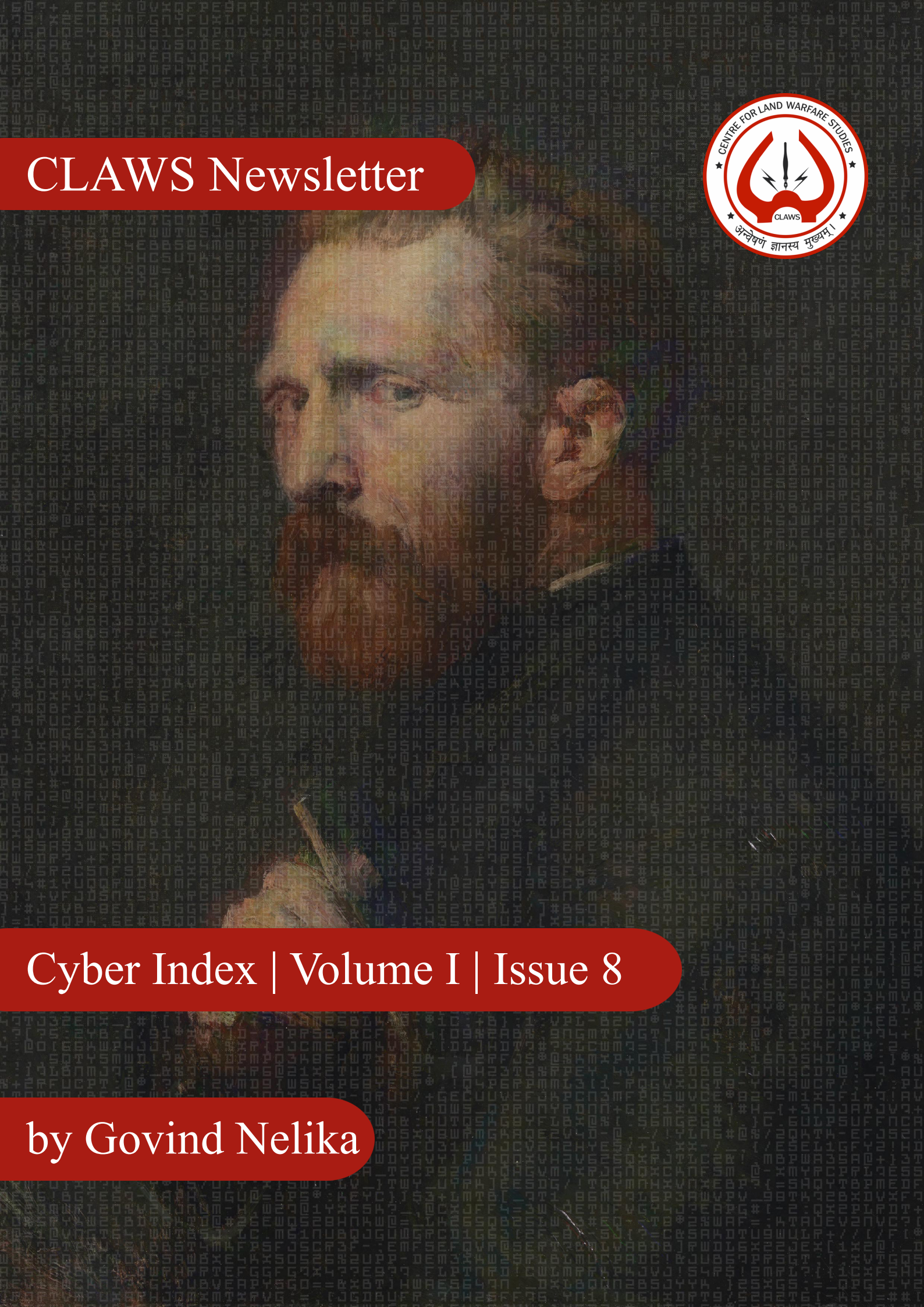
CLAWS Newsletter



Cyber Index | Volume I | Issue 8

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 newly fortnightlyseries 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

Opening News

NATO Allies Pledge 1.5% Of GDP To Boost Cybersecurity & Protect Critical Infrastructure

At the 2025 Hague Summit, NATO members committed to a landmark defence-spending framework—raising total defence and security-related expenditure to 5% of GDP by 2035, including a specific earmark of up to 1.5% for cybersecurity, critical-infrastructure protection, network defence, civil resilience, and innovation. This redefinition reflects a strategic pivot by the Alliance, acknowledging cyberspace as a contested domain and underscoring the imperative of integrated threat mitigation spanning digital and physical assets. The commitment translates into substantial funding for vulnerability management—enabling supply-chain audits, security upgrades for dual-use infrastructure, and investment in detection and defence systems tasking public-private threat-sharing.

However, implementation faces operational headwinds: defining eligible expenditures, securing buy-in from lower-spending allies (e.g., Spain), balancing fiscal constraints, and translating increased budgets into measurable cyber resilience. Strategically, the plan assumes that allocating GDP percentages will drive modernised infrastructure and enhanced cyber deterrence, yet success hinges on robust oversight, inter-state coordination, and incentive alignment to meet the 2029 review and 2035 goals. The initiative also presumes that central funding can effectively bolster both national and NATO-wide readiness, though without clear metrics or risk-based prioritization, there is a threat of inefficiency or misallocation. Overall, NATO's two-tiered funding pledge marks a watershed in digital resilience policy, blending traditional defence with cybersecurity and infrastructure hardening—addressing modern threat landscapes while raising complex questions around accountability, policy coherence, and alliance-wide capability delivery.

Read more: https://www.cybersecurityintelligence.com/blog/nato-allies-pledge-15-of-gdp-to-boost-cybersecurity-and-protect-critical-infrastructure-8501.html

Taiwan fortifies its digital defences as Chinese coercion intensifies

Taiwan is facing an unprecedented surge in cyber threats, with over 2.4 million daily attacks—primarily from Chinese state-linked actors—targeting government networks, critical infrastructure, and semiconductor firms. These operations, including spyware like BADBAZAAR and MOONSHINE, and AI-driven disinformation campaigns, aim to erode public trust, surveil activists, and destabilize Taiwan's political system. In response, the government has launched the NT$8.8 billion 7th National Cybersecurity Development Program, created a National Cybersecurity Center to enhance real-time threat monitoring, and is pursuing legislative reforms to expand private-sector protections. At CYBERSEC 2025, President Lai called for deeper cyber collaboration among democracies. Taiwan's efforts reflect a whole-of-society approach to digital resilience, highlighting the strategic role of cybersecurity in geopolitical deterrence. Its experience underscores the urgent need for integrated threat mitigation, stronger cyber governance, and collective defense as authoritarian regimes increasingly weaponize the digital domain.

Read more: https://aspicts.substack.com/p/the-monthly-roundup-dr-nathan-attrill

Google DeepMind's AI Agent Dreams Up Algorithms Beyond Human Expertise

Google DeepMind has unveiled a groundbreaking AI system called AlphaEvolve, which can independently discover novel algorithms that outperform those devised by humans. By combining its Gemini large language model with evolutionary search techniques, AlphaEvolve has managed to improve on decades-old methods, such as the Strassen algorithm for matrix multiplication, producing more efficient and provably correct solutions. Unlike traditional AI models that replicate existing knowledge, AlphaEvolve generates genuinely new algorithms with real-world applications, including optimizing data centre operations and chip design. Experts highlight this as a significant leap toward AI not just assisting but actually driving innovation in complex sci-

entific and engineering tasks.

Read more: https://www.wired.com/story/google-deepminds-ai-agent-dreams-up-algorithms-beyond-human-expertise/

NSA cyber director Luber to retire at month's end

Dave Luber, a 38-year veteran of the National Security Agency, is set to retire as the agency's Cybersecurity Directorate leader on May 30, 2025. Appointed director in March 2024 after serving nearly four years as deputy, Luber played a pivotal role in bolstering intelligence-sharing on digital threats and fostering collaboration with critical infrastructure operators and industry partners. Before that, he was executive director of U.S. Cyber Command—overseeing 12,000 personnel and a $700 million budget—and previously led NSA Colorado and the Remote Operations Center within Tailored Access Operations. His departure coincides with major leadership upheavals at the NSA, including the firing of its chief and cuts of 8% of civilian staff under a federal downsizing initiative. Luber's exit, alongside the departures of his deputy and COO, marks a significant shift in the agency's cybersecurity leadership amid growing global digital threats.

Read more: **https://therecord.media/nsa-cyber-director-dave-luber-to-retire?**

United States of America (USA)

FTC's Ferguson tells lawmakers agency won't regulate AI until after problems occur

FTC Chair Andrew Ferguson's testimony before Congress, where he outlined a cautious, reactive approach to AI regulation. Ferguson emphasized that the agency would avoid preemptive rules and instead act only after concrete problems emerge, arguing that premature regulation could stifle innovation and give an advantage to entrenched players. This marks a departure from the more proactive stance of his predecessor, Lina Khan. Ferguson maintained that the FTC will continue using existing enforcement powers to target deceptive or harmful AI practices but rejected the need for new, anticipatory frameworks. This approach assumes that market dynamics and post-hoc enforcement can sufficiently manage risks, though it raises concerns about delayed responses to emerging harms, potential regulatory gaps, and the absence of clear national standards. The stance has broader implications for U.S. competitiveness, federal-state policy coordination, and the country's global positioning in AI governance.

Read more: https://therecord.media/ftc-ferguson-wont-regulate-ai-until-problems-arise?

Trump administration officially rescinds Biden's AI diffusion rules

The U.S. Department of Commerce has officially rescinded the Biden-era AI Diffusion Rule, which was scheduled to take effect on May 15, 2025, and introduced tiered limits on exporting advanced AI chips. The move, announced on May 13, reflects a shift in strategy: rather than broad, blanket restrictions, the Trump administration aims to pursue bilateral negotiations with individual countries. In the interim, the Commerce Department issued guidance reiterating that U.S. export regulations already prohibit the use of Huawei's Ascend AI chips worldwide, highlighted risks associated with training AI models in China, and advised firms to safeguard supply chains against diversion. Industry reaction was swift: semiconductor companies like Nvidia and AMD welcomed the change, with Nvidia's stock rising in response. Officials including BIS Under Secretary Jeffry Kessler stated the administration will "pursue a bold, inclusive strategy" to promote U.S. AI technology globally while protecting it from adversarial access, and plan to introduce a replacement policy in the future

Read more: https://techcrunch.com/2025/05/13/trump-administration-officially-rescinds-bidens-ai-diffusion-rules/

The People's Republic of China | China

China warns of legal consequences to those involved in US chip measures

China's Commerce Ministry has announced that any individuals or entities that assist in implementing U.S. export control measures—such as discouraging use of Huawei's Ascend AI chips—could face legal liabilities under China's Anti-Foreign Sanctions Law, framing this as retaliation against "discriminatory restrictive measures" imposed by the U.S. This policy aims both to deter international compliance with U.S. restrictions and to assert China's sovereign right to technological development under international trade norms. The move underscores the cybersecurity relevance of semiconductor supply chains: controlling access to AI-capable chips implicates national resilience, vulnerability management, and digital sovereignty. From an operational standpoint, multinational firms face conflicting regulatory mandates—balancing U.S. export limitations designed to mitigate IP leakage and national security threats against China's countervailing legal risks intended to uphold domestic industry autonomy. Strategically, China assumes that legal enforcement will effectively blunt global participation in U.S.-led export governance, though this presumes sufficient jurisdictional reach and willpower to prosecute overseas actors. Yet enforcing these measures against foreign organizations poses practical challenges, including extraterritorial applicability and due process in global corporate contexts. Overall, the announcement signals a policy escalation in the U.S.–China tech rivalry, raising critical implications for digital resilience through diversified chip sourcing, enhanced supply chain transparency, and adaptive compliance frameworks capable of navigating dual regulatory environments.

Read more: https://www.reuters.com/world/china/china-warns-legal-consequences-those-involved-us-chip-measures-2025-05-21/?

New office in China for existing employees 'a continuation of longstanding presence there,' Nvidia tells GT

Nvidia has clarified that its rumored new R&D facility in Shanghai is not an expansion, but rather an extension of existing operations—leased to house current staff, not intended for new GPU design or IP development to navigate US export constraints. The company emphasized that export controls banning its Hopper series H20 chips effectively ended sales of its advanced AI datacenter hardware in China, impacting its competitiveness in a market projected to reach US $50 billion within two to three years. With these restrictions in place, local Chinese competitors are now able to leverage the vacated market space, echoing strategic concerns about America's ability to maintain technological dominance . From a cybersecurity and export control perspective, this situation underscores the tension between safeguarding intellectual property and enabling global R&D presence: the policy aims to mitigate the risk of core GPU design and sensitive IP leaking to entities under adversarial influence, yet it complicates vulnerability management for multinational firms seeking to operate securely across regulated zones. Operationally, Nvidia faces the challenge of balancing compliance—ensuring that no controlled designs are transmitted to China—with maintaining agility and innovation in a core growth market. Strategically, policymakers must weigh the effectiveness of export bans in protecting national IP against the unintended acceleration of local ecosystems empowered by protected market access. The underlying assumption here is that infrastructure leases do not equate to on shored R&D, but enforcement agencies will likely scrutinize any evidence of design replication or IP transfer. The broader implication is that digital resilience now extends beyond cybersecurity defenses—it encompasses supply chain integrity, regulatory compliance, IP governance, and strategic market positioning under a fragmented global tech regime.

Read more: https://www.globaltimes.cn/page/202505/1334463.shtml

China slams US abuse of export restrictions on Huawei chips

China's Ministry of Commerce vigorously condemned the U.S. for misusing export control regulations to impose stringent restrictions on Huawei's Ascend chips, labeling the action as "non market and unilateral bullying." Spokesperson He Yongqian asserted that these measures unjustly threaten the global semiconductor supply chain, violate international trade norms, and jeopardize mutually beneficial cooperation between Chi-

nese and American companies. The ministry pledged to take decisive action to safeguard Chinese enterprises' legitimate rights and interests, and demanded that the U.S. immediately reverse its policy moves.

Read more: http://english.scio.gov.cn/pressroom/2025-05/16/content_117878419.html?

Russia – Ukraine

Russian hackers breach orgs to track aid routes to Ukraine

A state-sponsored cyberespionage campaign by Russia's GRU-linked APT28 (Fancy Bear/Forest Blizzard) has actively targeted international organizations across defense, transportation, IT services, air traffic, and maritime sectors in the U.S. and 12 European countries since 2022, with the objective of surveilling and potentially disrupting flows of military and humanitarian aid into Ukraine. The adversary employed a blend of stealth techniques—spear-phishing, password-spraying, and exploitation of Microsoft Exchange and Roundcube vulnerabilities—to infiltrate trusted third-party networks and pivot laterally using living-off-the-land tools (PsExec, Impacket, RDP, Certipy, ADExplorer) and custom backdoors like Headlace and Masepie. Critically, operators hijacked over 10,000 internet-connected cameras at border crossings, rail and traffic nodes, and military sites to gather real-time logistical intelligence (e.g., cargo manifests, container IDs, shipment routes). The campaign's digital footprint suggests careful stealth—trusted protocols, close-proximity infrastructure, MFA enrollment tactics, and staggered exfiltration—to evade detection. Joint advisories from 21 intelligence agencies caution that such reconnaissance may prelude disruptive cyber or physical action. From a cybersecurity standpoint, vulnerabilities in default credentials, unpatched connected devices, and weak network segmentation in OT environments expose significant systemic risks. The operational response must emphasize robust vulnerability management—patching, credential hygiene, device audits, network visibility—and bolster digital resilience through segmentation, anomaly detection, and cross-sector collaboration. Strategically, this campaign underscores the importance of securing logistics and aid supply chains under geopolitical tension and elevates the role of multinational threat intel sharing and policy-aligned regulatory frameworks. Underlying assumptions include reliance on metadata as actionable intelligence and the ability of publicly circulated technical advisories to mitigate exploitation; neither fully addresses the persistent challenges of attribution, the scale of camera-based espionage, and ensuring proactive security compliance across diverse infrastructure operators.

Read more: https://www.bleepingcomputer.com/news/security/russian-hackers-breach-orgs-to-track-aid-routes-to-ukraine/

'Operation RoundPress' Targets Ukraine in XSS Webmail Attacks

Operation RoundPress is a sophisticated cyber-espionage campaign, active since 2023 and attributed with medium confidence to the Russian state-linked threat group Sednit (also known as APT28 or Fancy Bear). The attackers deployed spear-phishing emails laden with malicious JavaScript that exploits XSS vulnerabilities in widely used webmail platforms—including Roundcube, Horde, MDaemon (zero-day CVE 2024 11182), and Zimbra (CVE 2024 27443). Merely opening the email in an affected webmail client enabled the script to harvest login credentials, two-factor authentication secrets, email content, contacts, and account settings—all exfiltrated to command-and-control servers. Primary targets are government entities, military and defense contractors in Ukraine, Bulgaria, Romania, and beyond, but the campaign has also struck agencies in Africa, Europe, and Latin America. While the malware doesn't maintain persistence beyond the browser session, the breadth of stolen data poses significant risk. Security experts urge immediate patching of vulnerable webmail systems, strengthening email defenses, and promoting robust cyber hygiene measures

Read more: https://www.darkreading.com/threat-intelligence/operation-roundpress-ukraine-xss-webmail-attacks?

DPRK-Backed TA406 Targets Ukraine With Malware Campaigns

North Korea–linked threat group TA406 has been targeting Ukrainian government entities since February 2025 in a cyber-espionage campaign aimed at gathering strategic intelligence. Using spear-phishing emails disguised as think tank outreach, the group deployed malware via password-protected archives and malicious scripts to steal credentials, system data, and establish persistence. Unlike Russian cyberattacks focused on battlefield disruption, TA406's operations appear designed to assess Ukraine's political and military resilience, likely to inform North Korea's policy and support decisions amid the ongoing conflict.

Read more: https://www.infosecurity-magazine.com/news/dprk-backed-ta406-targets-ukraine/

Nippon-koku | Japan

New Japan law allows preemptive defense of infrastructure cyberattack

Japan's newly enacted "active cyberdefense" law marks a significant shift in its cybersecurity posture, enabling preemptive measures during peacetime to counter rising cyber threats targeting national infrastructure. Driven by recent cyberattacks on sectors such as aviation and banking, the legislation establishes a legal foundation for real-time monitoring of cross-border communications metadata—such as IP addresses—while explicitly excluding domestic traffic and message content to safeguard constitutional rights. Crucially, the law mandates that critical infrastructure operators, including those in energy and transport, report cyber breaches to the government, enhancing threat visibility and response coordination. Operational responsibility for neutralizing hostile servers initially rests with law enforcement agencies, with the Self-Defense Forces authorized to intervene in complex or premeditated attacks, signaling a militarized cybersecurity escalation path.

To address civil liberty concerns, the government incorporated provisions to protect personal privacy and established an independent oversight panel with pre-authorization powers for surveillance and countermeasures, reflecting an attempt to balance security imperatives with democratic safeguards. Strategically, the policy underscores Japan's intent to align its cyber defense capabilities with those of the U.S. and Europe, emphasizing proactive vulnerability management and digital resilience in the face of increasingly sophisticated threat actors. However, challenges remain in operational execution, particularly in delineating thresholds for military involvement, ensuring interagency coordination, and maintaining transparency in oversight mechanisms. The law's assumption that metadata analysis alone can effectively identify threats without infringing on privacy may be tested in practice, especially under conditions of persistent or state-sponsored cyber aggression. Overall, the legislation signals Japan's strategic pivot toward a more assertive cybersecurity doctrine, with substantial implications for national policy, international cyber norms, and the evolving balance between security and civil liberties.

Read more: https://english.kyodonews.net/articles/-/53912?

The Republic of Singapore

Singapore's Chief of Cybersecurity David Koh: Navigating the New Global Tech Order

Singapore's Commissioner of Cybersecurity, David Koh, emphasizes how global shifts in trade, technology, and geopolitics are reshaping cybersecurity. He notes that traditional globalization models like free trade and just-in-time supply chains are being replaced by friend-shoring and on-shoring, increasing national control over technological resources. Koh also highlights a growing preference for bilateral agreements over multilateral forums, even as Singapore continues to champion inclusive platforms like the UN's Open-ended Working Group on cyber norms. Crucially, he observes a trend toward the securitization of technology: what was once seen as a benign, collaborative domain is increasingly treated as a strategic asset, entangled with national security and political leverage. This shift creates a more fragmented technology landscape, risks interoperability

breakdowns, and disproportionately harms smaller and developing countries lacking influence or resources. Koh warns that unless countries commit to interoperable standards and protect inclusive dialogue, the global digital ecosystem may fracture—undermining economic, social, and even safety aspects of interconnected systems.

Read more: https://www.justsecurity.org/113390/global-tech-david-koh/

Islamic Republic of Pakistan

Cybernet Taps Nokia for 1.2T High-Speed National Fiber Network in Pakistan

Pakistan's Cybernet has partnered with Nokia to deploy a groundbreaking national optical fiber backbone capable of delivering 1.2 terabits per second per wavelength, using Nokia's 1830 GX platform with ICE7 coherent optics. In its first phase, this next generation infrastructure will connect more than 25 cities and provide over 50 Tbps of long haul capacity, bolstering services like data-center interconnect, enterprise networks, and Cybernet's consumer brand, StormFiber. The network's high-speed, low-latency backbone will also support cross-border transit to Central Asia, strengthening both domestic and regional connectivity. Cybernet sees the deployment as essential to meeting surging bandwidth demands and enhancing user experience, while Nokia emphasizes that this scalable, cost-effective solution will drive Pakistan's digital transformation and integrate its infrastructure into the global digital economy.

Read more: https://techafricanews.com/2025/05/07/cybernet-taps-nokia-for-1-2t-high-speed-national-fiber-network-in-pakistan/

European Union

Europol and Microsoft disrupt world's largest infostealer Lumma

Europol's European Cybercrime Centre (EC3), in collaboration with Microsoft, has successfully dismantled the Lumma Infostealer infrastructure—identified as the world's largest information-stealing malware—targeting millions of compromised endpoints to harvest credentials, financial data, and personal information for illicit sale on criminal marketplaces. This joint operation demonstrates an effective threat mitigation model combining public-private intelligence-sharing, forensic takeover of command-and-control servers, and marketplace disruption. The takedown significantly enhances digital resilience by severing a critical node in the cybercriminal ecosystem and signals robust supply-chain defense through coordinated takedown efforts. However, operational challenges persist: malware developers can adapt or migrate to decentralized infrastructures, and sustaining post-disruption monitoring demands continuous effort. Strategically, the case underscores the importance of regulatory frameworks that encourage cross-sector partnerships and reinforce vulnerability management—not only via cybersecurity hygiene but by targeting cybercrime infrastructure at scale. Underlying assumptions include the belief that authority over core criminal servers and marketplaces sufficiently degrades threat actor capabilities, and that public-private cooperation is both scalable and enforceable across jurisdictions. Policymakers should view this as a benchmark for future operations, where law enforcement and industry must collaborate under clear legal mandates, shared intelligence standards, and rapid operational synchronization to ensure enduring cyber stability.

Read more: https://www.europol.europa.eu/media-press/newsroom/news/europol-and-microsoft-disrupt-world%E2%80%99s-largest-infostealer-lumma

EU launches a European vulnerability database to boost its digital security

The European Commission has launched the European Vulnerability Database (EVD) to enhance the EU's cybersecurity autonomy and reduce reliance on foreign systems like the U.S.-based CVE. Operated by ENISA

and funded by the Digital Europe Programme, the EVD aims to centralize and manage public disclosures of software vulnerabilities relevant to the EU. It supports digital sovereignty, aligns with the Cyber Resilience Act, and fosters a multi-stakeholder approach involving both public and private actors. While strategically significant, the success of the EVD depends on widespread participation, interoperability with existing standards, and its ability to balance European independence with global cybersecurity coordination.

Read more: https://digital-strategy.ec.europa.eu/en/news/eu-launches-european-vulnerability-database-boost-its-digital-security

South Asia

Vietnam faces the fallout of US trade volatility

Vietnam is finding itself on the front line of Washington's increasingly erratic trade policies. After President Trump announced a 90 day pause on broad tariffs beginning 9 April 2025—soon followed by sharp spikes reaching up to 145% on Chinese goods and later rolls backs to 115%—Vietnam, heavily reliant on US exports, experienced a sharp market shock. The dong weakened and the VN Index plunged, casting uncertainty over export sectors like electronics, footwear, apparel, and seafood. Although the tariff suspension offered temporary relief, it also underscored the structural vulnerability of export-driven economies to sudden policy shifts. In response, Vietnam has tightened inspections on Chinese-origin inputs, imposed anti dumping duties on steel, and pledged reforms such as lowering tariffs on US imports and boosting purchases of American goods. But deeper fixes are needed. Experts argue that Vietnam must diversify its markets beyond the US—by expanding ties with the EU, Japan, ASEAN, and China—and move up the value chain toward technology, semiconductors, renewable energy, and digital services. Active engagement in trade agreements like CPTPP and RCEP, strengthening institutional trade safeguards, and aligning domestic policies to promote high value manufacturing are also critical. Otherwise, Vietnam risks being caught in geopolitical crosswinds, unable to rely on the now-unstable multilateral trade order.

Read more: https://eastasiaforum.org/2025/05/12/vietnam-faces-the-fallout-of-us-trade-volatility/

Sri Lanka stalls Starlink over security and sovereignty concerns

Sri Lanka has paused the rollout of SpaceX's satellite broadband service Starlink, citing national security and digital sovereignty concerns. While Starlink's extensive low-Earth orbit constellation could help bridge the country's connectivity gaps—especially in remote, underserved, and disaster-prone regions—the government argues its encrypted traffic bypasses local routing and oversight, creating "blind spots" outside state control. This pause, initiated independently rather than under external pressure, reflects a broader shift toward stronger regulation of foreign digital infrastructure under Sri Lanka's new administration. The introduction of the Online Safety Act and the establishment of an Online Safety Commission further underscore this shift, placing foreign services under scrutiny for national security, disinformation, and accountability. Previously fast tracked by the former administration, Starlink's approval now requires deeper integration with domestic telecom infrastructure or partnerships with local providers to satisfy regulatory demands. Though this cautious stance may stall progress toward universal internet access, it highlights the trade-off between digital inclusion and state oversight—and signals the importance of defined policies governing foreign-operated cloud, satellite, and AI platforms in safeguarding Sri Lanka's digital sovereignty.

Read more: https://www.aspistrategist.org.au/sri-lanka-stalls-starlink-over-security-and-sovereignty-concerns/

Middle East

US offers $10 million for intel on Iran-linked hacker in ICS malware campaign against critical infrastructure

The U.S. Department of State has announced a $10 million Rewards for Justice bounty for intelligence identifying or locating a cyber actor known as "Mr. Soul" (aka "Mr. Soll"), affiliated with Iran's IRGC-linked "CyberAv3ngers" group, which deployed the IOCONTROL malware to infiltrate and disrupt industrial control systems (ICS/SCADA) globally—including U.S. critical infrastructure—by exploiting weak defaults on routers, PLCs (notably Unitronics Vision), HMIs, IP cameras, and firewalls. The campaign, attributed to six IRGC-CEC officials charged under the CFAA and sanctioned by the U.S. Treasury, demonstrates a strategic threat vector targeting operational technology platforms across utilities, manufacturing, and healthcare sectors. Claroty and Armis analysis confirms IOCONTROL functions as a Linux-based backdoor—targeting ARM-based IoT/OT devices and capitalizing on vulnerability management lapses such as unchanged default credentials. The U.S. response—combining bounty incentives, targeted sanctions, and CISA advisories—highlights an integrated policy approach to enhance resilience through supply-chain oversight, proactive threat mitigation, and regulatory pressure on ICS vendors and operators. Operational challenges include attributing anonymized threat actors, securing widespread IoT/OT asset inventories, and enforcing hardening standards across decentralized infrastructure environments. Strategically, the assumption that financial incentives and sanctions will yield actionable intelligence rests on the premise of insider cooperation; however, persistence in default-credential vulnerabilities indicates deeper systemic neglect. Policymakers must now reconcile the role of international cyber diplomacy with domestic resilience mandates, while cybersecurity professionals face the urgent task of fortifying ICS networks through rigorous vulnerability management, zero-trust segmentation, and cross-sector coordination.

Read more: https://industrialcyber.co/industrial-cyber-attacks/us-offers-10-million-for-intel-on-iran-linked-hacker-in-ics-malware-campaign-against-critical-infrastructure/

OpenAI to help UAE develop one of world's biggest data centers, Bloomberg News reports

OpenAI is reportedly partnering with UAE-based technology firm G42 to develop one of the world's largest AI-focused data centers, known as the "Stargate" project, in Abu Dhabi. The planned facility will have a massive 5-gigawatt capacity and is expected to play a central role in expanding global AI infrastructure. While OpenAI's involvement has not been officially confirmed, it is expected to act as a major anchor tenant once the center becomes operational. This initiative follows a broader UAE–U.S. technology partnership aimed at positioning the UAE as a global AI hub. The data centre, slated to launch in 2026, reflects the Gulf state's growing ambition to lead in the high-performance computing and artificial intelligence sectors.

Read more: https://www.reuters.com/world/middle-east/openai-help-uae-develop-one-worlds-biggest-data-centers-bloomberg-news-reports-2025-05-16/

Vulnerabilities

Researchers Expose New Intel CPU Flaws Enabling Memory Leaks and Spectre v2 Attacks

Researchers from ETH Zurich and Vrije Universiteit Amsterdam have discovered new vulnerabilities in modern Intel CPUs that bypass existing Spectre v2 defenses, enabling attackers to leak sensitive memory across privilege boundaries. One flaw, called Branch Privilege Injection (CVE 2024 45332), exploits timing issues in branch prediction to inject malicious code paths from user space into kernel space, leaking data like password hashes even on patched systems. Another set, known as Training Solo, revives Spectre v2-style attacks across user and virtual machine boundaries, with faster data leakage rates.

These flaws affect Intel CPUs from the 9th generation onward. Intel has released microcode updates with

minimal performance impact (~2–3%) to mitigate the threats. Researchers stress the need for firmware and OS updates, while noting that speculative execution remains a persistent architectural challenge in CPU design.

Read more: https://thehackernews.com/2025/05/researchers-expose-new-intel-cpu-flaws.html

Critical SAP NetWeaver Vuln Faces Barrage of Cyberattacks

A critical zero-day vulnerability in SAP NetWeaver Visual Composer, tracked as CVE 2025 31324 with a maximum CVSS score of 10, has prompted a widespread cyberattack campaign targeting unsecured SAP systems. Initially disclosed and patched by SAP on April 24–25, 2025, the vulnerability enables unauthenticated attackers to upload arbitrary files and execute code remotely, leading to full system compromise via JSP web shells. Researchers at ReliaQuest and Forescout Vedere Labs have observed active exploitation: unknown threat actors and Chinese-linked APT groups have dropped web shells like "rrx.jsp" and "dyceorp.jsp" to establish command-and-control and persistence. The Shadowserver Foundation reported over 450 Internet-facing NetWeaver instances vulnerable—149 in the U.S., 50 in India, and 37 in Australia. Moreover, on May 12, a second critical zero-day, CVE 2025 42999 (CVSS 9.1), was discovered in the same Visual Composer component, intensifying the risk. Experts strongly recommend immediate patching, or, if patching isn't immediately feasible, disabling the Visual Composer module and restricting access to affected endpoints to thwart further exploitation.

Read more: https://www.darkreading.com/vulnerabilities-threats/critical-sap-netweaver-vuln-cyberattacks?

Advisory Update on Cyber Threat Activity Targeting Commvault's SaaS Cloud Application (Metallic)

CISA's May 22, 2025 update on cyber threat activity targeting Commvault's SaaS cloud backup solution, Metallic, reveals adversaries breached application logic in Commvault's Azure-hosted Microsoft 365 backup service—compromising client secrets and enabling unauthorized access to customer M365 environments. The advisory indicates this breach is likely part of a broader campaign exploiting SaaS misconfigurations, default configurations, and excessive privilege assignments—highlighting persistent vulnerability management gaps in cloud-native applications. To mitigate risk and strengthen digital resilience, CISA urges organizations to monitor Entra audit and sign in logs for irregular modifications, implement conditional access tied to approved IP ranges via premium licensing, rotate compromised credentials, and limit service principal privileges to the minimum necessary. Additionally, on-premise users are advised to restrict management interface exposure, deploy web application firewalls, and patch known vulnerabilities—further supported by inclusion of the related CVE 2025 3928 in the U.S. Known Exploited Vulnerabilities Catalog. This comprehensive set of recommendations underscores the cybersecurity imperative of treating identity, credential, and access management (ICAM) as front-line defense in cloud deployments, balanced by threat detection, incident response alignment, and policy enforcement. Operationally, the advisory highlights challenges in implementing conditional access uniformly—particularly where licensing constraints exist—and emphasizes the need for ongoing credential hygiene and proactive auditing. Strategically, the alert assumes that visibility into Entra logs combined with credential rotation and network restrictions can effectively disrupt attack chains, but success depends on organizational maturity, resource investment, and cross-platform coordination. Overall, the update underscores a paradigm shift: digital resilience now requires SaaS-native visibility controls, identity-centric vulnerability management, and regulatory awareness of cloud service configuration governance.

Read more: https://www.cisa.gov/news-events/alerts/2025/05/22/advisory-update-cyber-threat-activity-targeting-commvaults-saas-cloud-application-metallic

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.