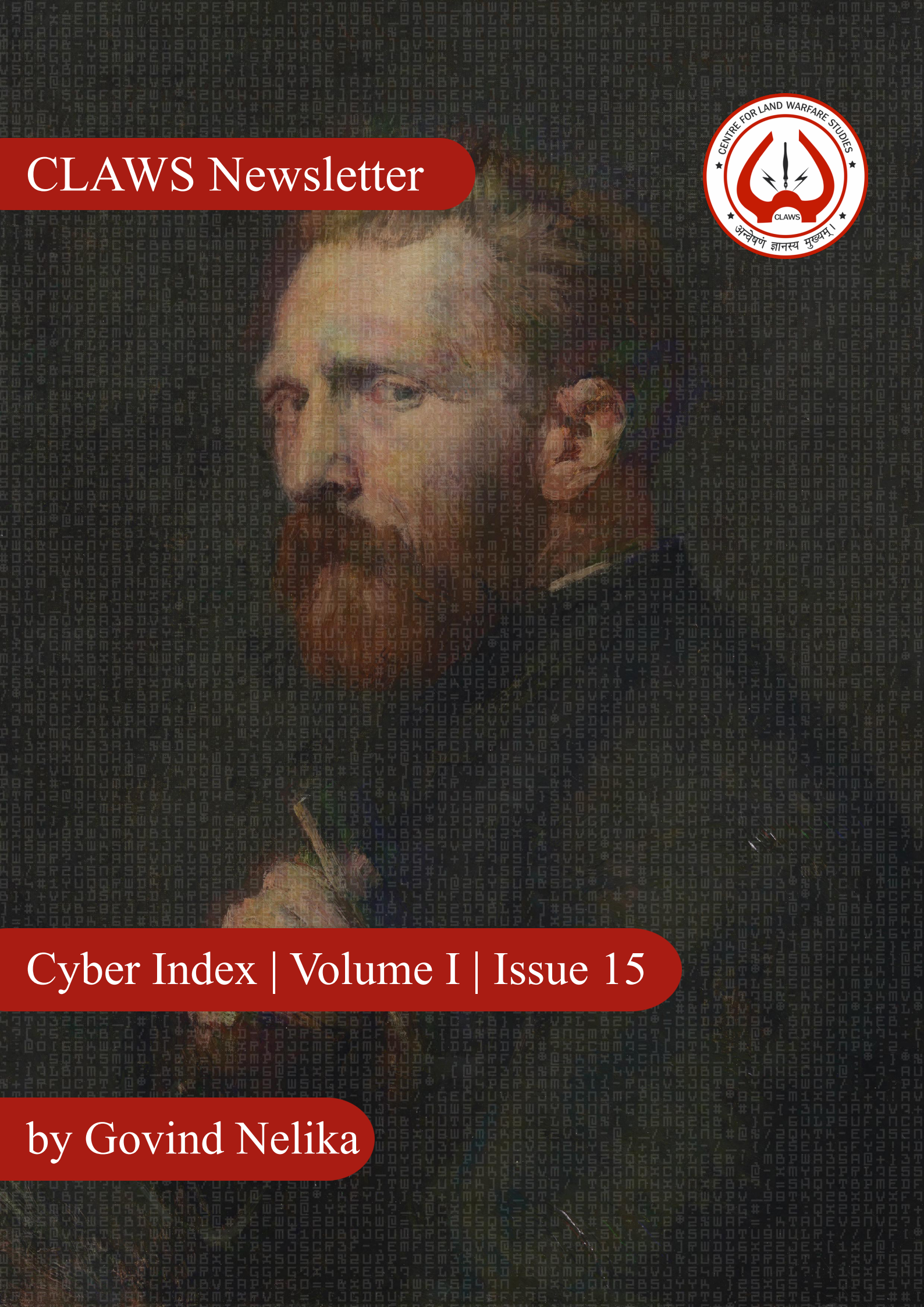
CLAWS Newsletter



Cyber Index | Volume I | Issue 15

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

Embrace chips, India, and skip those tech dreams

India is intensifying its drive to build a domestic semiconductor industry, with the government allocating more than $10 billion in subsidies since 2022 and preparing to double that amount. Prime Minister Narendra Modi has pledged that India will secure a "significant share" of a market projected to exceed $1 trillion, positioning the country as a "full-stack semiconductor nation." Initial successes include the production of chips developed by India's space program for satellites and missiles, though these use 180-nanometer technology—mature by global standards, with Taiwan's TSMC now advancing toward 2-nanometer production. Current government-backed projects include plans for 28-nm fabrication at CG Power & Industrial Solutions in Gujarat and nine additional plants involving partners from Japan, Taiwan, the U.S., and Israel.

The broader context reflects both economic ambition and national security concerns. The primary goal is not competing in cutting-edge AI processors or advanced mobile chips, where East Asian firms dominate, but ensuring supply-chain resilience for critical domestic industries such as automobiles, household electronics, and defense systems. Mature node chips, though less profitable than advanced processors, remain vital for most industrial applications and can provide India with strategic autonomy should global disruptions—such as geopolitical conflicts or export controls—cut off supplies. Analysts caution that chasing advanced fabrication below 16 nm could divert scarce resources and delay progress in building a robust mid-range manufacturing base. Strategically, India's approach illustrates a balancing act between aspiration and pragmatism: by prioritizing legacy technologies, the country can secure its manufacturing ecosystem, build workforce expertise, and strengthen economic sovereignty, while gradually positioning itself to enter higher-value segments over the long term. This effort aligns with broader global trends of semiconductor nationalism, where states seek to localize production capacity to mitigate vulnerabilities exposed by the pandemic and ongoing U.S.-China technology competition.

Read more: https://economictimes.indiatimes.com/industry/cons-products/electronics/embrace-chips-india-and-skip-those-tech-dreams/articleshow/123842412.cms?from=mdr

DoD R&E chief says Pentagon will trim 'critical technology' list

The U.S. Department of Defence (DoD) is moving to streamline its list of "critical technologies," a framework originally set at 14 priority areas under former Under Secretary of Defence for Research and Engineering Heidi Shyu in 2023. Emil Michael, the current head of Research and Engineering, announced that the Pentagon will trim the list to emphasize only the domains considered truly essential to national defence. While he did not reveal exact numbers, he confirmed that high-priority areas such as artificial intelligence, directed energy, and hypersonic will remain central. Michael explained that this approach prevents unchecked expansion of the list, which risks diluting focus and resources. The changes coincide with an organizational shift that places the Chief Digital & AI Office (CDAO) under Research and Engineering, a move designed to give the office greater institutional authority and closer ties to private-sector innovators in artificial intelligence and large language models. Emphasis was also placed on cost-effective solutions: for example, developing directed energy systems as lower-cost air defence alternatives compared to traditional missile interceptors.

At the same time, the department is working to expand and diversify its defence industrial base, ensuring that both hardware and software suppliers are more robustly engaged in delivering emerging capabilities. The strategic implication of this realignment is a sharper focus on depth rather than breadth, concentrating resources in areas where adversaries such as China are investing heavily, and where rapid fielding could decisively affect deterrence and warfighting effectiveness.

Therefore by trimming the technology priorities and strengthening industry partnerships, the DoD is signalling a shift toward pragmatic innovation balancing cutting-edge research with affordability, scalability, and

industrial resilience positioning the U.S. to remain competitive in the accelerating global technology race.

Read more: https://breakingdefence.com/2025/08/dod-re-chief-says-pentagon-will-trim-critical-technology-list/?

ASML, Mistral AI Enter Strategic Partnership

ASML Holding NV, the world's leading semiconductor equipment manufacturer, and French artificial intelligence company Mistral AI have announced a strategic partnership aimed at integrating advanced AI models into semiconductor design, manufacturing, and operational processes. This collaboration, formalized through a long-term agreement, positions ASML as the lead investor in Mistral AI's €1.3 billion Series C funding round, granting the Dutch firm an 11 percent equity stake. The initiative reflects growing convergence between semiconductor manufacturing and artificial intelligence, as ASML seeks to leverage Mistral's frontier AI expertise to enhance the performance, speed, and efficiency of its holistic lithography systems, which are central to global chip production. Beyond capital investment, the agreement includes provisions for joint research efforts, with a focus on accelerating product development cycles and addressing emerging technological opportunities in both the AI and semiconductor ecosystems.

ASML will also secure a seat on Mistral AI's Strategic Committee, enabling direct influence over the company's future strategy and technological roadmap. The deal underscores the geopolitical and economic stakes surrounding semiconductor and AI supply chains, with Europe seeking to reduce reliance on foreign technology providers and strengthen its competitiveness in critical digital infrastructure. For ASML, the partnership offers a pathway to sustain its technological edge amid intensifying global competition in chipmaking, while for Mistral AI, the collaboration enhances credibility, resources, and market positioning against established AI players. Strategically, the alliance highlights a broader trend of cross-sector integration between AI innovators and semiconductor leaders, signaling that future breakthroughs in chip performance will increasingly depend on AI-driven optimization. At a time of mounting geopolitical rivalry over advanced technologies, the partnership carries implications not only for industrial competitiveness but also for national security, as the fusion of AI and semiconductor capabilities becomes central to defense, economic resilience, and global technological leadership.

Read more: https://www.asml.com/en/news/press-releases/2025/asml-mistral-ai-enter-strategic-partnership

Hackers threaten to turn stolen art into AI training data

A newly identified ransomware group called LunaLock has launched an extortion campaign targeting digital art communities, most notably the art-platform Artists&Clients. LunaLock claims to have breached and encrypted data on that platform including artwork, source code, and user personal data and is demanding a US$50,000 ransom to decrypt the data, delete stolen files, and avert further damage.

What sets this case apart is LunaLock's novel threat: if the ransom is not paid, the group says it will not only leak the stolen data but also submit all the artwork to AI companies for use in their training datasets. This combines traditional ransomware tactics (encryption + leak threats) with a kind of "AI extortion" leveraging concerns about intellectual property, model training consent, and irrevocable use of creative work in large language/image models.

The attack was publicly declared via a Tor-based leak site. The platform was said to be compromised around August 30, 2025. LunaLock's communication includes a warning to users to pressure the site owners to meet the demand, otherwise art and personal data will be exposed and used in AI datasets. LunaLock's ransom demand may be payable in cryptocurrency (Bitcoin or Monero) according to some sources.

This operation reflects growing tensions around AI, copyright, and data privacy. For artists and platforms, it raises the risk that stolen work could end up embedded in AI training models, from which removal is

difficult or impossible. It also sets a precedent for extortionists exploiting both the legal and ethical ambiguity around AI training. Broader implications include pressure on platforms to defend creative IP more aggressively, potential legal and regulatory fallout (e.g. under data protection laws), and an incentive for new protective tools. Already, some tools (e.g. Glaze and Nightshade) exist to subtly alter artworks to disrupt unauthorized training of AI models.

In sum, LunaLock's approach marks an escalation in ransomware strategy: it blends data theft, encryption, public exposure, and the irreversible dimension of AI model training as levers for coercion. The case highlights how creative sectors are now in the crosshairs of cybercrime, especially where AI is concerned, and underlines the need for both technical safeguards and legal regimes that protect intellectual property and data rights in the AI era.

Read more: https://www.politico.com/newsletters/weekly-cybersecurity/2025/09/08/hackers-threaten-to-turn-stolen-art-into-ai-training-data-00549940

China's chip startups are racing to replace Nvidia

China's technology sector is accelerating efforts to develop domestic alternatives to U.S.-made advanced chips as American export restrictions tighten access to Nvidia's high-performance GPUs. The push is led by a mix of state-backed enterprises, private startups, and major firms like Huawei, Baidu, and Alibaba, all aiming to reduce reliance on foreign suppliers critical for training large-scale artificial intelligence models. A growing number of Chinese chip designers—including Cambricon, Moore Threads, Biren Technology, MetaX, Enflame, and Hygon—are racing to fill the gap, with some drawing on ex-Nvidia and AMD talent. These companies are attracting heavy investor interest, forming alliances with AI developers, and preparing IPOs to secure funding for costly research and development. Several firms, such as Cambricon and Biren, have unveiled GPUs modeled after Nvidia's A100 and H100, while Moore Threads claims its processors can already run large Chinese models like DeepSeek and Qwen. Yet, the path forward is fraught with challenges: most startups are loss-making, many face U.S. blacklisting that blocks access to Taiwan Semiconductor Manufacturing Company (TSMC), and their customer base is largely limited to state-owned enterprises. Meanwhile, tech giants like Baidu and Alibaba are deploying homegrown chips in massive data centers, while Huawei remains the strongest player in the sector.

The broader context is a deepening technological rivalry between Washington and Beijing, where semiconductors are a strategic battleground with national security and economic implications. If China succeeds in creating a competitive domestic chip ecosystem, it could blunt the impact of U.S. controls, safeguard its AI development trajectory, and reduce a critical vulnerability in its supply chain. However, consolidation is expected, with analysts predicting that only a handful of firms will survive long-term. This race underscores how export restrictions are reshaping global chip competition, fuelling both innovation and fragmentation in the semiconductor industry.

Read more: https://restofworld.org/2025/china-chip-startups-nvidia-us-export/?

United States of America (USA)

SECNAV Phelan Wants New Positions to Accelerate Navy Unmanned Programs

The U.S. Navy (Department of the Navy, DON), under Secretary John Phelan, has initiated a sweeping reorganization to accelerate its unmanned, robotic, and autonomous systems (RAS) programs. The key actors include Phelan himself, the Office of the Assistant Secretary of the Navy for Research, Development and Acquisition (RD&A), the Program Executive Office (PEO), and other leadership offices across the Navy and Marine Corps.

Contextually, this move addresses long-standing fragmentation in how unmanned systems are managed portfolio and acquisition authorities are currently scattered across multiple commands and offices, slowing down

development, procurement, integration, and deployment. Great power competition, threats in contested maritime domains, and the increasing importance of autonomous platforms in future naval warfare are major drivers.

Specifically, a memo dated September 3 orders creation of three new senior positions: a Deputy Assistant Secretary of the Navy for RAS; a Program Executive Office for RAS; and a Portfolio Acquisition Executive for RAS. These roles are intended to unify oversight, streamline requirements, contracting, cybersecurity authorities, and systems commands for RAS. Alongside, there is a 30-day "sprint" led by the principal military deputy in RD&A, tasked to deliver an implementation plan within that window. During this period, all RAS-related acquisition decisions and contracting actions—including awards and modifications—are paused unless explicitly approved by the designated acquisition executive. The plan must propose a transition schedule, a proposed organizational chart, proposal for consolidating program elements into fewer "cohesive" portfolios, optimal geography for organizations, and address talent/billet requirements. The goal is to have the new leadership offices reach initial operational capacity within 90 days.

Strategically, this reorganization reflects the Navy's assessment that unmanned/autonomous systems are no longer experimental add-ons but foundational to "hybrid fleet" concepts of manned plus unmanned platforms enabled by AI and autonomy. By centralizing authority and clarifying responsibility, the DON hopes to increase speed, reduce duplication, improve cybersecurity oversight, and deliver more capable systems in contested environments. Internationally and for national security, this fits broader trends where military forces are institutionalizing autonomy and robotics to maintain technology edge, respond more quickly to threats, and shift doctrine toward distributed, unmanned capabilities in contested, maritime, and multi-domain operations.

Read more: https://news.usni.org/2025/09/04/secnav-phelan-wants-new-positions-to-accelerate-navy-unmanned-programs

Trump to host tech CEOs for first event in newly renovated Rose Garden

U.S. President Donald Trump convened more than two dozen top technology and business executives for a high-profile dinner in the newly renovated White House Rose Garden, marking a significant moment of engagement between his administration and the tech sector. Attendees included Mark Zuckerberg of Meta, Tim Cook of Apple, Bill Gates, Sam Altman of OpenAI, Sundar Pichai of Google, Safra Catz of Oracle, and Lisa Su of AMD, highlighting a cross-section of leaders from artificial intelligence, enterprise software, cloud computing, and semiconductors. Elon Musk was invited but did not attend personally, instead sending a representative. The event comes at a time when the relationship between Washington and Silicon Valley is being reshaped. Following Trump's 2024 election victory, many technology leaders have begun recalibrating their positions on issues such as regulation, antitrust scrutiny, AI governance, immigration, and diversity programs to align more closely with administration priorities. The dinner also followed a separate White House AI-focused event hosted by First Lady Melania Trump, underscoring the administration's strong interest in shaping policy discussions around emerging technologies.

The venue itself carried symbolic significance, as the Rose Garden was recently redesigned with a stone patio and umbrella-covered tables modeled after Trump's Mar-a-Lago resort, signaling a shift in how the space is used for state and industry engagement. Strategically, the gathering reflects the White House's recognition that technological leadership—particularly in AI and advanced computing—is central to U.S. national security and economic competitiveness, especially amid intensifying rivalry with China.By bringing leading tech figures into closer dialogue, the administration appears to be consolidating industry support to influence regulation, workforce policy, and innovation incentives. This development fits a broader global trend in which governments are forging closer ties with technology companies, acknowledging their pivotal role in shaping future industrial, economic, and geopolitical landscapes.

Read more: https://www.reuters.com/business/autos-transportation/trump-host-tech-ceos-first-event-newly-

renovated-rose-garden-2025-09-04/

US probes malware email targeting trade talks with China, WSJ reports

U.S. authorities are investigating a suspected cyber-espionage operation linked to China that targeted American trade discussions with Beijing. The campaign involved a malware-laden email spoofed to appear as if sent by Representative John Moolenaar, a Republican lawmaker and chair of a congressional committee on strategic competition with China. The phishing message, distributed in July, was directed at U.S. trade groups, law firms, and government agencies and contained an attachment posing as draft legislation. Cybersecurity analysts traced the malware to APT41, a hacker group with documented ties to Chinese intelligence, whose past operations have combined espionage with financially motivated intrusions. If opened, the attachment could have provided extensive unauthorized access to the recipients' networks, potentially exposing recommendations to the White House ahead of sensitive trade talks. The timing coincided with U.S.-China negotiations in Sweden that produced a temporary tariff truce, raising concerns the operation sought to give Beijing insights into Washington's bargaining position.

The FBI confirmed awareness of the incident and is coordinating with partner agencies, while the U.S. Capitol Police launched an investigation after staff noticed unusual inquiries about the email. Moolenaar denounced the attack as part of Beijing's broader strategy to undermine U.S. national security and influence trade policy. The Chinese embassy in Washington denied involvement, stating that China opposes cyberattacks and warning against attributing blame without evidence. Strategically, the attempted intrusion highlights how trade negotiations, alongside military and technology disputes, have become prime targets of state-sponsored cyber activity in an era of intensifying U.S.-China rivalry. By exploiting trust in a known lawmaker and embedding malware in seemingly routine legislative documents, the operation reflects a broader trend in which adversarial states deploy advanced persistent threat groups to infiltrate policymaking circles, gather intelligence, and potentially shape the geopolitical balance in ongoing economic conflicts.

Read more: https://www.reuters.com/world/us/us-probes-malware-email-targeting-trade-talks-with-china-wsj-reports-2025-09-07/

Commonwealth of Australia

Australia emerges as quantum computing player with role in Microsoft chip

Australia is emerging as a significant player in the global quantum computing landscape, notably through its collaboration with Microsoft on the development of the Majorana 1 quantum processor. This processor, unveiled in early 2025, is the first to utilize topological qubits, a novel approach that promises enhanced stability and scalability in quantum computing. Researchers from the University of Sydney, led by physicist David Reilly, played a pivotal role in this advancement, contributing to the design and fabrication of the chip. Their involvement underscores Australia's growing expertise and influence in quantum technologies.

The Australian government's strategic investments have been instrumental in fostering this sector. Since the 1990s, sustained funding has supported academic research and infrastructure development, such as the establishment of the A$150 million Sydney Nanoscience Hub. These initiatives have cultivated a robust ecosystem of startups and research institutions, positioning Australia as a hub for quantum innovation. Notable companies like Emergence Quantum, Diraq, and Q-CTRL are gaining international recognition, with some securing defense contracts from the United States.

This collaboration with Microsoft highlights Australia's strategic role in the quantum computing arena, challenging the perception of exclusive U.S. dominance in this field. As nations vie for leadership in emerging technologies, Australia's contributions to the Majorana 1 processor exemplify its growing influence and potential to shape the future of quantum computing.

Read more: https://www.msn.com/en-gb/money/technology/australia-emerges-as-quantum-computing-play-

er-with-role-in-microsoft-chip/ar-AA1MvfDC

People's Republic of China (PRC) | China

Cyberport may use Chinese GPUs at Hong Kong supercomputing hub to cut reliance on Nvidia

Hong Kong's government-run Cyberport is exploring the integration of Chinese-made graphics processing units (GPUs) into its Artificial Intelligence Supercomputing Centre to reduce dependence on U.S.-sourced Nvidia chips amid escalating China-U.S. geopolitical tensions. Key actors include Cyberport CEO Rocky Cheng Chung-ngam, four unnamed mainland Chinese GPU manufacturers, and Nvidia as the incumbent supplier. Since its launch in December 2024, Cyberport's facility has deployed Nvidia H800 GPUs, delivering 1,300 petaflops of computing power, with plans to expand to 3,000 petaflops by the end of 2025. The initiative to test Chinese GPUs reflects strategic considerations around supply chain resilience and diversification, as reliance on U.S. semiconductor technology has become a potential vulnerability given export restrictions and diplomatic frictions.

Technically, Cyberport purchased four GPUs from different Chinese vendors and is conducting performance benchmarking at its AI lab to evaluate which models meet operational requirements for high-performance AI workloads. Preliminary testing indicates that all four Chinese GPUs deliver performance comparable to Nvidia's H800, though cost considerations are expected to influence final procurement decisions. The evaluation process involves benchmarking AI training and inference tasks, monitoring thermal efficiency, and assessing integration with existing software frameworks and supercomputing infrastructure.

Strategically, adopting Chinese GPUs would allow Hong Kong to mitigate exposure to U.S. export controls while simultaneously fostering ties with mainland Chinese semiconductor manufacturers. This shift aligns with a broader trend among Asian research and industrial hubs seeking to balance technological sovereignty with access to global innovation ecosystems. The move also underscores the rising geopolitical dimension of advanced computing infrastructure, where decisions about processor sourcing are increasingly influenced by national security, economic resilience, and cross-border technological competition, particularly in AI-driven sectors that underpin both commercial and defence applications.

Read more: https://www.scmp.com/tech/article/3325469/cyberport-may-use-chinese-gpus-hong-kong-supercomputing-hub-cut-reliance-nvidia?

How China's military surged ahead in tech by firing up competition among suppliers

China's military modernization has accelerated through a deliberate strategy of fostering competition between state-owned defense conglomerates and private technology firms, significantly advancing the country's weapons and unmanned systems capabilities. Key actors include major state-backed entities, private defense contractors, universities, and research institutes operating under Beijing's military-civil fusion strategy, which integrates commercial innovation into military research. This approach has produced a diverse array of systems, including at least five nuclear-capable missiles—three capable of reaching the continental United States, a submarine-launched ballistic missile, and a long-range air-launched missile—alongside advanced unmanned aerial vehicles (UAVs) ranging from reconnaissance-strike drones to "loyal wingman" and fighter-like combat drones. Most of these systems were unveiled during a high-profile military parade in Beijing, illustrating both operational readiness and technological maturity.

Technologically, China's UAV sector demonstrates extensive experimentation, leveraging multiple configurations, advanced autonomy, and next-generation propulsion and sensor technologies. The interplay between state and private entities has fostered rapid iteration, lower development costs, and accelerated deployment timelines. Universities and research institutes provide specialized expertise, while the private sector injects flexibility and market-driven innovation. Traditional state-owned firms continue to anchor large-scale weapons development, ensuring strategic oversight and alignment with national objectives.

Strategically, this competitive ecosystem has strengthened China's capacity to project power, enhance deterrence, and expand operational flexibility across multiple domains, including nuclear, air, and unmanned systems. By combining state control with private-sector dynamism, Beijing is rapidly closing technological gaps with global military leaders, signaling a shift in the balance of military-industrial power. Internationally, this trend underscores the rising importance of hybrid innovation models in defense modernization, where competition among suppliers accelerates technological advancement while reinforcing national security objectives, potentially altering regional and global strategic calculations in the Indo-Pacific and beyond.

Read more: https://www.scmp.com/news/china/military/article/3324640/how-chinas-military-surged-ahead-tech-firing-competition-among-suppliers?

Walling Off China

The United States' strategy to curb China's technological rise, particularly in artificial intelligence and advanced semiconductors, has experienced a significant reversal amid evolving geopolitical and economic considerations. The primary actors include the U.S. federal government—specifically the Commerce Department's Bureau of Industry and Security (BIS), the White House, and national security officials—as well as major U.S. tech corporations like Nvidia and Advanced Micro Devices (AMD), with China as the targeted state. Initially, under both the Trump and Biden administrations, the U.S. implemented stringent export controls on high-performance AI chips such as Nvidia's A100 and H100, aiming to preserve American supremacy in AI and related military, intelligence, and economic domains. These controls relied on cooperation from key semiconductor-producing allies, including Japan and the Netherlands, and were reinforced following heightened tensions around events such as Nancy Pelosi's 2022 visit to Taiwan, which Beijing met with aggressive military posturing.

Technically, the controls restricted sales of cutting-edge GPUs and chipmaking equipment critical for AI development, effectively delaying China's access to frontier computing capabilities. These restrictions were intended to maintain a generational lead in AI hardware, which U.S. officials viewed as essential for sustaining technological and strategic advantages. However, in 2025, the U.S. administration reversed certain prohibitions, allowing sales of Nvidia H20 and AMD MI308 chips to China in exchange for negotiated concessions, signaling a shift from a strictly containment-focused strategy to a transactional approach. Analysts warn this may accelerate China's AI development, as access to high-end hardware addresses one of its key bottlenecks, potentially enabling rapid domestic advancement in AI capabilities.

Strategically, this pivot underscores the challenges of enforcing technological containment in a globally integrated semiconductor supply chain and the tension between national security imperatives and economic or diplomatic incentives. The episode illustrates the fragility of U.S. export controls as a tool to maintain AI dominance and reflects broader trends in which advanced technologies are increasingly central to geopolitical competition, trade policy, and national security planning, highlighting the ongoing complexity of U.S.-China technology rivalry.

Read more: https://www.thewirechina.com/2025/09/07/walling-off-china/?

Republic of China (ROC) | Taiwan

Taiwan signs MOU on drone cooperation with Poland, Ukraine

Taiwan's defence industry has formalized a new partnership with Ukraine and Poland through the signing of a memorandum of understanding (MOU) focused on cooperation in unmanned aerial vehicle (UAV) technology. The agreement was concluded during the International Defence Industry Exhibition (MSPO) in Kielce, Poland, one of Europe's largest defence expos. Under the terms of the MOU, Taiwan will contribute technological expertise and components, Ukraine will provide research and development capacity, and Poland will share its operational experience and industrial know-how. The Taiwanese delegation, led by Taiwan Defence

Industry Development Association President Tony Hsu and comprising representatives from about 20 defence firms—including members of the Thunder Tiger Group and the Taiwan Excellence Drone International Business Opportunities Alliance—underscored the country's intent to strengthen its role in international defence supply chains. Ukrainian participation was represented by the Lviv Tech Cluster, while Polish involvement came through the Taiwan-Poland Chamber of Commerce.

The initiative highlights the increasing importance of drone technology in modern warfare, with Ukraine's battlefield experience against Russia providing unique insights into UAV applications, and Poland emerging as a key NATO logistics and defence hub. By linking Taiwan's advanced manufacturing capabilities with European partners' practical expertise, the cooperation is expected to boost industrial capacity, deepen defence-technology exchanges, and strengthen trilateral security collaboration. Strategically, the partnership reflects Taiwan's efforts to expand its defence diplomacy beyond traditional U.S. and East Asian partners, securing footholds in Europe where military innovation and geopolitical tensions are intensifying. It also signals a broader international trend toward cross-border defence-industrial integration, particularly in drone and autonomous systems, which are rapidly reshaping military doctrines and national security planning worldwide.

Read more: https://www.taipeitimes.com/News/taiwan/archives/2025/09/04/2003843227?

European Union | EU

EU says von der Leyen's plane GPS system was jammed, Russian interference suspected

The European Union has accused Russia of jamming the GPS system of European Commission President Ursula von der Leyen's aircraft during a flight to Bulgaria, an incident that underscores the escalating contest between Moscow and Brussels over security in Eastern Europe. The disruption occurred as the plane approached the southern Bulgarian city of Plovdiv, forcing air traffic controllers to rely on ground-based navigation systems to ensure a safe landing. Bulgarian authorities linked the interference to Russian activity, although it remains unclear whether von der Leyen's aircraft was specifically targeted. GPS jamming works by emitting powerful ground-based signals that overpower weaker satellite transmissions, potentially creating dangerous conditions during approaches or departures. This episode follows earlier accusations by Estonia that Russia had disrupted GPS navigation in the Baltic region, with Finnair flights diverted after losing positional accuracy.

EU officials stressed that the incident highlights the growing threat of electronic warfare, particularly as von der Leyen toured frontline states bordering Russia, Belarus, and the Black Sea to demonstrate support for Ukraine after more than three years of war. In response, EU Defence Commissioner Andrius Kubilius announced plans to expand the bloc's network of low-orbit satellites to better detect and counter interference. Strategically, the incident reinforces European resolve to strengthen defence capabilities, reduce vulnerabilities in critical infrastructure, and accelerate military investment. More broadly, it signals Russia's willingness to employ hybrid tactics—including electronic disruption—to challenge EU mobility and deterrence in contested regions. If sustained, such activity risks undermining aviation safety, destabilizing confidence in navigation systems, and complicating civilian and military operations near NATO's eastern flank, deepening the confrontation between Moscow and Western institutions.

Read more: https://www.reuters.com/world/europe/eu-says-von-der-leyens-plane-gps-system-was-jammed-russian-interference-2025-09-01/

APT28 Campaign Targeting Polish Government Institutions

Poland's national cybersecurity agencies, CERT Polska (CSIRT NASK) and CSIRT MON, uncovered a coordinated malware campaign targeting Polish government institutions, attributed to APT28, a cyber-espionage group linked to Russia's GRU. The operation relied on highly tailored phishing emails crafted to provoke curiosity, such as messages about alleged scandals involving Polish and Ukrainian officials. Victims were lured

to links hosted on legitimate free services like run.mocky.io and webhook.site, which redirected users to malicious payloads while masking detection. Attackers used a ZIP archive disguised as images, containing a fake executable (.jpg.exe), a hidden batch script, and a malicious DLL. The technique exploited DLL side-loading, where the disguised calculator app triggered the execution of a substitute WindowsCodecs.dll, which in turn launched a malicious BAT script. This chain executed browser-based commands that fetched further payloads while showing real photos to maintain credibility. Subsequent scripts employed obfuscation, registry manipulation, and repeated downloads to ensure persistence, while also concealing malicious processes within legitimate Microsoft Edge operations.

This campaign highlights how state-backed threat actors increasingly exploit commonly used developer and IT tools to evade detection while minimizing operational costs, a tactic observed across multiple advanced persistent threat (APT) groups. By leveraging familiar services and disguising malware within everyday file types, attackers increase the likelihood of bypassing defences and deceiving targets. Strategically, the incident underscores Russia's continued reliance on cyber operations to weaken European governments, disrupt decision-making, and gather intelligence amid broader geopolitical tensions. For Poland, a NATO and EU frontline state, the intrusion attempts reaffirm its position as a priority target in Russia's hybrid warfare strategy. More broadly, the campaign illustrates the evolving sophistication of cyber-espionage, where technical deception, social engineering, and operational blending converge, posing persistent threats not only to national security institutions but also to the integrity of Europe's wider defence and political infrastructure.

Read more: https://cert.pl/en/posts/2024/05/apt28-campaign/

European Court Backs Transatlantic Data Pact — For Now

The European Union's General Court has upheld the US–EU Data Privacy Framework, a transatlantic accord allowing the transfer of personal data between the two regions, rejecting a French challenge that sought to overturn it. The framework, adopted in 2023, is critical to the functioning of global digital commerce, covering everything from email services and cloud storage to hotel bookings and artificial intelligence training. More than 2,800 American firms, including major tech companies, rely on this system to process European data. Without it, businesses would face costly and legally fragile alternatives such as contractual clauses, disrupting trade worth hundreds of billions of euros annually.

The court's ruling addressed concerns that U.S. surveillance laws permit excessive access to Europeans' data. It found that the creation of the U.S. Data Protection Review Court provided sufficient safeguards by limiting executive interference and requiring judicial oversight of bulk collection. Still, critics, including French MEP Philippe Latombe and Austrian activist Max Schrems, argue the framework rests on shaky ground, pointing to the review court's ties to the Department of Justice and recent U.S. political decisions, such as the removal of oversight board members, as evidence of weak protections.

The ruling temporarily stabilizes a transatlantic system that has twice before collapsed under European Court of Justice scrutiny, in the Schrems I (2015) and Schrems II (2020) cases that invalidated earlier agreements. Strategically, the decision preserves critical data flows underpinning the global digital economy, while also buying time for Washington and Brussels to demonstrate that the United States can provide "essentially equivalent" privacy protections to those in Europe. However, with a possible appeal to the EU's highest court and a 2027 review looming, the framework's long-term survival remains uncertain, keeping transatlantic digital relations on a fragile foundation.

Read more: https://cepa.org/article/european-court-backs-transatlantic-data-pact-for-now/

Republic of Korea | South Korea

South Korea to bolster cybersecurity measures against hacking, disinformation

South Korea's National Security Council, in coordination with the National Intelligence Service, the Ministry of National Defence, the Ministry of Science and ICT, the police, and the Ministry of Foreign Affairs, has unveiled a National Cybersecurity Basic Plan that marks a decisive step in addressing intensifying cyber threats, with a particular focus on state-backed operations linked to North Korea. The plan responds to a pattern of hostile cyber activity that includes large-scale cryptocurrency thefts used to finance Pyongyang's nuclear and missile programs, intrusions into South Korean defence contractors aimed at acquiring sensitive military technologies, and disinformation campaigns designed to destabilize public opinion and weaken democratic institutions. Central to the initiative is a transition toward an active cyber defence posture, allowing for proactive and potentially retaliatory measures to deter malicious actors, while simultaneously reinforcing the resilience of domestic systems.

On the technical front, the strategy calls for the deployment of artificial intelligence-driven monitoring and response capabilities capable of detecting abnormal behaviour in real time, as well as the segmentation of networks to ensure that critical national and public systems are securely separated from general internet access points, thereby creating a multi-layered defence architecture. In addition to these protective measures, the government has emphasized the need to systematically counter the spread of disinformation and foreign influence operations, recognizing that psychological and informational vulnerabilities can be as damaging to national security as direct intrusions into infrastructure. Beyond the domestic scope, Seoul has pledged to deepen its cooperation with democratic allies on cybersecurity matters and to actively participate in shaping international rules and norms for responsible behaviour in cyberspace, aligning itself with broader efforts to strengthen global governance in the digital domain.

Taken together, the plan underscores the strategic recognition that cyber warfare has become a core instrument of statecraft, one that threatens not only national defence but also economic stability and social cohesion, and it positions South Korea to respond with a comprehensive, technologically advanced, and internationally coordinated approach that mirrors the wider global trend of integrating offensive, defensive, and normative dimensions into national cyber strategies.

Read more: https://en.yna.co.kr/view/AEN20240901001900315

Russian Federation & Ukraine

Ukraine's cyber chief on Russian hackers' shifting tactics, US cyber aid

Ukraine's State Service of Special Communications and Information Protection (SSSCIP), led by Brigadier General Oleksandr Potii, is intensifying defenses against persistent Russian cyber operations that run parallel to the ongoing war. Since the 2022 invasion, Ukraine has endured thousands of attacks, but recent statistics highlight a marked decline in large-scale "critical" incidents, dropping from over 1,000 in 2022 to 367 in 2023 and just 59 in 2024. This reduction reflects both improved defensive capacity and the higher costs Russia now faces in mounting complex campaigns. Rather than large-scale disruptions, Moscow's tactics have increasingly shifted toward espionage, data theft, and distributed denial-of-service attacks aimed at undermining institutions, stealing intelligence, and preparing potential strikes on energy infrastructure ahead of winter. Ukraine's Computer Emergency Response Team actively tracks around 80 hacker groups, cataloging their methods to anticipate future threats, while simultaneously hardening critical systems against novel attack vectors.

International partnerships form the backbone of Ukraine's resilience, with Kyiv closely collaborating with European allies and U.S. agencies such as the Cybersecurity and Infrastructure Security Agency (CISA). These partnerships are reciprocal, with Ukraine benefiting from advanced tools and training while providing allies with unique, real-time insights into Russian tactics that could later be deployed against Western systems. Despite leadership turnover within SSSCIP, institutional capacity has steadily expanded, enabling consistent threat monitoring and rapid response. However, Russia's demonstrated ability to engineer new cyber tools—such as those deployed in disruptive strikes on Ukraine's railway system—illustrates the persistent danger and adaptability of its hackers. Strategically, Ukraine's experience underscores how cyber conflict has become a

permanent battlefield in modern warfare, where state-backed actors not only seek to paralyze infrastructure and exfiltrate intelligence but also refine capabilities for use beyond Ukraine, making its defenses an essential pillar of global cybersecurity.

Read more: https://therecord.media/ukraine-cyber-chief-on-russia-hacks-us-aid

West Asia

UAE Debuts QuantumConnect: A New Era in Secure Communications

Abu Dhabi's Technology Innovation Institute (TII), along with local partners VentureOne and e&, have launched QuantumConnect, a hardware-based encryption platform designed to embed quantum security directly into fibre-optic infrastructure across the UAE. Key actors include TII (research & development), VentureOne (ATRC's venture builder), e& (telecom/ICT operator), and regulatory bodies under the UAE's new Cryptography Executive Regulation and federal ICT laws.

The move responds to mounting concerns over cyber threats, especially those posed by the future arrival of quantum computers, which are expected to render current cryptographic techniques vulnerable. QuantumConnect uses Quantum Key Distribution (QKD) to transmit encryption keys as quantum particles—making eavesdropping or key duplication detectable by physical principles. The system is designed to integrate with existing fibre networks, enabling organisations to scale use of quantum-safe encryption while meeting regulations for sectors with high sensitivity like finance, government, and healthcare. The platform has already been deployed in some live settings, demonstrating practical improvements in data protection and regulatory compliance.

Accompanying this launch is a complementary testbed in Abu Dhabi Global Market (ADGM) involving a three-node QKD deployment connecting three sites within the financial centre. That test network acts as a "living lab," allowing stakeholders to test real-world use cases, validate operational reliability, and observe how quantum-secure communications perform under commercial traffic and standards.

Strategically, this development positions the UAE as one of the early adopters of quantum-secure infrastructure in a commercial context, strengthening the country's resilience against evolving cyber threats. It signals that governments and industry are no longer treating quantum security as academic or futuristic, but as urgent and implementable. On an international scale, this aligns with global efforts to future-proof critical infrastructure, particularly in jurisdictions seeking greater digital sovereignty, stronger privacy guarantees, and protections against both conventional cyberattacks and emerging quantum risks.

Read more: https://meobserver.org/technology/2025/09/07/uae-debuts-quantumconnect-a-new-era-in-secure-communications/?

Malware & Vulnerabilities

ScarCruft Uses RokRAT Malware in Operation HanKook Phantom Targeting South Korean Academics

ScarCruft, also known as APT37 or InkySquid, a North Korean state-linked threat group, has launched a new cyber-espionage campaign called Operation HanKook Phantom targeting South Korean academics, former officials, and researchers associated with the National Intelligence Research Association. The operation, uncovered by Seqrite Labs, reflects ongoing geopolitical tensions between North and South Korea, where sensitive research and policy data are high-value intelligence assets. Attackers employed spear-phishing emails carrying politically themed lures, including a fake "National Intelligence Research Society Newsletter Issue 52" and a document mimicking a public statement by Kim Yo Jong, to trick recipients into opening malicious attachments. These attachments were delivered as compressed ZIP archives containing Windows shortcut

(LNK) files disguised as PDFs, which upon execution installed RokRAT, a malware strain long attributed to APT37.

RokRAT possesses a wide range of capabilities, including system reconnaissance, file enumeration, screenshot capture, command execution, and downloading of additional payloads. Data exfiltration is routed through popular cloud platforms such as Google Drive, Dropbox, pCloud, and Yandex Cloud, a method that blends malicious traffic with legitimate services to evade detection. In some cases, the operation leveraged obfuscated PowerShell and batch scripts for fileless, in-memory execution, further complicating identification. Notably, one variant masqueraded its traffic as Chrome file uploads to avoid suspicion. The campaign demonstrates ScarCruft's refinement of technical tradecraft, combining social engineering, stealthy loaders, and cloud-based data exfiltration. Strategically, the operation highlights the persistent threat North Korean advanced persistent threats pose to South Korea's national security ecosystem, particularly its academic and policy research community. More broadly, this campaign exemplifies a global trend in which state-aligned actors exploit cloud infrastructure and politically resonant lures to enhance cyber-espionage effectiveness, underscoring the rising difficulty of distinguishing hostile activity from legitimate network behaviour.

Read more: https://thehackernews.com/2025/09/scarcruft-uses-rokrat-malware-in.html?

SAP S/4HANA Critical Vulnerability CVE-2025-42957 Exploited

A critical vulnerability identified as CVE-2025-42957 has been disclosed in SAP S/4HANA, one of the world's most widely used enterprise resource planning (ERP) platforms. The flaw, reported by SAP SE and cataloged in the U.S. National Vulnerability Database, affects function modules exposed via the Remote Function Call (RFC) interface. Attackers with valid user privileges can exploit the weakness to inject arbitrary ABAP (Advanced Business Application Programming) code into the system, bypassing essential authorization checks. This effectively functions as a backdoor, granting the attacker the ability to fully compromise targeted systems by undermining confidentiality, integrity, and availability. The vulnerability has been rated CVSS 9.9 (Critical), with an attack vector that is network-based, requires low complexity, and does not demand user interaction—making it highly exploitable once access credentials are obtained.

The broader context is significant, as SAP S/4HANA underpins critical operations for governments, multinational corporations, and industries such as energy, finance, and logistics. A successful exploitation could allow threat actors—whether cybercriminal groups or state-backed entities—to manipulate financial records, disrupt supply chains, exfiltrate sensitive corporate or government data, or implant persistent access for long-term espionage. The vulnerability highlights the enduring risks of insecure code execution pathways within large-scale enterprise applications, where even authorized user accounts can be weaponized against the system. SAP has issued a security advisory and mitigation guidance through its patch management channels, but exploitation remains a concern for organizations with delayed update cycles. Strategically, this disclosure underscores how advanced persistent threats are likely to prioritize enterprise resource systems as attack surfaces, given their central role in global business and government operations. It also illustrates a broader trend in cybersecurity: attackers are increasingly exploiting trusted, high-value platforms to achieve systemic impact, elevating the need for rapid patch deployment, least-privilege enforcement, and continuous monitoring within enterprise environments.

Read more: https://nvd.nist.gov/vuln/detail/CVE-2025-42957

Operation BarrelFire: NoisyBear targets entities linked to Kazakhstan's Oil & Gas Sector.

Kazakhstan's oil and gas sector, particularly employees of state-owned KazMunaiGas (KMG), was targeted in a sophisticated cyber campaign named Operation BarrelFire, attributed to a newly identified threat actor tracked as NoisyBear by Seqrite Labs. Although KMG later confirmed the operation was a simulated internal exercise, the technical sophistication mirrors real-world attacks and provides insights into potential threat scenarios. The campaign used spear-phishing emails exploiting a compromised finance department account

to deliver malicious ZIP attachments, containing decoy documents and shortcut (.LNK) files that executed PowerShell-based loaders. These loaders, dubbed DOWNSHELL, deployed batch scripts that manipulated system memory and disabled security tools, such as AMSI (Antimalware Scan Interface), to ensure undetected execution. The final stage involved DLL implants that could have provided persistent access and remote control over affected endpoints. The decoy documents were crafted to appear as official HR or internal IT communications, including policy updates, salary schedules, and instructions in Russian and Kazakh, enhancing credibility and reducing suspicion among targets.

Technically, the campaign showcased multiple evasion techniques, including string concatenation to bypass static detection, reflective loading of PowerShell scripts, obfuscation of .NET assemblies, and staged payload execution. The infrastructure relied on remote servers to host the malicious scripts and facilitate dynamic deployment. Although simulated, the exercise reflects how state-backed or highly skilled cyber threat groups could exploit trusted internal communication channels to infiltrate energy sector operations, a critical national infrastructure.

Strategically, this operation underscores the vulnerabilities of Central Asian energy assets to targeted cyber intrusions, whether by foreign adversaries or internal testing scenarios, highlighting the need for robust phishing defenses, continuous monitoring, and endpoint security. It also illustrates broader trends in cybersecurity, where attackers increasingly combine social engineering, multi-stage malware, and evasion techniques to compromise industrial control systems, demonstrating that energy infrastructure remains a high-value target with significant implications for national security, economic stability, and geopolitical leverage.

Read more: https://www.seqrite.com/blog/operation-barrelfire-noisybear-kazakhstan-oil-gas-sector/

Akira Ransomware Group Utilizing SonicWall Devices for Initial Access

The Akira ransomware group, a ransomware-as-a-service (RaaS) actor active since early 2023, has increasingly exploited vulnerabilities in SonicWall network appliances to gain initial access into enterprise networks. Key actors include Akira, SonicWall (the U.S.-based firewall and VPN vendor), and Rapid7, which is monitoring the threat and providing mitigation guidance. The operation exploits weaknesses in SonicWall's MySonicWall.com cloud backups, the SSLVPN component, and default LDAP group configurations. Attackers gain access to backup configuration files, exposing credentials, tokens, and service settings, which they then leverage to escalate privileges, access sensitive data, disable security measures, and deploy ransomware at the hypervisor or server level. The group also abuses the Virtual Office Portal, which in certain default configurations allows public access, enabling them to manipulate MFA/TOTP settings if valid credentials are available.

Technically, the attack flow involves exploiting known vulnerabilities such as CVE-2024-0015 and misconfigured default groups, followed by privilege escalation, lateral movement, and hypervisor-level encryption of files. The campaign is consistent with Akira's standard modus operandi: targeting edge devices and network appliances to achieve operational impact, steal sensitive data, and disrupt business continuity. The approach demonstrates the strategic targeting of network infrastructure as an attack vector, combining configuration exploitation, credential theft, and administrative access abuse to maximize impact while evading detection.

Strategically, this campaign highlights the growing risk posed by supply-chain-adjacent attacks on network appliances and VPN infrastructure, particularly as remote access devices become ubiquitous in corporate networks. Organizations using SonicWall appliances are urged to apply patches, reset credentials, enforce MFA, and segment backups to prevent catastrophic compromise. Internationally, the Akira campaign reflects a broader trend in ransomware operations that increasingly target enterprise hardware vulnerabilities to bypass traditional defenses, emphasizing the need for continuous monitoring, proactive vulnerability management, and comprehensive incident response strategies to safeguard critical IT infrastructure.

Read more: https://www.rapid7.com/blog/post/dr-akira-ransomware-group-utilizing-sonicwall-devices-for-initial-access/

Introducing HybridPetya: Petya/NotPetya copycat with UEFI Secure Boot bypass

ESET researchers have identified a novel ransomware variant named HybridPetya, a copycat of the infamous Petya and NotPetya malware, distinguished by its capability to compromise both legacy BIOS and modern UEFI-based systems. HybridPetya leverages the recently disclosed CVE-2024-7344 vulnerability to bypass UEFI Secure Boot on outdated systems, installing a malicious EFI application onto the EFI System Partition to encrypt the Master File Table (MFT) of NTFS-formatted drives. Unlike NotPetya, which was primarily destructive, HybridPetya retains recoverable decryption keys, allowing it to function as conventional ransomware. Samples were initially uploaded to VirusTotal from Poland in February 2025, though telemetry indicates no widespread deployment in the wild.

Technically, HybridPetya operates through a UEFI bootkit that first evaluates the encryption status of the system before proceeding. It extracts encryption keys and nonces from configuration files, applies Salsa20 encryption to critical boot files, and marks progress through dedicated counter files on the EFI partition. Its installer can exploit outdated firmware to bypass Secure Boot protections, a method that could enable persistent, stealthy control over high-value systems. The malware's architecture allows both single-system targeting and potential future adaptation for broader network propagation, mirroring the operational design of prior Petya and NotPetya campaigns, which caused multi-billion-dollar disruptions globally.
Strategically, HybridPetya illustrates the growing trend of ransomware actors targeting low-level firmware and UEFI interfaces to circumvent traditional security controls, expanding the attack surface of critical infrastructure and enterprise environments. Its design highlights vulnerabilities in system firmware management and the need for robust patching, firmware integrity monitoring, and backup strategies. Internationally, the discovery underscores the persistent risk of advanced ransomware evolving beyond software-level exploitation toward hardware and firmware compromise, signaling a shift in threat actor sophistication that could have profound implications for national cybersecurity preparedness, corporate risk management, and global IT supply chain security.

Read more: https://www.welivesecurity.com/en/eset-research/introducing-hybridpetya-petya-notpetya-copycat-uefi-secure-boot-bypass/

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.