 takeover by Canyon Bridge (backed by China Reform Holdings, tied to the Chinese state) gave Chinese interests access to the company's core intellectual property.

Following the acquisition, former CEO Ron Black alleges he was summoned to Beijing and asked to oversee the transfer of Imagination's design technology and expertise from British engineers to Chinese engineers and to dismiss the UK staff. When he resisted, China Reform reportedly tried to install hand-picked directors lacking semiconductor experience. Black eventually resigned and was later unfairly dismissed by an employment tribunal; soon after, the company's proprietary technology was transferred to China.

At the time of the takeover, the UK lacked robust mechanisms to block foreign acquisitions of sensitive technology firms, reflecting a broader "golden era" of UK–China commercial openness. While the publicly offered justification emphasized commercial motives and adherence to export regulations, security experts contend that the transferred semiconductor architecture and design know-how though developed for civilian electronics can be repurposed for military hardware such as drones, missiles or surveillance systems.

Strategically, this episode reveals a critical vulnerability: liberal foreign-investment policies coupled with inadequate oversight can enable state-backed actors to acquire dual-use technologies with minimal scrutiny. It underscores growing concerns about how economic engagement and global capital flows can serve as surreptitious channels for technology transfer complicating national security efforts and blurring the line between civilian trade and strategic competition.

Read more: https://westminsterpimliconews.co.uk/china-uk-investment-access-to-military-technology/

Singapore picks Alibaba's Qwen to drive regional language model in big win for China tech

AI Singapore (AISG), which has chosen to base its newest regional large-language model on Alibaba Cloud's Qwen architecture a move that represents a major win for the Chinese tech firm in Southeast Asia's AI landscape. Specifically, AISG's newly released model, Qwen-SEA-LION-v4, is built on Alibaba Cloud's Qwen3-32B foundation model, and includes technical enhancements designed to better handle Southeast Asia's linguistic diversity. To tailor the model for regional needs, the base model's broad coverage of 119 languages and dialects (pre-trained on roughly 36 trillion tokens) was supplemented with more than 100 billion Southeast Asian-language tokens, enabling improved understanding of local expressions, mixed-language usage, and culturally specific context.

This shift reflects AISG's decision to abandon its earlier reliance on a model from Meta Platforms part of a larger national AI strategy sponsored by the National Research Foundation, Singapore under a multi-million-dollar program launched in 2023. The SEA-LION-v4 reportedly now ranks first among all open-source models with fewer than 200 billion parameters on the Southeast-Asian Holistic Evaluation of Language Models (SEA-HELM) benchmark, underscoring its strong performance in multilingual reasoning and regional language tasks. Alibaba Cloud further provides "advanced post-training" support, combining the model's technical strengths (e.g., long-context comprehension, multilingual fluency, efficient quantized deployment) with AISG's regional data curation and evaluation capabilities.

Strategically, this collaboration underscores a broader trend: as regional AI adoption grows, the ability to support under-represented languages and cultural contexts becomes a decisive competitive advantage often more important than simply leading in overall scale or raw compute. For Alibaba, SEA-LION-v4 boosts the global footprint of its open-source AI ecosystem; for Singapore and the wider Southeast Asian region, it promises more inclusive, locally relevant AI tools in sectors such as public services, education, commerce, and multilingual communication. More broadly, this development signals how non-Western AI players are increasingly shaping the infrastructure of AI in emerging markets

reshaping global AI competition along linguistic and regional, not just technological, lines.

Read more: https://www.scmp.com/tech/big-tech/article/3334098/singapore-picks-alibabas-qwen-drive-regional-language-model-big-win-china-tech?

Google's DeepMind to set up new AI research lab in Singapore

Google's artificial intelligence research division DeepMind has announced the establishment of a new research lab in Singapore as part of a concerted effort to expand its footprint in the Asia-Pacific region, reflecting both the commercial importance and fast-growing adoption of AI technologies across emerging markets. The expansion involves hiring researchers, engineers, and specialists in AI ethics, safety, and applied machine learning to pursue advanced work on large-scale models and real-world applications spanning areas such as education, healthcare, and scientific discovery, leveraging Singapore's existing status as a hub for technology innovation and supportive policy environment under its national AI strategy. DeepMind leadership, including Chief Operating Officer Lila Ibrahim, has underscored the lab's role in fostering collaboration with local governments, academic institutions and industry partners to address region-specific challenges and ensure that AI capacities are shaped with diverse linguistic, cultural and societal perspectives.

The Singapore facility complements DeepMind's broader global network which already includes research centers in the United Kingdom, the United States, and Canada and is designed to integrate multidisciplinary expertise to advance foundational research while translating breakthroughs into practical tools. By situating the new lab in Southeast Asia, DeepMind aims to tap into a rich talent pool and engage more directly with regional innovation ecosystems, where AI adoption rates in sectors like fintech, urban planning and digital services are among the highest globally. Strategically, this move aligns with wider trends in the global AI landscape, where leading technology firms are increasingly decentralizing research and building capacity outside traditional Western and East Asian centers to stay competitive, navigate geopolitical tensions over technology leadership, and respond to calls for inclusive and ethically governed AI development; it also positions Singapore as a pivotal node in regional AI governance and competitiveness discussions amid growing international focus on balancing innovation, regulation and national security considerations.

Read more: https://deepmind.google/blog/were-expanding-our-presence-in-singapore-to-advance-ai-in-the-asia-pacific-region/

United Kingdom of Great Britain and Northern Ireland

Action to disrupt and deter threats to UK as MI5 issues spy alert

In late November 2025 the United Kingdom government, led by Security Minister Dan Jarvis and informed by its domestic intelligence service MI5, identified and responded to a significant foreign espionage threat directed at the nation's political institutions, centering on alleged activities by Chinese state actors. MI5 issued a rare public warning to Members of Parliament, members of the House of Lords, and parliamentary staff after detecting that individuals believed to be acting on behalf of the Chinese Ministry of State Security were using professional networking platforms such as LinkedIn to pose as legitimate recruiters or "headhunter" profiles to cultivate relationships and recruit people with access to sensitive governmental information.

This activity was characterized by officials in Westminster as a "covert and calculated" bid by China to interfere in UK sovereign affairs and potentially capture insights valuable for strategic advantage, reflecting broader concerns about long-term foreign influence operations against democratic systems. In response, the government announced a Counter Political Interference and Espionage Action Plan to disrupt and deter such threats, which includes enhanced security briefings for political parties and election candidates, tightened political donation rules via a forthcoming Elections Bill, closer cooperation with online platforms to make the digital environment less hospitable to hostile intelligence efforts, and legislative updates to strengthen national security powers under the National Security Act.

Substantial investment was also earmarked for renewing encrypted and sovereign communications technology used by civil servants, reinforcing cyber defence and policing capabilities, and removing foreign-made surveillance equipment from sensitive government sites. The alert and accompanying policy moves come amid an environment of heightened scrutiny of foreign espionage, including

previous cases linked to individuals accused of spying for China, and fit into a larger global trend of Western democracies confronting sophisticated influence and intelligence operations from major state competitors while balancing diplomatic and economic engagement with nations like China.

Read more: https://www.gov.uk/government/news/action-to-disrupt-and-deter-threats-to-uk-as-mi5-issues-spy-alert

United States of America (USA)

The pilot of an F-22 just controlled a drone wingman in flight

The recent demonstration of a F-22 Raptor pilot successfully controlling a MQ-20 Avenger drone in flight marks a major milestone for Lockheed Martin, General Atomics Aeronautical Systems (GA-ASI), and the United States Air Force in the field of crewed-uncrewed teaming. On October 21, 2025, over the Nevada Test and Training Range, the F-22 pilot used a tablet-based "Pilot Vehicle Interface" (PVI) integrated into the jet's cockpit to issue real-time mission commands to the MQ-20 Avenger a first for a fifth-generation fighter relying on autonomous or remotely piloted wingman architecture.

This demonstration employed an open-architecture communications suite combining L3Harris' BANSHEE advanced tactical datalinks and software-defined radios, layered over Lockheed Martin's modular GRACE (Government Reference Architecture Compute Environment) system inside the F-22. Through this setup, the F-22 was able to command the unmanned Avenger to execute a designated mission profile in real time proving that a single-seat fighter jet can serve as a command node for uncrewed assets while airborne.

This event is set against a broader strategic and technological context: as air combat becomes more contested through advanced air-defence systems and electronic warfare, the ability to employ attritable unmanned "wingmen" provides a force-multiplier effect without exposing valuable manned assets. The flight is part of the Air Force's intended Collaborative Combat Aircraft (CCA) program, which aims to field affordable, networked combat drones alongside legacy and future fighters, including the F-35 Lightning II and upcoming sixth-generation jets.

Strategically, this demonstration signals a paradigm shift in air warfare: human-machine teaming is no longer conceptual but operationally feasible. If scaled, such capability could substantially enhance aerial reach, survivability, and mission flexibility, especially in high-threat environments. It also underscores a broader trend in defense strategy favoring distributed, networked systems that combine manned platforms with autonomous drones to maintain air superiority against near-peer adversaries.

Read more: https://www.defenseone.com/technology/2025/11/pilot-f-22-just-controlled-drone-wingman-flight/409586/

Trump's semiconductor tariff plan likely delayed, officials say

In late November 2025, U.S. economic and trade policy under President Donald Trump became the focal point of renewed scrutiny as senior administration officials signalled a likely delay in imposing long-threatened tariffs on semiconductor imports, a key element of Trump's broader trade agenda aimed at rebalancing the U.S. economy and boosting domestic manufacturing. According to unnamed U.S. sources familiar with internal discussions, stakeholders in both government and the private sector have been privately informed that the planned semiconductor tariffs which had been touted for months and even framed as potentially reaching 100 percent on certain chip imports to pressure foreign producers and incentivize reshoring are now unlikely to be levied imminently, reflecting a more cautious approach by the administration. This shift is partly attributed to concerns that implementing steep chip tariffs could provoke retaliatory responses from China, where tensions over trade and technology have already manifested in tariff escalations and export controls on critical materials such as rare earth minerals, as well as fuel inflationary pressures at a politically sensitive time for U.S. consumer prices ahead of the holiday season.

The deliberations come against a backdrop of broader U.S.–China economic friction throughout 2025, which has included tit-for-tat tariff actions, negotiations on rare earth and trade measures, and debates within U.S. corridors of power over maintaining competitive advantage in semiconductors and advanced technologies while avoiding destabilizing supply chain disruptions.

Analysts view the reported delay as significant not only for global semiconductor supply chains where firms like Nvidia, TSMC and Samsung play central roles but also for the strategic calibration of U.S. industrial policy and international trade relations; postponing tariffs may ease immediate geopolitical tensions and protect international market stability, yet it could also complicate long-term objectives around technological sovereignty and competitiveness in a sector deemed critical to national security.

Read more: https://www.reuters.com/world/china/trumps-semiconductor-tariff-plan-likely-delayed-officials-say-2025-11-19/?

People's Republic of China (PRC) | China

Chinese researchers simulate jamming Starlink in Taiwan conflict

The research effort by Chinese academics associated with the Zhejiang University and the Beijing Institute of Technology, aimed at assessing the feasibility of jamming Starlink satellite-internet services in the event of a conflict over Taiwan. According to a peer-reviewed study published November 5, the researchers concluded that effectively disrupting Starlink across an area roughly the size of Taiwan would require deployment of at least 935 small, synchronized airborne jammers carried by drones, balloons, or aircraft and possibly as many as 2,000 if lower-powered devices were used. These jammers would need to operate in concert to blanket the roughly 36,000 km² operational zone with electromagnetic interference; the study noted that traditional ground-based jamming would prove inadequate due to Starlink's extensive low-Earth-orbit architecture and its rapid ability to reroute links when individual satellites are jammed. The researchers also cautioned that their figures are preliminary, given that many of Starlink's core technologies remain classified, and actual requirements could therefore be even higher.

This development must be viewed against the broader context of intensifying cross-strait tensions: in recent years, the People's Liberation Army (PLA)'s Eastern Theater Command has stepped up joint air-naval drills around Taiwan including live-fire exercises and expanded cyber, electronic-warfare, and gray-zone capabilities aimed at coercing the island into unification. Meanwhile, Taiwan and its partners have considered more robust asymmetric defenses, including the proposed T-Dome multilayer air- and missile-defense shield. The new study signals Beijing is thinking not only in traditional military terms ships, aircraft, missiles but also in terms of electronic warfare and denial of external communications support to Taipei during a crisis. Strategically, this work underscores a growing recognition in Chinese defense planning of the critical importance of communications infrastructure in modern warfare and the vulnerability of satellite-Internet systems to coordinated electronic-warfare campaigns. If implemented, such jamming capabilities could degrade Taiwan's ability to coordinate with allies, hamper civilian resilience, and complicate as-yet-unannounced reinforcement operations. More broadly, the research fits into a global trend in which states treat space-based comms and data links as contested battlefields in their own right meaning that control over satellite connectivity, or the ability to deny it, may become as significant as control over land, sea, or air.

Read more: https://www.taipeitimes.com/News/taiwan/archives/2025/11/24/2003847754

Republic of China (ROC) | Taiwan

Taiwan warns of biases, data breach in Deepseek, other Chinese AI

The growing security concern raised by the National Security Bureau (NSB) of Taiwan, following its inspection of five China-origin generative AI apps Deepseek, Doubao, Yiyan, Tongyi and Yuanbao. The inspections, carried out jointly with the Ministry of Justice Investigation Bureau (MJIB) and the Criminal Investigation Bureau (CIB), evaluated each app across 15 security-related indicators covering personal data collection, permission usage, data transmission and sharing, system-level information extraction, and biometric data access as well as an additional 10 indicators assessing the content generated by those models.

Results were alarming: all five apps failed multiple security benchmarks. For instance, Tongyi failed 11 out of the 15 security checks, while Doubao and Yuanbao failed 10, Yiyan failed 9 and Deepseek failed 8. The violations included invasive data practices such as requesting location access, collecting screenshots, harvesting device identifiers, and imposing unfair privacy terms suggesting potential risks to individual privacy and to business or state secrets in corporate environments.

Moreover, the content produced by these generative-

AI systems consistently aligned with Beijing's political narratives. When asked about cross-Strait issues, the models produced output stating that "Taiwan is not a country," calling it "an inalienable part of China," and refusing to use terms like "democracy," "freedom," or "human rights." Such results indicate that the underlying data systems are subject to political censorship or control, potentially serving as tools for influence operations or disinformation campaigns.

Strategically, this raises serious national-security and sovereignty concerns for Taiwan. The findings show that widespread adoption of tools developed under different political systems could expose citizens, businesses and government institutions to data leaks, privacy violations, and politically motivated content bias. In the broader context of intensifying cross-Strait tensions and information warfare, the NSB's warning underscores how digital technology and AI have become new frontiers in state-level competition where soft power, surveillance capabilities and information control can be wielded alongside traditional military and diplomatic pressure.

Read more: https://focustaiwan.tw/cross-strait/202511160005?

TSMC files lawsuit against former executive on security concerns

The Taiwan Semiconductor Manufacturing Company (TSMC), and the primary actors are its former Senior Vice President Wei-Jen Lo and Intel. TSMC has filed a lawsuit in Taiwan's Intellectual Property and Commercial Court against Lo, alleging he breached his employment and non-compete agreements, along with Taiwan's Trade Secrets Act, by joining Intel in October 2025 shortly after retiring, and potentially transferring proprietary technology to the U.S. firm. The complaint cites a "high probability" that Lo disclosed or transferred confidential information related to advanced chip-making processes (including 5 nm, 3 nm, and particularly the cutting-edge 2 nm node) developed under his oversight. In response, Taiwanese prosecutors have launched a criminal investigation: they raided two of Lo's residences, seizing computers, USB drives and other digital devices under warrants, and moved to freeze his assets – actions that escalate the dispute from a civil contractual matter to a potential national security issue under Taiwan's laws. Meanwhile, Intel has publicly denied any misappropriation, stating it sees "no merit" to the claims and affirms its policies to prevent unauthorized use of third-party intellectual property.

This development comes amid intensifying global competition in semiconductor manufacturing, especially for leading-edge nodes that enable high-performance computing and AI hardware. TSMC's fear is that leakage of its process know-how to Intel already a major industry rival seeking to regain technological leadership could undermine its competitive edge and erode the value of years of research and development investment. The involvement of prosecutors and potential invocation of national-security legislation reflect Taiwan's recognition that advanced semiconductor technology is a strategic asset with economic and security dimensions. In a broader sense, the case illustrates a growing trend in the global tech industry: as chipmaking becomes ever more strategic, talent mobility and corporate-to-corporate transfers of key personnel increasingly raise national security and intellectual-property concerns, especially when such talent has deep knowledge of advanced fabrication processes that underpin next-generation computing.

Read more: https://www.reuters.com/world/asia-pacific/tsmc-files-lawsuit-against-former-executive-security-concerns-2025-11-25/?

European Union | EU

Simpler EU digital rules and new digital wallets to save billions for businesses and boost innovation

The main subject is a new regulatory framework, proposed by the European Commission (EC), that seeks to monitor and curb foreign subsidies used to distort the EU internal market. The Commission is acting in conjunction with the 27 EU member states and aims to shield European firms and markets from unfair competition fueled by state-backed financial support outside the EU.

Contextually, this comes amid growing concerns that non-EU governments provide large-scale subsidies often not transparent to companies operating in or exporting to Europe, giving them an advantage over EU-based competitors. In a tightly integrated internal market, such distortions can undermine fair competition, investment, and economic stability.

The developments include a formal announcement of a comprehensive control regime under which

non-EU companies receiving foreign public support may be subject to thorough screening when they bid for public tenders, invest in EU companies, or otherwise affect EU markets. The regime grants the European Commission powers to investigate foreign subsidies, assess their potential distortive effects, and impose remedies for example, requiring repayment of subsidy advantages, or blocking investments or acquisitions by subsidised foreign firms. The new rules will apply broadly across sectors, covering mergers and public procurement alike.

Technically, the mechanism will rely on mandatory disclosure of subsidies by non-EU firms or on flagging mechanisms by member-state authorities, with defined thresholds for subsidy size and impact enabling tailored scrutiny where foreign financial support might pose risks to competition, market access, or strategic industries.

Strategically, this initiative represents a significant shift in how Europe addresses foreign economic influence: by explicitly treating foreign subsidies as potential threats to market fairness and sovereignty. It aligns with a broader global trend in which major powers adopt protective economic tools whether export controls, investment scrutiny, or subsidy oversight to defend domestic industries. For the EU, the regime aims to preserve level-playing fields, safeguard competitiveness of European firms, and reduce susceptibility to foreign state-driven economic leverage. That, in turn, reinforces economic resilience and market integrity in an era of intensifying global competition.

Read more: https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2718

The Commonwealth of Australia

Australia's weapons programs exposed in defence industry cyber attacks

The main subject is a wave of cyber-intrusions targeting the Australian Defence Force (ADF) and associated military projects, allegedly carried out by a hacking group known as Redback. According to the recent disclosure by security authorities and the Australian Signals Directorate (ASD), Redback penetrated networks tied to multiple ADF procurement and research-and-development programmes, compromising sensitive documents related to weapons systems, capability roadmaps and future projects.

Contextually, the campaign arrives amid heightened global interest in defence and technological intelligence with strategic adversaries increasingly using cyber-espionage as a cost-effective alternative to traditional spying or sabotage. The ADF's modernization efforts, encompassing advanced maritime, aerospace and electronic-warfare capabilities, make it a high-value target for any actor seeking to glean insights into Australia's defence posture or share such details with third-party states. The specific developments include forensic confirmation that Redback exploited unpatched vulnerabilities in legacy collaboration-tools and used spear-phishing to gain initial access. Once inside, the hackers moved laterally across networks, harvested credentials, and exfiltrated troves of classified related to future procurement plans. Some exfiltrated archives reportedly included specifications for missile-defence systems and classified scenario-planning documents. The breach was detected after unusual outbound data flows flagged by intrusion-detection systems. Although no destructive sabotage was detected, the theft of intellectual property and classified planning data is assessed as severe.

Strategically, the incident underlines how cyber-espionage is increasingly undermining traditional notions of security. For Australia, it raises urgent questions about how well its defence-industrial base and procurement processes are insulated against advanced persistent threats. Internationally, the attack reflects a broader trend: in current great-power competition, state-affiliated or state-tolerated hacking groups serve as force multipliers capable of collecting sensitive military intelligence with minimal risk. The Redback operation thus not only erodes secrecy around ADF capabilities, but potentially informs adversarial planning, complicating deterrence and undermining trust in secure procurement.

Read more: https://www.abc.net.au/news/2025-11-19/defence-cyber-attacks-adf-military-projects-redback-hackers/105999222?

West Asia | Middle East

Frontline Intelligence: Analysis of UNC1549 TTPs, Custom Tools, and Malware Targeting the Aerospace and Defence Ecosystem

UNC1549 is a cyber-espionage group conducting sustained intrusions against aerospace and defence organizations, targeting entities that manage high-value intellectual property, advanced engineering

data, and sensitive supply-chain systems. Its activity occurs within a broader geopolitical environment defined by rapid military modernization, competition over dual-use technologies, and an increasing reliance on globally distributed digital infrastructure. These conditions create fertile ground for state-linked actors to exploit technical vulnerabilities and extract strategic advantage without direct confrontation.

The group's operations typically begin with credential theft or socially engineered phishing designed to compromise user access points. Once inside, UNC1549 relies heavily on living-off-the-land techniques, using legitimate administrative tools to evade detection while moving laterally across networks. Their focus includes build servers, CAD repositories, configuration-management systems, and collaborative engineering platforms sources that store design files, prototype data, component specifications, and project roadmaps. Data exfiltration is conducted through encrypted channels, often blended with normal network traffic, allowing the group to siphon sensitive material quietly while monitoring real-time updates to engineering environments.

The strategic implications are significant. Aerospace and defence firms serve as custodians of technologies that underpin national military capabilities, from guidance systems and propulsion components to mission-critical communications architectures. Compromise of this information can accelerate an adversary's ability to develop competing systems, undermine export-controlled advantages, or craft countermeasures tailored to proprietary designs. More broadly, UNC1549's campaign highlights systemic weaknesses in supply-chain security, including reliance on legacy tools, insufficient segmentation, and inconsistent patching standards. As cyber-espionage becomes a preferred instrument of state competition, safeguarding the defence-industrial base requires hardened development pipelines, continuous monitoring, and deeper coordination between private industry and national security agencies to ensure resilience against long-term, stealthy threat actors.

Read more: https://cloud.google.com/blog/topics/threat-intelligence/analysis-of-unc1549-ttps-targeting-aerospace-defense

Russian Federation & Ukraine

Ukraine signs deal to obtain 100 French-made Rafale warplanes

The defence agreement between Ukraine and France, signed by their leaders Volodymyr Zelenskiy and Emmanuel Macron, to upgrade Ukraine's aerial and air-defence capabilities amid its ongoing war with Russia. Under the letter of intent, Ukraine will acquire up to 100 newly manufactured Dassault Rafale multirole fighter jets over the next decade, along with air-defence systems, drones, munitions (including guided bombs and missiles), and supporting radar and interceptor systems.

This agreement comes at a moment when Ukraine faces intensified Russian drone and missile attacks, particularly targeting civilian infrastructure and frontline areas a backdrop that underscores Kyiv's urgent need to strengthen its long-range strike response and airspace control. The French offer includes not just the aircraft but also next-generation ground-based air-defence batteries (notably the SAMP/T system), associated radars, and aerial drones presenting a comprehensive upgrade to Ukraine's defensive and offensive aerial posture.

Although the letter is preliminary and not a final purchase contract, the deal marks a strategic shift: it is aimed at building a robust, long-term Ukrainian air force and air-defence architecture capable of deterring further Russian aggression. Training and production support are included, but actual delivery of jets is expected to take time, given pilot training requirements and manufacturing schedules.

Strategically, this development carries weight far beyond mere equipment acquisition: it signals deepening defence-industrial cooperation between Ukraine and major European powers, potentially reshaping the balance of air- and missile-defence in the region. If fully realized, the enhancement of Ukraine's aerial capabilities could strengthen its deterrence posture, influence the trajectory of the conflict, and embed long-term military integration between Kyiv and Western allies reflecting a broader trend of expanding European commitment to Ukraine's defence.

Read more: https://www.reuters.com/business/aerospace-defense/zelenskiy-france-seal-air-defence-warplane-deals-2025-11-17/?

Hacker NoName057(16) launched distributed-denial-of-service attacks against multiple political-party and government websites

In mid-November 2025, multiple Danish political party websites were rendered temporarily unavailable due to distributed denial-of-service (DDoS) attacks, with Denmark's Agency for Public Safety (Styrelsen for Samfundssikkerhed) confirming that several party sites experienced overload traffic that disrupted access and that the situation was being monitored in coordination with the Defence Intelligence Service (FE) and other authorities. The incidents occurred in the lead-up to Denmark's local and regional elections and matched a broader pattern of rising DDoS activity targeting municipal, regional and political digital assets, which Danish intelligence had earlier assessed as a high cyber threat in the election context. Pro-Russian hacking groups publicly claimed responsibility for these specific attacks on social media, aligning with similar claims of targeting political and media sites to create informational disruption around electoral events, although officials reported that voting processes were not directly affected.

DDoS attacks, which flood servers with excessive traffic to deny legitimate user access, do not inherently compromise underlying data or systems but can degrade availability and require technical mitigation efforts and adaptive defenses to restore service and counter evolving tactics. These events form part of a larger escalation in cyber operations linked to geopolitical tensions in Europe, where state-aligned or ideologically motivated actors increasingly deploy low-cost, high-impact methods such as DDoS to influence public perception and signal capability without overtly destructive outcomes. The attacks underscore the strategic vulnerability of political and government digital infrastructure during sensitive democratic processes and highlight the imperative for robust cybersecurity measures, interagency cooperation and continuous threat assessment to protect electoral integrity and public trust against persistent and sophisticated cyber threats.

Read more: https://samsik.dk/artikler/2025/11/flere-partiers-hjemmesider-ramt-af-ddos-angreb/

Malware & Vulnerabilities

Second Sha1-Hulud Wave Affects 25,000+ Repositories via npm Preinstall Credential Theft

The central subject is a renewed global supply-chain attack targeting the open-source JavaScript ecosystem a second wave of the campaign known as Shai-Hulud 2.0 with primary actors including malicious cyber-attackers exploiting compromised maintainer accounts on the npm (Node Package Manager) registry, targeting developers, CI/CD pipelines, and cloud-native infrastructure worldwide. Between November 21 and 23, 2025, attackers published trojanized versions of hundreds of legitimate npm packages including widely used ones by Zapier, PostHog, ENS Domains and Postman embedding malicious preinstall scripts (setup_bun.js) that automatically install the Bun JavaScript runtime and then execute a second payload (bun_environment.js). Upon installation whether on a developer's workstation or a CI server the malware uses a tool (previously used in the first Shai-Hulud wave) to scan the environment for secrets: API keys, cloud credentials (AWS, GCP, Azure), npm/GitHub tokens, environment variables, and other sensitive files.

Once harvested, the stolen credentials are exfiltrated not via an obvious command-and-control server, but by creating public repositories on GitHub often with names that reference "Sha1-Hulud: The Second Coming." The malware also attempts to establish persistent backdoors by installing self-hosted GitHub Actions runners under the name "SHA1HULUD," which allow remote command execution on infected machines. If exfiltration or persistence fails for instance if authentication fails or no valid tokens are available the malware triggers a destructive fallback: it wipes the entire user home directory, erasing writable files, effectively serving as a "scorched earth" contingency.

By November 24, security vendors confirmed that more than 25,000 GitHub repositories across roughly 350–500 distinct maintainers/users had been impacted, with compromised packages infecting development environments, build servers, and cloud workflows across all major operating systems (Linux, macOS, Windows). This new wave shows a marked escalation from the September 2025 campaign the malicious code now runs at the preinstall stage (making human action unnecessary), uses the Bun runtime to evade detection, supports self-replication and credential reuse to infect further packages, and incorporates stealthier exfiltration via GitHub rather than a fixed external server. Strategically, Shai-Hulud

2.0 represents a worrisome turning point in software supply-chain security and cloud infrastructure risk: by compromising trusted open-source dependencies, attackers can silently propagate, harvest secrets, and gain persistent remote access to critical systems including CI/CD pipelines and cloud environments. For organizations, the incident underscores that supply-chain attacks are no longer limited to opportunistic typosquatting or benign dependency confusion: they can be automated, destructive, and capable of undermining large swathes of global software infrastructure. In a broader international context, it adds urgency to calls for stricter supply-chain hygiene, automated dependency auditing, secrets management, and zero-trust CI/CD practices; and it signals that as development ecosystems grow in complexity, the battle for software integrity may become a foundational dimension of cybersecurity in the digital economy.

Read more: https://thehackernews.com/2025/11/second-sha1-hulud-wave-affects-25000.html?

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.