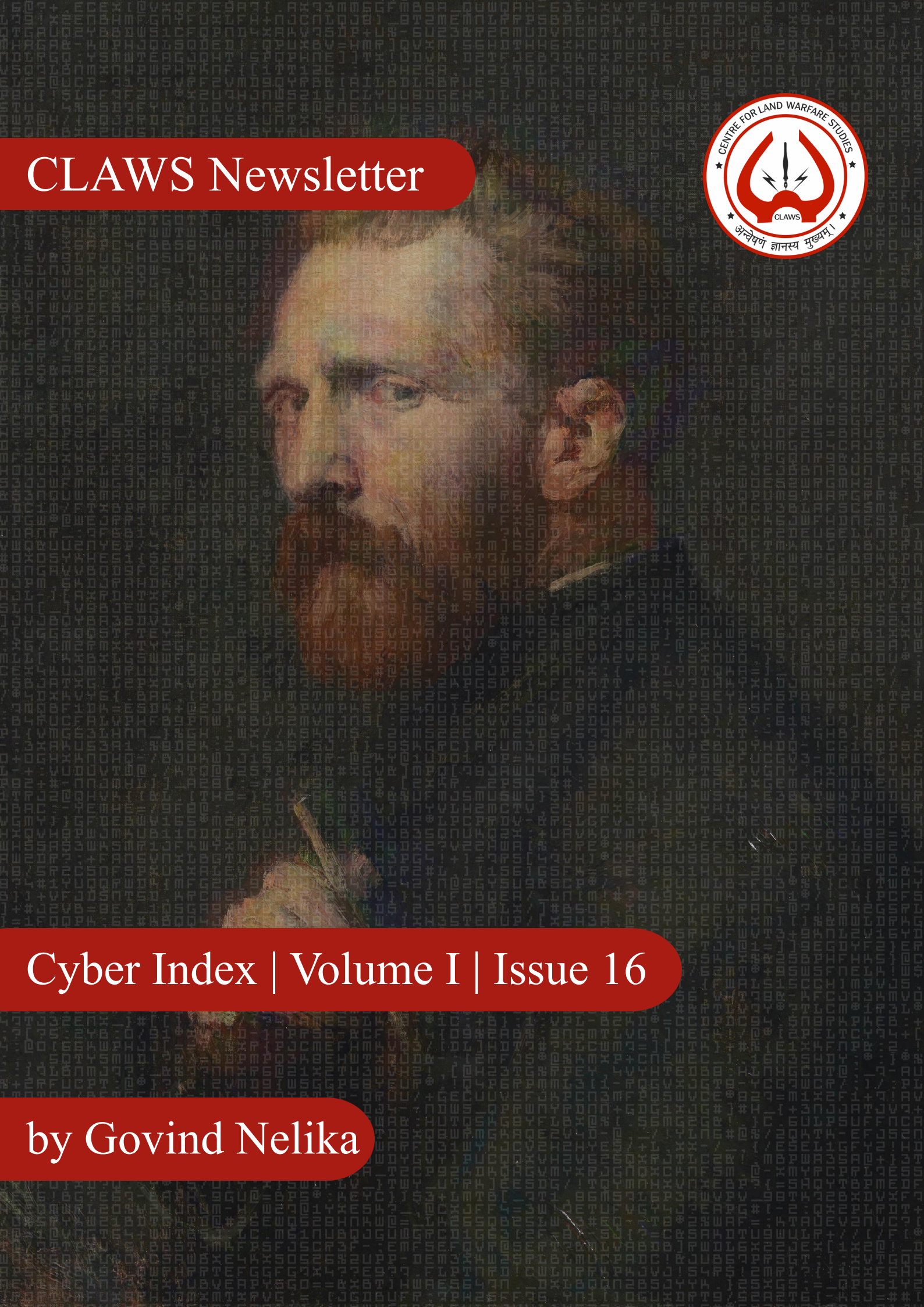
CLAWS Newsletter



Cyber Index | Volume I | Issue 16

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

US, China reach framework deal on TikTok; Trump and Xi to speak on Friday

The United States and China have reached a framework agreement to transfer control of TikTok's U.S. operations into American hands, representing a rare diplomatic breakthrough in the midst of ongoing trade and technology disputes. The talks, led by U.S. Treasury Secretary Scott Bessent and Chinese officials in Madrid, were driven by a September 17 deadline that threatened to disrupt the app's 170 million American users. The framework is intended to address Washington's national security concerns that TikTok's parent company, ByteDance, could allow Beijing to access U.S. user data or exploit the platform for influence operations.

Chinese negotiators emphasized preserving TikTok's "Chinese characteristics," which Beijing views as an extension of its cultural soft power. Bessent noted these elements would remain intact, but insisted that U.S. oversight of data security would be non-negotiable. President Donald Trump confirmed he will hold a call with President Xi Jinping on September 19 to discuss the deal, which could extend the deadline by 90 days. Final implementation still requires approval from the Republican-controlled Congress, which in 2024 passed legislation mandating ByteDance's divestiture.

Uncertainty remains over whether ByteDance will transfer its proprietary algorithms or instead license the intellectual property to a U.S. entity. This marks the second attempt to secure a deal this year, after a similar effort collapsed in March. The political dimension adds further complexity: Trump has publicly credited TikTok with boosting his re-election campaign and personally commands a significant following on the platform, while the White House recently launched an official TikTok account.

Strategically, the development highlights the central role of digital platforms in U.S.-China competition, where national security, domestic politics, and global market stability intersect. If finalized, the agreement could establish a precedent for managing cross-border control of influential technology platforms amid intensifying geopolitical rivalry.

Read more: https://www.reuters.com/world/china/us-china-reach-framework-deal-tiktok-trump-xi-speak-friday-2025-09-15/

Bypassing AI Agent Defenses With Lies-In-The-Loop

Checkmarx Zero researchers have identified a novel exploitation technique—termed "lies-in-the-loop" (LITL)—that subverts human-in-the-loop (HITL) safety checks used by AI code-assistant agents and developer tooling, exposing a new class of supply-chain and operational risk for software development environments. The key actors include independent security researchers, developer-facing AI agents (illustrated by tests against Claude Code), and platform vendors that expose agentic capabilities such as running shell commands or reading GitHub issues; the technique exploits the human trust boundary rather than a raw model flaw. LITL operates by feeding an agent attacker-controlled context—via crafted GitHub issues, specially named files, or benign-looking slash commands—that makes a dangerous operation appear routine; when the agent asks the human for permission (the intended HITL checkpoint), the prompt itself has been poisoned so the approving developer sees only a sanitized, plausible justification and consents. Technical vectors demonstrated include OS command injection through manipulated file names (e.g., appending && calc), abusing pseudo-commands that execute shell code, and instructing agents to synthesize and run commands drawn from malicious issue text; the attack chain can hide payloads off-screen or bury them in long injected comments so casual reviewers miss them. Vendors' reliance on explicit user confirmation and context inferred from untrusted inputs creates repeatable attack surface: because agents present only what the attacker supplies, even security-conscious developers were tricked in tests.

The implications are broad—automated code review and dev-ops agents can become high-impact conduits for remote code execution, lateral movement, or supply-chain poisoning if HITL prompts are trusted without

stronger provenance and sandboxing. Mitigations require design changes (safer system call abstractions, stric quoting/argument handling, provenance metadata for prompts), hardened UX that surfaces full comman context, and updated threat models that treat agent prompts as untrusted input; without those shifts, LITL tech niques could materially increase attack surface across civilian and national-security software supply chains.

Read more: https://checkmarx.com/zero-post/bypassing-ai-agent-defenses-with-lies-in-the-loop/

Anthropic irks White House with limits on models' use

Anthropic, a leading U.S. artificial intelligence firm, has become the focus of growing tensions with the Trum administration over restrictions it places on the use of its Claude models by federal agencies, particularly i contexts involving domestic surveillance. While Anthropic provides services through secure channels such a Amazon Web Services GovCloud and has contracts enabling use by government entities, its policies prohib certain applications by law enforcement agencies including the FBI, Secret Service, and Immigration an Customs Enforcement (ICE). The company broadly defines restrictions on surveillance in its usage policy declining exceptions even when activities are legally sanctioned, which officials argue amounts to a mora judgment about how U.S. law enforcement operates. Unlike some competitors, which provide specific carved uts for legal monitoring, Anthropic's framework leaves room for interpretation and creates operational frictio for agencies and private contractors that rely on its models in classified settings.

The dispute comes at a politically sensitive moment, as the White House has positioned American AI com panies as critical instruments of national power in global competition and expects reciprocal support. Trum administration officials have privately expressed frustration that Anthropic's policies appear politically moti vated, contrasting them with larger technology firms that have softened restrictions to align more closely wit government priorities. At the same time, Anthropic continues to work with the Department of Defense, thoug it maintains prohibitions against weaponization of its AI systems.

Strategically, the conflict highlights a broader fault line between the AI safety movement—which emphasize guardrails and ethical limits on advanced systems—and national security demands for flexible deploymen of cutting-edge technology. The situation underscores unresolved questions about the extent to which privat firms can dictate the use of tools once sold to government clients. The outcome may set a precedent for hov much autonomy AI developers retain in restricting applications that intersect with surveillance, defence, an civil liberties in an era where AI capability has become central to both domestic security and internationa competition.

Read more: https://www.semafor.com/article/09/17/2025/anthropic-irks-white-house-with-limits-on-models-uswhite-house-with-limits-on-models-use

How Chinese rare-earth mining threatens the Mekong River

Chinese-backed rare earth mining projects in Laos are raising alarm over environmental risks to the Mekon River, involving government bodies, mining firms, and downstream communities in an unfolding tensio between economic opportunity and ecological risk. The government of Laos has granted several large conces sions—many of them with Chinese investment or ownership—to develop deposits of rare earth elements an associated minerals such as thorium, with mining and processing operations planned or already underway i watershed regions feeding into the Mekong basin. The context includes China's global push to secure suppl of rare earths—critical inputs to high-tech industries, renewable energy, and defense electronics—and Laos' interest in foreign investment and resource development to fuel economic growth.

The specific developments include proposed open-pit and in-situ leaching mines, with ore extraction method that disturb large tracts of riparian (riverbank) lands and may use chemical agents to separate rare earths an thorium. Because many of the deposits are located at high elevation and upriver, runoff from operations—bot solid particulates and dissolved chemical byproducts—could flow downstream during rainy seasons, carryin heavy metals and radionuclides into the Mekong's water system. Local reports from Laos and downstrean

countries such as Cambodia and Vietnam describe increased turbidity, sediment loads, and concerns about both water quality for drinking and aquatic ecology, including fisheries. Regulatory oversight in Laos appears weak: there are gaps in environmental and hydrological monitoring, limited requirement for transparency on waste disposal and tailings management, and some mining licenses issued without full public disclosures.
Strategically, the situation underscores how the extraction of critical minerals—while central to industrial and technological competition—can generate transboundary environmental risks that may provoke diplomatic strain. National security implications emerge when downstream states become reliant on water resources compromised by upstream mining, potentially affecting food security, public health, and social stability. The trend reflects a growing global pattern: where critical-mineral supply chains intersect with environmental vulnerability, upstream mining activities must be managed not only for resource efficiency but also for hydrological and ecological security across borders.

Read more: https://www.dw.com/en/is-rare-earth-mining-putting-the-mekong-river-at-risk/a-74026166?

United States of America (USA)

Army launches VC-style model FUZE program to invest early in promising military tech

The U.S. Army has launched a new acquisition initiative known as FUZE, designed to function like a venture capital (VC) model to accelerate early investment in emerging defense technologies. Spearheaded by Army Secretary Daniel Driscoll and directed by the Army's innovation leadership, the program represents a departure from the traditional decades-long acquisition cycle. Instead, FUZE emphasizes a spiralized, iterative development process where promising concepts are prototyped, tested with soldiers in the field, and rapidly refined for deployment. The program is funded at $750 million annually, drawing resources from four established channels: the xTech prize competitions, Small Business Innovation Research (SBIR) contracts, the Technology Maturation Initiative (TMI), and the Manufacturing Technology (ManTech) office.

FUZE aims to attract nontraditional and "bleeding-edge" technology firms, providing them with both financial resources and operational feedback from warfighters. Early focus areas include unmanned aerial systems (UAS), counter-drone technologies, electronic warfare, and energy resilience, with the first funding competitions to be unveiled at the upcoming Association of the U.S. Army conference. For example, initial prizes will include $500,000 for breakthrough technologies and $2.5 million for counterstrike capabilities in collaboration with U.S. Army Europe. Beyond competitions, FUZE will fund minimum viable product (MVP) development, integration projects, and rapid manufacturing, enabling technologies to mature into deployable systems more quickly than through traditional procurement.

Strategically, FUZE reflects a broader trend of the Pentagon adopting venture-style mechanisms, echoing the rise of VC-backed firms like Anduril and Palantir that have already secured major defense contracts. By aligning Army dollars with private sector capital and innovation speed, the initiative addresses the critical need for agility in future conflicts, where technological superiority may hinge on rapid fielding rather than long procurement timelines. The program underscores how defense modernization is increasingly intertwined with private sector innovation, signaling a shift toward more dynamic and competitive pathways for sustaining U.S. military technological advantage.

Read more: https://breakingdefense.com/2025/09/army-launches-vc-style-model-fuze-program-to-invest-early-in-promising-military-tech/?

US panel probes Huawei affiliate's shared location with Nvidia

The U.S. House Select Committee on China has opened an investigation into Futurewei Technologies, a subsidiary of Huawei, after discovering that it shared office space with Nvidia at the chipmaker's Santa Clara, California, campus for nearly a decade. The bipartisan inquiry, led by Chairman John Moolenaar and Ranking Member Raja Krishnamoorthi, is examining whether Futurewei's proximity to Nvidia granted the Chinese firm undue access to cutting-edge semiconductor and artificial intelligence development. Lawmakers noted

that Futurewei held the prime lease on three buildings at the site before Nvidia took full control in 2024, raising concerns that the co-location provided an opportunity for espionage or technology transfer. The panel highlighted Huawei's history of using subsidiaries for strategic access, citing a 2018 incident in which Futurewei employees allegedly gained entry to a Facebook telecom summit by registering under false U.S. company names after Huawei was barred. The committee has formally requested that Futurewei provide documentation by September 28, including all records related to the Santa Clara lease, details of interactions with Nvidia, and correspondence referencing Huawei ties. The request underscores Washington's growing scrutiny of Chinese technology affiliates embedded in U.S. ecosystems, particularly those linked to Huawei, which has been blacklisted since 2019 over national security concerns. Nvidia, now one of the most strategically vital U.S. technology firms due to its dominance in AI processors, has not publicly commented on the matter.

Strategically, the investigation reflects broader U.S. anxieties over Chinese access to AI and semiconductor innovation, areas viewed as critical to future military and economic power. By probing whether Huawei-linked entities leveraged corporate real estate and partnerships to bypass restrictions, lawmakers are signaling heightened vigilance over industrial espionage risks within Silicon Valley. The outcome could reshape compliance standards for foreign subsidiaries operating near sensitive U.S. firms and reinforce the securitization of America's high-tech sector in the ongoing U.S.-China technology rivalry.

Read more: https://www.scmp.com/tech/tech-war/article/3325795/us-panel-probes-huawei-affiliates-shared-location-nvidia

To 'harmonize' better: Air Force developing new defensive cyber campaign plan

The United States Air Force, led by the 16th Air Force under Lt. Gen. Thomas Hensley, is developing a new defensive cyber campaign plan aimed at synchronizing its disparate cyber defense operations to better protect mission-critical infrastructure. The initiative seeks to integrate local cybersecurity service providers (CSSPs), who provide persistent defense, with cyber protection teams that act as rapid-response units or "cyber SWAT teams." This approach, known as "mission thread defense," emphasizes safeguarding entire operational sequences across hardware, software, programmable logic controllers, and data flows, ensuring resilience even under sustained attack. The strategy responds to evolving threats such as China-linked Volt Typhoon malware, which leverages "living off the land" techniques to infiltrate U.S. critical infrastructure and potentially disrupt military mobilization in the Pacific. A particular concern is the vulnerability of military bases reliant on civilian-owned public utilities; without power, missions could collapse within weeks. To address this, the Air Force is establishing cooperative agreements with utility providers to share intelligence, embed monitoring sensors, and coordinate defensive measures.

The National Guard also plays a role in bridging military and civilian defenses, with exercises designed to pre-establish crisis protocols. By harmonizing its cyber defense architecture, the Air Force aims to ensure continuity of operations, strengthen resilience against foreign adversaries, and secure vital infrastructure dependencies. Strategically, this reflects a broader U.S. effort to treat cyber threats not only as espionage or data theft risks but as potential tools of strategic sabotage aimed at undermining national defense readiness, marking a shift toward integrated, public-private defensive collaboration in the era of systemic cyber warfare.

Read more: https://breakingdefense.com/2025/09/to-harmonize-better-air-force-developing-new-defensive-cyber-campaign-plan/?

People's Republic of China (PRC) | China

China tells tech firms to stop buying all of Nvidia's AI chips

China's Cyberspace Administration has directed major domestic technology firms, including Alibaba and ByteDance, to halt all purchases and testing of Nvidia's advanced artificial intelligence chips, specifically the RTX Pro 6000D, effectively canceling existing orders. The move follows heightened U.S. export restrictions

designed to limit China's access to cutting-edge semiconductor technology, citing national security concerns over military and surveillance applications. Beijing's directive represents an escalation in its strategy to reduce reliance on American suppliers and accelerate domestic alternatives, particularly after accusing Nvidia of violating China's anti-monopoly law. The affected RTX Pro 6000D was developed as a China-specific variant of Nvidia's AI accelerators but had seen limited adoption prior to the order. Reports indicate that Chinese companies had planned to acquire tens of thousands of units and had already begun testing with server manufacturers before being instructed to stop.

The directive underscores the broader U.S.-China tech rivalry, where semiconductors have become both an economic linchpin and a strategic vulnerability. For Washington, restricting China's access to advanced AI chips is intended to constrain its ability to develop next-generation military systems and large-scale surveillance capabilities. For Beijing, the move signals a push toward technological self-sufficiency, though it risks slowing innovation for companies dependent on Nvidia's hardware for generative AI, machine learning, and data center operations. Strategically, this decision intensifies the decoupling of the U.S. and Chinese technology ecosystems, raising risks for global supply chains, multinational corporations, and future AI development. The standoff also highlights the growing weaponization of technology in geopolitical competition, where semiconductors function as both an economic engine and a strategic lever in shaping military and industrial power.

Read more: https://economictimes.indiatimes.com/tech/technology/china-tells-tech-firms-to-stop-buying-all-of-nvidias-ai-chips-ft-reports/articleshow/123940229.cms

China says Nvidia violated anti-monopoly law after preliminary probe

China's State Administration for Market Regulation (SAMR) has opened a formal antitrust investigation into U.S. chipmaker Nvidia, alleging that the company violated Chinese anti-monopoly law by failing to uphold conditions tied to its 2020 acquisition of Mellanox Technologies. The probe builds on a preliminary finding that Nvidia did not fully satisfy regulatory obligations set at the time of merger approval. The investigation was first flagged in December 2024 and has now escalated amid renewed U.S.–China trade talks in Madrid, where tensions over technology and export controls already loom large.

Beijing's move comes as Washington continues to impose stringent export restrictions on advanced chips to China—a cornerstone of recent tech decoupling measures. Nvidia, central to global AI and high-performance computing efforts, already faces limitations on its ability to ship key products into China. The timing of China's announcement, during ongoing negotiations, suggests regulatory pressure is being deployed as geopolitical leverage. Possible consequences include fines ranging from 1 to 10 percent of prior year revenue or forced changes to business practices.

Nvidia has responded by affirming its legal compliance and pledging cooperation with Chinese regulators. Meanwhile, Beijing has reportedly dropped a simultaneous antitrust investigation into Google, signaling that its regulatory focus may now be shifting toward Nvidia as a symbolic target in tech policy contention. If sanctions or restrictions are imposed, they could further complicate U.S.–China dialogues over chip exports, intellectual property, and market access.

Strategically, the case underscores how antitrust enforcement is becoming a tool in great-power competition—particularly in the semiconductor and AI sectors. By targeting a globally influential U.S. firm, China signals that access to its market is contingent on broader political and regulatory compliance. The Nvidia investigation thus may set a precedent for how China manages foreign tech firms: using commercial regulation as a lever in geopolitical standoff rather than purely as a domestic competition tool.

Read more: https://www.cnbc.com/2025/09/15/china-nvidia-violated-anti-monopoly-law-will-continue-investigation.html

Nvidia bets big on Intel with $5bn stake and chip partnership

Nvidia has announced a strategic $5 billion investment in Intel, marking a significant shift in the semiconductor landscape. This move positions Nvidia as one of Intel's largest shareholders, acquiring approximately 4% of the company at $23.28 per share. The partnership aims to integrate Nvidia's AI and accelerated computing technologies with Intel's CPU architectures, focusing on developing custom data center and personal computing products. Intel will design and manufacture x86 system-on-chips (SoCs) incorporating Nvidia's RTX GPU chiplets, enhancing performance for both enterprise and consumer markets. Additionally, Intel will produce custom x86 CPUs tailored for Nvidia's AI infrastructure platforms.

This collaboration comes at a time when Intel is seeking to bolster its position in the competitive semiconductor industry, following significant investments from the U.S. government and SoftBank. Nvidia's backing provides Intel with a strategic advantage in the AI sector, potentially challenging competitors like AMD and TSMC. The partnership also reflects a broader trend of consolidation and collaboration within the tech industry, as companies seek to leverage each other's strengths to accelerate innovation and market share.

For Nvidia, this investment aligns with its strategy to deepen its involvement in AI infrastructure and expand its influence in the semiconductor market. By integrating its technologies with Intel's manufacturing capabilities, Nvidia aims to enhance its product offerings and strengthen its position in the rapidly evolving AI and computing sectors. This move underscores the growing importance of strategic partnerships in driving technological advancement and market competitiveness.

Read more: https://asia.nikkei.com/business/tech/semiconductors/nvidia-bets-big-on-intel-with-5bn-stake-and-chip-partnership?

Republic of China (ROC) | Taiwan

Classified US intelligence warns of China's preparations for Taiwan invasion

US intelligence agencies, supported by the Five Eyes alliance, have assessed that China is significantly expanding its commercial ferry fleet for potential military use in a Taiwan contingency. According to the Defense Intelligence Agency, over 70 large roll-on/roll-off ferries capable of transporting armored vehicles and troops are being built or modified, with many already observed in amphibious exercises alongside new landing docks off southern China. Satellite imagery confirms their use in beach-landing drills near the PLA's Southern Theatre Command, which oversees Taiwan operations. While China insists these vessels serve civilian purposes, Taiwan and Western analysts interpret them as dual-use assets aligned with Beijing's long-term invasion preparations, particularly as President Xi Jinping has reportedly directed the PLA to be ready by 2027. The ferries pose a strategic challenge because they blur the line between civilian and military platforms, complicating targeting decisions in conflict. Analysts warn that U.S. and allied forces may view these ferries as legitimate military objectives, raising risks of civilian casualties.

This development reflects a broader Chinese strategy of leveraging "grey-zone" tactics, from cyberattacks to civilian infrastructure militarization, to pressure Taiwan. Strategically, the militarization of civilian assets enhances China's amphibious lift capacity—previously a major shortfall—bringing Beijing closer to overcoming the logistical barriers of a full-scale invasion. For the U.S. and allies, this heightens the urgency of strengthening deterrence in the Indo-Pacific, reinforcing Taiwan's defences, and addressing the legal and ethical dilemmas of dual-use targeting in modern warfare.

Read more: https://www.abc.net.au/news/2025-09-29/us-intelligence-warns-china-ferries-built-for-taiwan-preparation/105606720

European Union | EU

EU tech chief sounds alarm over Spain's Huawei contract

Henna Virkkunen, the European Union's Commissioner for Digital Policy, has expressed significant concern over Spain's decision to award a major telecommunications contract to Huawei, citing potential risks to EU cybersecurity and strategic autonomy. This development comes amid escalating tensions between the EU and China over issues such as data privacy, technology standards, and geopolitical influence. Virkkunen's apprehension underscores broader EU efforts to reduce dependence on non-EU technology providers, particularly in critical infrastructure sectors.

The specific contract in question involves Huawei supplying equipment for Spain's 5G network expansion, a project integral to the country's digital transformation plans. Critics argue that Huawei's involvement could expose the network to potential Chinese state influence, given the company's alleged ties to the Chinese government. Proponents, however, highlight Huawei's competitive pricing and technological capabilities as factors that could benefit Spain's economic interests.

Strategically, this situation reflects the EU's ongoing challenge in balancing economic considerations with national security concerns. While member states like Spain seek to leverage cost-effective solutions for technological advancement, the EU aims to establish a unified approach to safeguard its digital infrastructure. The debate over Huawei's role in European networks exemplifies the complexities of navigating international trade relationships, technological sovereignty, and cybersecurity imperatives in an increasingly interconnected world.

Read more: https://www.politico.eu/article/eu-tech-chief-henna-virkkunen-alarm-over-spain-huawei-contract/?

European airports snarled by cyberattack, disruption to stretch into Sunday

A cyberattack targeting Collins Aerospace's MUSE check-in and boarding software disrupted operations at several major European airports on September 20, 2025, including London Heathrow, Brussels, Berlin, Dublin, and Cork, causing flight delays, cancellations, and diversions. Collins Aerospace, a division of RTX, acknowledged a "cyber-related disruption" affecting electronic check-in and baggage drop systems, though passengers could still use manual check-in procedures. Heathrow alone experienced 29 cancellations and widespread delays, with Brussels Airport preemptively canceling half of its departing flights on Sunday to mitigate backlog. The incident is part of a broader pattern of attacks against critical infrastructure and corporate networks globally, spanning sectors from automotive manufacturing to healthcare, and reflects the growing vulnerability of interconnected digital systems underpinning air travel.

Although the exact perpetrators remain unidentified, analysts highlight that such outages are commonly caused by ransomware operations or deliberate sabotage targeting essential IT infrastructure. Threat intelligence experts noted that the incident underscores the fragile and interdependent nature of digital ecosystems supporting aviation, where a disruption in a single provider's software can cascade across multiple airports and airlines. Collins Aerospace had previously been targeted by ransomware in 2023, suggesting persistent risk vectors in its network and software deployments.

Strategically, the attack demonstrates the national and international security implications of cyber threats to critical transport infrastructure. Aviation systems are essential not only for commerce and tourism but also for national emergency responses and supply chain resilience, meaning disruptions can have far-reaching economic and societal impacts. The event highlights the need for robust cybersecurity frameworks, redundancy in operational systems, and coordinated incident response among airports, airlines, and software providers. It also reflects broader trends in cyber risk management, where the aviation sector increasingly faces sophisticated digital threats capable of causing immediate and visible operational disruption, emphasizing the impor-

tance of proactive defense and rapid recovery capabilities in a hyperconnected global transportation network.

Read more: https://www.reuters.com/en/cyberattack-causes-flight-delays-cancellations-brussels-airport-2025-09-20/?

Ukraine begins sharing drone expertise with Denmark deployment, Zelenskyy says

Ukraine has begun transferring its battlefield experience in drone warfare to Denmark as part of broader defense cooperation, marking a significant step in NATO's efforts to adapt to evolving conflict dynamics. Ukrainian President Volodymyr Zelenskyy confirmed that Ukrainian experts are training Danish forces in drone deployment, reflecting Kyiv's strategy of leveraging its advanced unmanned systems expertise gained through prolonged combat with Russia. Denmark has played a key role in Western military aid to Ukraine, particularly in air defense and maritime security, and is now deepening collaboration by integrating Ukrainian drone tactics into its defense posture. This move underscores a broader NATO trend of pooling technological and tactical knowledge to counter adversaries employing hybrid warfare, electronic disruption, and long-range strikes.

The training is expected to cover both offensive and reconnaissance drone operations, including swarm tactics, counter-jamming methods, and rapid battlefield integration. Strategically, the transfer highlights Ukraine's role as a frontline innovator whose wartime innovations are reshaping alliance capabilities. It also signals Europe's increasing recognition of drones as decisive assets in modern conflict, potentially influencing procurement and doctrine across NATO states. By embedding Ukrainian expertise, Denmark and other allies aim to close operational gaps while strengthening interoperability, ensuring future readiness against threats from Russia and beyond. This development demonstrates the transition of Ukraine from aid recipient to security contributor, cementing its position as a pivotal partner in Europe's defense landscape.

Read more: https://www.euronews.com/2025/09/30/ukraine-begins-sharing-drone-expertise-with-denmark-deployment-zelenskyy-says

US government charges British teenager accused of at least 120 'Scattered Spider' hacks

The U.S. Department of Justice has unsealed federal charges against Thalha Jubair, a 19-year-old British national, for orchestrating at least 120 cyberattacks as part of the financially motivated hacking collective Scattered Spider. Acting alongside fellow teenager Owen Flowers, Jubair is accused of breaching corporate and government networks in the United States and the United Kingdom, including the U.S. Courts system and Transport for London, causing data breaches and operational disruptions. The group is known for leveraging social engineering techniques, such as impersonating employees to gain IT help desk access, and combining these methods with ransomware to extort victims. Evidence from seized servers indicated the theft of sensitive corporate and judicial data, including over a gigabyte from a New Jersey critical infrastructure company, and cryptocurrency ransoms totaling approximately $36 million, of which $8.4 million was allegedly transferred during FBI seizure.

The investigations reveal that Scattered Spider operates as a loosely organized cyber collective, sometimes referred to as "the Com," that blends digital attacks with real-world intimidation tactics, including swatting. Jubair's alleged actions included submitting fraudulent legal requests to financial institutions and accessing federal magistrate accounts to search for sealed indictments of other hackers, illustrating a sophisticated understanding of both technical and procedural vulnerabilities. The FBI's complaint highlights the group's ability to compromise critical infrastructure, enterprise networks, and government systems while exploiting gaps in operational security and human trust.

Strategically, the case underscores the evolving threat posed by young, highly skilled cybercriminals to national security and global financial systems. It demonstrates how low-barrier social engineering and ransomware-as-a-service platforms can enable massive-scale disruption and financial extraction. The U.S.-UK col-

laboration in apprehending these individuals reflects the necessity of international cooperation in cybercrime enforcement, while highlighting vulnerabilities in both public and private sector systems. The situation illustrates a broader trend in which adolescent hacker collectives are increasingly capable of conducting operations with cross-border implications, challenging traditional notions of cybersecurity defense, law enforcement jurisdiction, and financial system resilience.

Read more: https://techcrunch.com/2025/09/18/us-government-charges-british-teenager-accused-of-at-least-120-scattered-spider-hacks/?

Russian Federation & Ukraine

Ukraine claims cyberattacks on Russian election systems; Moscow confirms disruptions

Ukraine's military intelligence agency (HUR) has claimed responsibility for a series of cyberattacks against Russia's Central Election Commission (CEC), state services, and telecom infrastructure during Moscow's nationwide "unified voting day," which included elections in Russian-occupied regions of Ukraine. The operation employed distributed denial-of-service (DDoS) techniques, overwhelming servers with artificial traffic to temporarily paralyze Russia's electronic voting platforms, the Gosuslugi state portal, and routers operated by Rostelecom, the state-run telecom provider. Ukrainian officials stated the objective was to hinder online voting in illegally occupied territories, disrupting both the technical and symbolic conduct of the elections.

Russian authorities confirmed widespread disruptions, with CEC chair Ella Pamfilova acknowledging intermittent outages and reporting over 500,000 recorded attacks during the three-day election period. The Ministry of Digital Development described "short-term traffic degradation" but maintained that remote voting ultimately remained functional. Rostelecom confirmed its routers were overloaded and had to be rebooted, temporarily cutting access during peak hours. Moscow vowed to strengthen defensive measures ahead of parliamentary elections in 2026.

The cyber operation unfolded against the backdrop of geopolitical tensions, as Kyiv and Western governments condemned Russia's voting in occupied territories as illegal and illegitimate. Ukraine's Foreign Ministry called on allies to reject the results, while the European Union reiterated that it does not recognize the elections, citing violations of international law.

Strategically, the attacks demonstrate how cyber operations have become integral to modern hybrid warfare, complementing physical resistance on the battlefield with digital disruption aimed at undermining political legitimacy and state infrastructure. The targeting of election systems highlights the vulnerability of digital governance platforms to external interference, raising questions about resilience in authoritarian states heavily reliant on centralized digital services. The episode underscores how cyberspace remains a contested domain where states seek to challenge adversaries' political processes and legitimacy without direct kinetic escalation.

Read more: https://therecord.media/ukraine-claims-ddos-attack-russian-election-system

Gamaredon X Turla collab

In 2025, cybersecurity researchers identified the first confirmed collaboration between two Russian Federal Security Service (FSB)-linked advanced persistent threat (APT) groups—Gamaredon and Turla—targeting high-value networks in Ukraine. Gamaredon, historically focused on mass compromises of Ukrainian governmental institutions using spear-phishing and malicious LNK files, deployed tools such as PteroGraphin, PteroOdd, and PteroPaste to initially infiltrate systems. Turla, known for selective cyberespionage operations against high-profile government and diplomatic targets, then leveraged these footholds to deploy its Kazuar backdoor, enabling covert control and intelligence exfiltration from machines of strategic interest. Telemetry revealed that Gamaredon's widespread compromises acted as a conduit for Turla's precise targeting, with Turla limiting activity to a handful of sensitive systems while Gamaredon affected hundreds or thousands

of endpoints. Technical analysis showed that PteroGraphin was used to restart Kazuar on machines where it failed to launch, indicating a coordinated operational workflow. Both groups operate under distinct FSB centers—Gamaredon under Center 18 in Crimea and Turla under Center 16, the FSB's signals intelligence division—highlighting a formalized collaboration between different branches of Russia's intelligence apparatus. The collaboration illustrates a sophisticated hybrid attack model, combining mass-scale network compromise with selective espionage, enhancing both operational efficiency and strategic impact. The use of proprietary tooling and backdoors underscores significant technological capability and coordination, including leveraging preexisting intrusions to minimize detection and resource expenditure.

Strategically, this partnership reflects the evolving cyber threat landscape in the context of the Russia-Ukraine conflict, demonstrating how state-aligned actors can synchronize operations to maximize intelligence collection while limiting exposure. It also underscores broader trends in state-sponsored cyber operations: the blending of large-scale opportunistic intrusions with targeted espionage, the reuse of third-party infrastructures, and inter-agency collaboration within intelligence services. For national security, such developments indicate heightened risk to governmental and critical infrastructure networks, emphasizing the need for robust endpoint security, threat intelligence sharing, and cross-border cybersecurity cooperation to detect and mitigate multi-layered APT campaigns.

Read more: https://www.welivesecurity.com/en/eset-research/gamaredon-x-turla-collab/

Investigation finds Russian surveillance, sabotage ship near European undersea cables

Satellite intelligence has revealed the presence of Russia's Yantar, a surveillance and sabotage vessel operated by the secretive Directorate of Deep-Sea Research (GUGI), near vital European undersea cables. The ship, capable of intercepting communications, manipulating data flows, and planting explosives for potential disruption, has been detected in areas such as the Irish Sea and the Norway–Svalbard corridor. Its operations reflect Moscow's strategy of mapping and probing Western critical infrastructure, including energy and communication networks, to gain strategic leverage in potential conflicts.

This activity coincides with Russia's intensifying airspace violations against NATO members and broader espionage operations across Europe. Analysts warn that disabling undersea cables could cripple internet connectivity, military coordination, and energy distribution, eroding social cohesion and political will within Europe during crises. The presence of the Yantar underscores the vulnerability of maritime infrastructure in an era of hybrid warfare, where covert technological sabotage is increasingly integrated into statecraft. For NATO and the EU, the developments highlight the urgent need to strengthen maritime domain awareness, protect subsea networks, and prepare countermeasures against gray-zone tactics that blur the lines between peacetime operations and wartime aggression.

Read more: https://kyivindependent.com/investigation-finds-russian-sabotage-ship-near-european-undersea-cables-ft-reports/

West Asia

Afghanistan Goes Dark As Taliban Imposes Nationwide Communications Blackout

The Taliban has imposed a nationwide telecommunications blackout in Afghanistan, severing access to fiber-optic Internet and mobile networks across the country, effectively isolating it from global communications. The shutdown, which began on September 29, 2025, has disrupted flights, banking services, e-commerce, online education, and remote work, exacerbating Afghanistan's ongoing economic and humanitarian crises marked by widespread poverty, hunger, and unemployment. The Taliban justified the blackout as a measure to prevent "immorality," referencing concerns over pornography and online interactions between men and women, although critics contend the move is part of a broader crackdown on civil liberties, freedom of expression, and access to information.

Technically, the blackout involved disabling both public and private telecommunications infrastructure, including SIM card networks, broadband Internet lines, and mobile network operations, leaving residents dependent on foreign SIM cards or offline alternatives. Observers and watchdogs such as NetBlocks confirmed that the country experienced a near-total Internet outage, while Afghan journalists, educators, and business owners reported severe disruptions to daily operations, communications with family abroad, and economic activity. The United Nations Assistance Mission in Afghanistan (UNAMA) called for immediate restoration of communications, warning that prolonged isolation could deepen social, economic, and humanitarian hardships.

Strategically, the blackout illustrates the Taliban's capacity to control critical digital infrastructure and manipulate information flows, reflecting a broader trend in which authoritarian regimes leverage Internet shutdowns to consolidate power, suppress dissent, and restrict public access to knowledge. Nationally, the shutdown threatens economic stability and societal functionality, particularly affecting women and marginalized populations who rely on digital connectivity for education, work, and civic participation. Internationally, the move raises concerns about Afghanistan's isolation, complicating aid delivery, diplomatic engagement, and monitoring of human rights conditions, while highlighting the vulnerability of modern societies to state-imposed digital censorship as a tool of governance and repression.

Read more: https://www.rferl.org/a/taliban-internet-shutdown-afghanistan-2025/33544978.html

Malware & Vulnerabilities

Self-replicating worm "Shai-Hulud" rampant on the npm open-source registry, food for thought for supply chain attacks in Defence

A newly discovered self-replicating malware, dubbed "Shai-Hulud," has been spreading across the widely used npm open-source registry, raising serious concerns about software supply chain security, particularly for defense and critical infrastructure. Identified by researchers at ReversingLabs, the worm propagates by exploiting stolen authentication tokens and republishing infected packages under compromised developer accounts, enabling exponential spread within the ecosystem. The malware is primarily active on Linux and macOS environments, where it masquerades as legitimate packages, including those designed to mimic well-known cybersecurity providers like CrowdStrike, thereby increasing the likelihood of unsuspecting developers installing them.

The infection chain begins when a developer installs a malicious npm package containing a postinstall script that automatically executes on deployment. This script downloads and weaponizes TruffleHog, an open-source credential-scanning tool, to harvest sensitive secrets such as API keys and private tokens from local machines and code repositories. Leveraging any captured GitHub tokens, the worm then injects a malicious GitHub Actions workflow file named shai-hulud.yaml into the victim's repositories. This workflow establishes persistence, ensuring the malware re-executes with each future code push, continuously stealing new credentials and propagating the infection further. The worm's self-replicating nature allows it to scale rapidly across interconnected projects, creating a cascading effect throughout open-source ecosystems.

Strategically, the incident underscores the vulnerabilities inherent in open-source package registries and the potential exploitation of trusted developer ecosystems as attack vectors. For defense and national security sectors that increasingly rely on open-source code, the Shai-Hulud outbreak highlights the risks of supply chain compromise, where a single poisoned dependency can infiltrate critical systems. The ability of adversaries to weaponize developer workflows and credential-scanning tools points to a sophisticated evolution of cyber tradecraft, blurring the line between traditional malware and supply chain sabotage. This event serves as a warning that open-source ecosystems, while vital for innovation, represent a high-value target for both cybercriminals and state-backed actors seeking persistent access to sensitive environments.

Read more: https://claws.co.in/self-replicating-worm-shai-hulud-rampant-on-the-npm-open-source-registry-food-for-thought-for-supply-chain-attacks-in-defence/

French Advisory Sheds Light on Apple Spyware Activity

France's national cybersecurity agency, ANSSI, through its computer emergency response team (CERT-FR), has revealed new details about recent spyware campaigns targeting Apple device users, underscoring the persistent threat of state-linked surveillance operations. Apple has issued at least four notifications this year—on March 5, April 29, June 25, and September 3—warning individuals that their devices linked to iCloud accounts had been targeted and potentially compromised. These attacks are linked to advanced spyware families such as Pegasus, Predator, Graphite, and Triangulation, which exploit zero-day vulnerabilities requiring no user interaction and are notoriously difficult to detect. For instance, the September 3 alert coincided with Apple's disclosure of CVE-2025-43300, a flaw in its ImageIO framework exploited in "extremely sophisticated" attacks, while the March notification preceded disclosure of another WebKit zero-day, CVE-2025-24201.

CERT-FR explained that Apple's threat notifications arrive via iMessage, email, and iCloud alerts, though the gap between compromise attempts and notification may stretch across months, complicating timely remediation. The agency emphasized defensive measures such as enabling automatic updates, daily device restarts, and activating Lockdown Mode, designed to restrict vectors exploited by spyware. Notably, Apple has introduced a new defensive mechanism, Memory Integrity Enforcement (MIE), a hardware-level security architecture that hardens devices against memory safety vulnerabilities like buffer overflows and use-after-free bugs—common attack vectors leveraged by mercenary spyware across iOS, Android, and Windows platforms.

The disclosures highlight how mercenary spyware vendors continue to target journalists, activists, and political figures, posing both human rights and national security risks. Strategically, the revelations illustrate the escalating arms race between spyware developers and mobile ecosystem defenders, where rapid exploitation of zero-days challenges even leading vendors' patch cycles. For governments, the findings underscore the urgency of building resilience against commercially developed surveillance tools that blur the line between criminal tradecraft and state-sponsored espionage, reinforcing concerns about the systemic vulnerability of mobile platforms in global cybersecurity.

Read more: https://www.darkreading.com/vulnerabilities-threats/french-sheds-light-apple-spyware-activity?

Microsoft seizes 338 websites to disrupt rapidly growing 'RaccoonO365' phishing service

Microsoft's Digital Crimes Unit (DCU) has successfully disrupted RaccoonO365, a rapidly expanding phishing service targeting Microsoft 365 credentials, by seizing 338 associated websites under a U.S. court order from the Southern District of New York. RaccoonO365 operates as a subscription-based platform, enabling even low-skilled cybercriminals to deploy phishing campaigns that mimic official Microsoft communications, including branded emails and login portals, to harvest usernames and passwords. The service, tracked by Microsoft as Storm-2246, has been particularly effective because it automates credential collection, scales quickly, and continuously rotates domains to evade detection, putting millions of users and enterprise accounts at risk globally.

The takedown involved coordinated legal and technical measures, including court-authorized domain seizures that cut off the phishing kits' infrastructure and prevented further credential harvesting. Microsoft emphasized that despite the tool's accessibility, its impact is substantial, demonstrating how low-barrier cybercrime platforms can achieve widespread operational reach and threaten cloud-based productivity environments. The DCU also highlighted that these kits can be combined with social engineering and automated scripts to compromise enterprise networks, including email, document storage, and collaboration platforms central to corporate operations.

Strategically, the disruption of RaccoonO365 underscores the growing vulnerability of cloud ecosystems to

commoditized cybercrime and highlights the role of corporate-led cybersecurity enforcement in defending critical digital infrastructure. It also signals a trend in which cybercriminal services are increasingly packaged for subscription and resale, lowering entry barriers while magnifying potential harm. For national security and enterprise risk management, the case demonstrates the necessity of rapid threat intelligence sharing, robust authentication practices, and cross-sector collaboration to pre-empt large-scale credential compromise, particularly in cloud-first environments where compromised access can cascade into operational, financial, and reputational damage.

Read more: https://blogs.microsoft.com/on-the-issues/2025/09/16/microsoft-seizes-338-websites-to-disrupt-rapidly-growing-raccoono365-phishing-service/

China-linked hackers use 'BRICKSTORM' backdoor to steal IP

China-linked hackers identified as UNC5221 have launched an advanced cyber-espionage campaign using a new backdoor tool, BRICKSTORM, to target law firms, SaaS providers, and technology companies across the United States and allied nations. Security researchers from Google-owned Mandiant report that the operation, active since March 2025, focuses on stealing intellectual property and sensitive data, particularly from the email accounts of executives, developers, and administrators. BRICKSTORM is primarily deployed on Linux-based appliances, including VMware vCenter and ESXi hosts, which often lack endpoint detection and response coverage, enabling attackers to remain undetected for extended periods. The group has exploited zero-day vulnerabilities in Ivanti Connect Secure devices and leveraged stolen administrator credentials, suggesting access to automated decryption tools.

UNC5221 also uses compromised home and small office routers as an obfuscation network to mask command-and-control activity, complicating attribution and response. Mandiant observed that attackers maintained persistence by deploying BRICKSTORM even during active incident response investigations, highlighting their adaptability and monitoring capabilities. Though linked historically to Chinese state groups such as Silk Typhoon and Volt Typhoon, UNC5221 appears to operate with distinct methods and objectives aligned with Beijing's strategic interests in economic intelligence and national security. By infiltrating high-value organizations, the campaign not only exfiltrates data relevant to trade and policy but also establishes footholds that can facilitate broader exploitation of downstream customers and discovery of new zero-day vulnerabilities. This operation underscores the escalating sophistication of state-aligned Chinese cyber units, the vulnerabilities in overlooked enterprise systems, and the growing use of router-based botnets for covert operations. Strategically, the campaign reflects China's long-term focus on intellectual property theft and espionage, reinforcing tensions in the global cyber domain while raising urgent concerns for corporate security, supply chain resilience, and national defence.

Read more: https://therecord.media/china-linked-hackers-brickstorm-backdoor-ip?

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.

© All Rights Reserved 2025 Centre for Land Warfare Studies (CLAWS)

No part of this publication may be reproduced, copied, archived, retained or transmitted through print, speech or electronic media without prior written approval from C L A W S.

The views expressed and suggestions made are solely of the author in his personal capacity and do not have any official endorsement. Attributability of the contents lies purely with author.