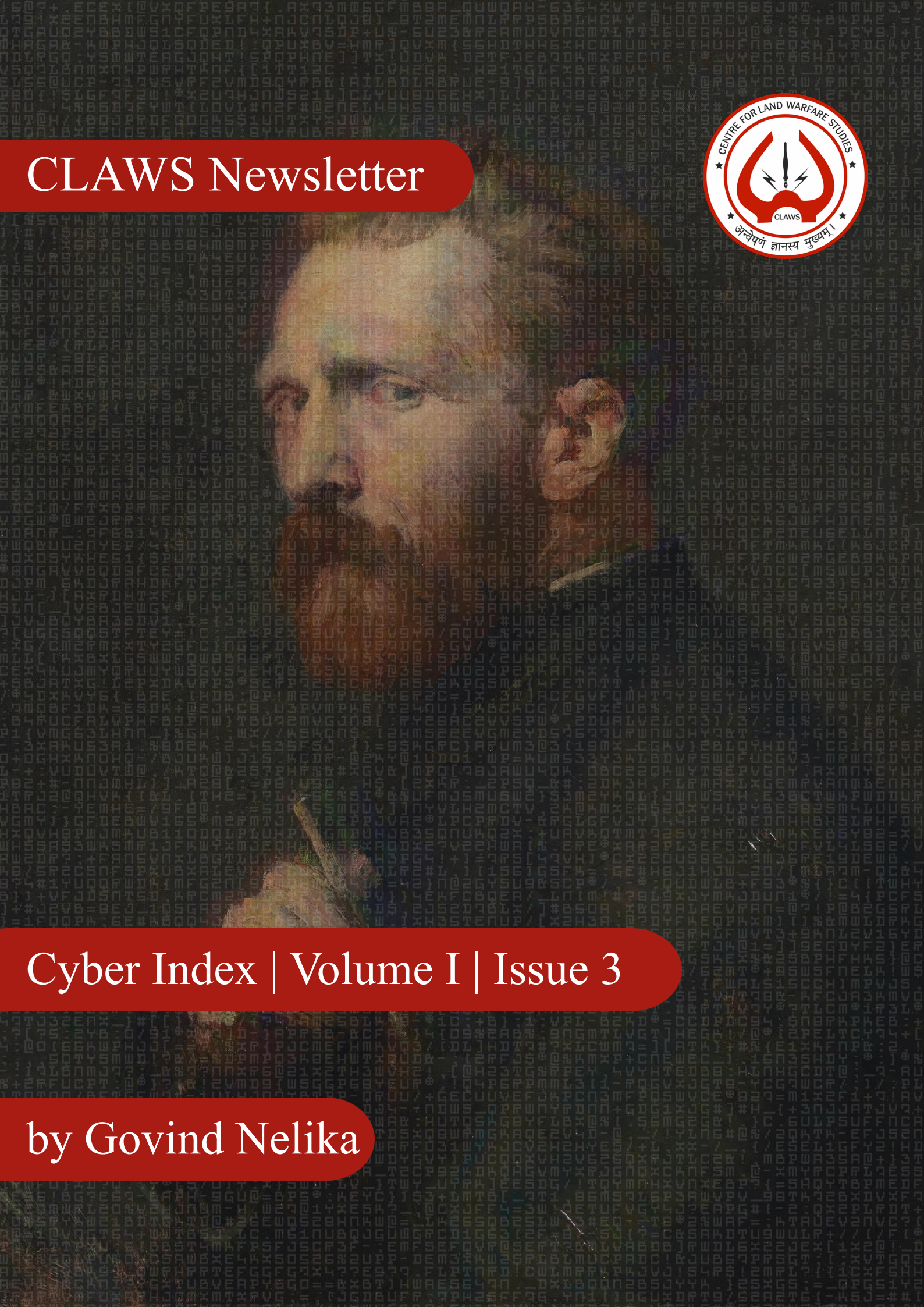
CLAWS Newsletter



Cyber Index | Volume I | Issue 3

by Govind Nelika

About us

The Centre for Land Warfare Studies (CLAWS) is an independent think tank based in New Delhi, India, dedicated to strategic studies and land warfare in the Indian context. Established in 2004 and registered under the Societies Registration Act, 1860, CLAWS operates as a membership-based organization governed by a Board of Governors and an Executive Council, under the Aegis of the Indian Army.

With a futuristic outlook and a policy-oriented approach, CLAWS focuses on national security issues, conventional military operations, and sub-conventional warfare. The Centre closely monitors regional conflicts and military developments within India's strategic frontiers, particularly in South Asia.

Committed to fostering strategic culture and informed policymaking, CLAWS disseminates its research to armed forces personnel, policymakers, members of the strategic community, and interested civilians. By facilitating in-depth studies and discussions, CLAWS contributes to shaping India's defense policies and military preparedness.

The CLAWS Newsletter is a newly fortnightlyseries under the leadership of Dr. Tara Kartha, Director Research & Academics. The newsletter features insightful content curated by CLAWS researchers, each specializing in their respective verticals. This initiative aims to provide in-depth analysis, strategic insights, and updates on key issues.

Contents

Opening News

Safe and Effective: Advancing Department of Defence Test and Evaluation for AI and Autonomous Systems

The Center for a New American Security (CNAS) recently published a report titled "Safe and Effective," authored by Josh Wallin, focusing on advancing the Department of Defense's (DoD) test and evaluation (T&E) processes for artificial intelligence (AI) and autonomous systems. As AI and autonomy increasingly influence modern warfare, the report emphasizes the necessity for the DoD to develop agile and iterative T&E frameworks that can keep pace with rapid technological advancements. Key recommendations include broadening test safety policies to address the unique characteristics of AI-enabled and autonomous systems, thereby improving testing efficiency. The report also highlights the importance of balancing technological innovation with responsible risk management to maintain the United States' competitive edge in a global landscape where adversaries are also advancing their AI capabilities.

Read more: https://www.cnas.org/publications/reports/safe-and-effective

United States of America (USA)

Hegseth orders suspension of cyber, information operations planning against Russia

Defence Secretary Pete Hegseth has directed U.S. Cyber Command to halt planning of cyber and information operations against Russia, aiming to encourage Russia to engage in negotiations with Ukraine. This suspension restricts U.S. cyber personnel from activities intended to influence or disrupt Russian decision-making in the digital realm. The order does not affect the National Security Agency's intelligence efforts targeting Russia. Critics, including Democratic lawmakers, argue that this move could weaken U.S. cyber defence and embolden Russian cyber activities. The Kremlin has welcomed the shift, with spokesperson Dmitry Peskov stating that the new U.S. foreign policy direction "largely coincides with our vision".

Read more : https://www.nextgov.com/cybersecurity/2025/03/hegseth-orders-suspension-cyber-information-operations-planning-against-russia/403415/

Pentagon Denies Report of Halt in Cyber Operations Versus Russia

The Pentagon has refuted claims that Defence Secretary Pete Hegseth ordered a cessation of offensive cyber operations against Russia. A senior defence official clarified that Hegseth has neither cancelled nor delayed any such operations, emphasizing that no stand-down order has been issued concerning actions targeting malicious Russian entities. This denial comes amid reports suggesting a pause in U.S. Cyber Command's offensive activities against Russia, which had raised concerns among lawmakers about potential vulnerabilities to Russian cyber threats. The Pentagon's reaffirmation underscores its commitment to maintaining robust cyber defence and offense strategies against adversarial actions

Read more : https://www.bloomberg.com/news/articles/2025-03-04/pentagon-denies-report-of-halt-in-cyber-operations-versus-russia?srnd=phx-technology

US communications agency to explore alternatives to GPS systems

The U.S. Federal Communications Commission (FCC) plans to vote on March 27 to explore alternatives to the Global Positioning System (GPS) due to rising national security concerns associated with reliance on a single navigation system. GPS is integral to positioning, navigation, and timing (PNT) across various sectors, including aviation, maritime, and automotive industries. FCC Chair Brendan Carr emphasized the need for redundant technologies to mitigate increased risks. Since 2023, there has been a notable rise in GPS interference, particularly spoofing, heightening the risk of accidents if navigational systems fail. The FCC's initiative aligns

with prolonged calls from President Donald Trump and bipartisan lawmakers to address these vulnerabilities. The upcoming vote will initiate an inquiry to identify and develop complementary or alternative PNT systems, engaging stakeholders from both government and industry. Additionally, the Federal Aviation Administration has been collaborating globally to authenticate navigation systems to combat spoofing threats.

Read more : https://www.reuters.com/business/media-telecom/us-communications-agency-explore-alternatives-gps-systems-2025-03-05/

https://www.theguardian.com/technology/2025/mar/14/what-could-apples-high-court-challenge-mean-for-data-protection?

United Kingdom of Great Britain and Northern Ireland

Activist Groups Challenge UK Demand for Apple Encryption Backdoor

Two UK human rights organizations, Privacy International and Liberty, have filed a legal complaint with the Investigatory Powers Tribunal (IPT) to contest the UK government's secret order demanding that Apple create a backdoor to its encrypted data. This order, issued under the Investigatory Powers Act (IPA), seeks to compel Apple to provide access to encrypted user data stored in iCloud, effectively compromising the end-to-end encryption offered by Apple's Advanced Data Protection service. Apple has refused to comply, stating, "We have never built a back door or master key to any of our products, and we never will." In response to the order, Apple withdrew its Advanced Data Protection feature from the UK market and lodged a legal complaint with the IPT. The activist groups argue that such a mandate infringes upon customers' rights to privacy and free expression and are advocating for the appeal to be heard publicly to ensure transparency.

Read more: https://www.macrumors.com/2025/03/14/activist-groups-challenge-uk-apple-backdoor/
https://www.theguardian.com/technology/2025/mar/14/what-could-apples-high-court-challenge-mean-for-data-protection?

Canada

China, Russia will 'very likely' use AI to target Canadian voters: Intelligence agency

Canada's Communications Security Establishment (CSE) has issued a warning that artificial intelligence (AI) technologies, such as deepfakes and large language models, could be exploited to interfere in the country's democratic processes. The CSE's report highlights the potential for AI to create highly convincing disinformation, making it challenging for citizens to distinguish between authentic and fabricated content. This development poses a significant threat to the integrity of elections, as malicious actors could use AI-generated content to mislead voters or discredit political figures. The CSE emphasizes the need for increased public awareness and the development of tools to detect and counteract AI-driven disinformation campaigns to safeguard Canada's democracy.

Read more : https://www.cbc.ca/news/politics/election-threat-artificial-intellligence-cse-1.7475483
https://www.cyber.gc.ca/en/guidance/cyber-threats-canadas-democratic-process-2025-update

The Republic of China (ROC) | Taiwan

What TSMC's $100 billion investment in the US means for Taiwan

Taiwan Semiconductor Manufacturing Co (TSMC) has announced a US$100 billion investment in the United States, increasing its total U.S. commitments to US$165 billion. This move follows U.S. President Donald Trump's threats to impose tariffs of up to 100 percent on overseas-made chips, accusing Taiwan of undermining the U.S. chip industry. While this investment may mitigate tariff threats, concerns arise about its impact on

Taiwan's economy and its strategic "silicon shield," which has historically deterred potential aggression from China. Some analysts fear that increasing TSMC's U.S. production could reduce Taiwan's geopolitical significance, potentially weakening U.S. incentives to defend the nation. Taiwanese officials plan to review the deal to ensure that the most advanced chip-making processes remain domestic. Conversely, some experts believe the investment could enhance Taiwan's security by strengthening ties with the U.S. and fostering growth in the chip industry.

Read more: https://www.taipeitimes.com/News/feat/archives/2025/03/06/2003832952

The People's Republic of China | China

China creates hacker-proof quantum satellite communication link with South Africa

Chinese scientists have successfully established a quantum communication link between China and South Africa, spanning approximately 12,800 kilometers (7,954 miles). This achievement was facilitated by China's quantum communication satellite, Mozi (also known as Micius), which transmitted quantum keys to ground stations in both countries. The use of quantum key distribution ensures that any eavesdropping attempts would be immediately detectable, thereby providing a highly secure communication channel. This development not only marks a significant milestone in international quantum communication but also underscores China's advancements in creating hacker-proof communication networks.

Read more : https://www.scmp.com/news/china/science/article/3302234/china-creates-hacker-proof-quantum-satellite-communication-link-south-africa

China's Strategic University Expansion: Cultivating AI Talent

China's leading universities, including Peking University, Renmin University, and Shanghai Jiao Tong University, are expanding undergraduate enrollment to align with national strategic priorities, particularly in artificial intelligence (AI), integrated circuits, and new energy sectors. This initiative aims to cultivate a robust domestic STEM talent pool, especially in light of recent U.S. visa restrictions affecting Chinese students. The success of AI startup DeepSeek, which developed cost-effective AI models comparable to those in the U.S., underscores the effectiveness of China's investment in STEM education. This expansion is part of a broader national effort to transform China into a "strong education nation" by 2035, focusing on innovation and educational efficiency.

Read more : https://www.devdiscourse.com/article/education/3301612-chinas-strategic-university-expansion-cultivating-ai-talent

China to launch 'sci-tech board' in bond market

China is set to introduce a "sci-tech board" within its bond market to facilitate the issuance of science and technology innovation bonds by financial institutions, tech companies, and private equity investment entities. Announced by Pan Gongsheng, governor of the People's Bank of China, during the third session of the 14th National People's Congress, this initiative aims to channel bond funds more effectively and cost-efficiently toward technological innovation. Additionally, China plans to optimize re-lending policies for sci-tech innovation and technological transformation, expanding the re-lending scale from the current 500 billion yuan (approximately $70 billion) to up to 1 trillion yuan to better meet enterprises' financing needs. Efforts will also focus on maintaining fiscal interest subsidies to reduce corporate financing costs and developing new structural monetary policy tools to support investment and financing in the sci-tech innovation sector. Wu Qing, chairman of the China Securities Regulatory Commission, indicated that the commission will enhance mechanisms dedicated to sci-tech enterprises and more precisely support the listing of high-quality technology companies

Read more: https://english.www.gov.cn/news/202503/06/content_WS67c9820bc6d0868f4e8f0819.html

China abruptly replaces tech czar behind AI and chip push

China has unexpectedly replaced Jin Zhuanglong, the nation's technology minister overseeing advancements in artificial intelligence (AI) and semiconductor development. Jin, a 60-year-old aerospace expert, had been absent from public view since December 2024, sparking speculation about his status. He has been succeeded by Li Lecheng, formerly the governor of Liaoning province, though no official reason for this abrupt change has been provided. This move marks the fourth ministerial replacement under President Xi Jinping's administration since 2023, following the dismissals of the ministers of defence, agriculture, and foreign affairs, amid an intensified anti-corruption campaign. Jin previously played a pivotal role in China's technological initiatives, including leading the development of the C919 passenger jet. His ministry, the Ministry of Industry and Information Technology, is crucial in regulating sectors such as heavy industry, telecommunications, and electronics, aligning with Xi's vision for China's economic transformation and technological self-reliance

Read more : https://www.straitstimes.com/asia/east-asia/china-abruptly-replaces-tech-czar-behind-ai-and-chip-push

US congressional panel urges Americans to ditch China-made routers

A U.S. congressional committee has urged Americans to remove Chinese-made wireless routers, specifically those manufactured by TP-Link, from their homes, citing security threats that could enable China to hack U.S. critical infrastructure. The House of Representatives Select Committee on China has called on the Commerce Department to investigate TP-Link Technology Co, the leading global seller of WiFi routers by unit volume. Rob Joyce, former director of cybersecurity at the National Security Agency, highlighted that TP-Link devices could expose users to cyber intrusions, potentially allowing hackers to leverage these vulnerabilities to attack critical infrastructure. In response, TP-Link stated there is no evidence linking the company to the Chinese government and asserted that their products do not pose unique national security risks. The company also noted that it has relocated its manufacturing operations to Vietnam after separating from its former China affiliate.

Read more : https://www.reuters.com/world/us/us-congressional-committee-china-urges-americans-ditch-tp-link-routers-2025-03-05/

Ukraine

Ukraine's cyber chief wants 'tens of thousands' more computer whizzes to combat Russian hackers

Colonel Oleksandr Potiy, head of Ukraine's State Service of Special Communications (Derzhspetszvyazku), emphasizes the need to decentralize cybersecurity efforts and cultivate a substantial workforce to counter persistent Russian cyber threats. The agency monitors approximately 3,000 Russian-led cyberattacks annually targeting Ukraine's civil government infrastructure. Potiy advocates for training "tens of thousands" of cybersecurity specialists and decentralizing authority to enhance resilience against these sophisticated Russian attacks.

Read more : https://kyivindependent.com/ukraines-cyber-chief-talks-decentralization-and-the-need-for-tens-of-thousands-more-computer-whizzes-to-combat-russian-hackers/

The Russian Federation

Russia Capitalizes on Development of Artificial Intelligence in Its Military Strategy

Russia has significantly increased its investment in artificial intelligence (AI), allocating a substantial portion of its state budget toward AI-driven military research. This funding aims to enhance Russia's technological edge in modern warfare, particularly in AI-enabled military applications. Russia's full-scale invasion of

Ukraine marked the first major conflict with widespread AI use. Ukraine, supported by U.S. AI firms, successfully countered Russian forces, prompting Russia to accelerate AI integration in command systems, drones, and air defense networks. Russia's focus and rapid development of AI has given it an advantage against Western weaponry regardless of the outcome of its invasion of Ukraine. Russia's AI development traces back to early Soviet experiments in the 1960s. It was not after its illegal annexation of Crimea in 2014, however, that Russia's military AI development accelerated

Read more : https://jamestown.org/program/russia-capitalizes-on-development-of-artificial-intelligence-in-its-military-strategy/

The Commonwealth of Australia

Power of persistence: Australian technology addresses challenge of space monitoring

Australia is enhancing its space-domain awareness capabilities through innovative technologies like FireOPAL, a passive sensor system developed by Lockheed Martin Australia in collaboration with Curtin University. FireOPAL employs wide-field optical sensors to continuously monitor vast sections of the sky, enabling near-real-time detection of satellite maneuvers within 60 to 120 seconds—a significant improvement over traditional methods that can take hours or days. This advancement allows civil space agencies and defense organizations to respond more swiftly to potential threats, such as collisions or adversarial satellite activities, thereby strengthening Australia's position in space monitoring and security.

Read more : https://www.aspistrategist.org.au/power-of-persistence-australian-technology-addresses-challenge-of-space-monitoring/

Nippon-koku (Japan)

U.S.-Japan Technology and Economic Security Achieving Resilience in an Era of Disruption

The report "U.S.-Japan Technology and Economic Security: Achieving Resilience in an Era of Disruption" by The National Bureau of Asian Research (NBR) examines how the United States and Japan are enhancing their economic and technological resilience against emerging challenges such as digital threats, supply chain vulnerabilities, and economic coercion. It highlights Japan's policy reforms, development finance initiatives in digital infrastructure, and collaboration with the U.S. on cybersecurity to safeguard economic interests. The U.S. is similarly focusing on policy adjustments and partnerships to boost economic resilience. Furthermore, the report emphasizes countering economic coercion and strengthening U.S.-Japan cooperation as essential components for achieving long-term economic security in a rapidly evolving global landscape

Read more : https://www.nbr.org/publication/us-japan-technology-and-economic-security-achieving-resilience-in-an-era-of-disruption/

Japan losing to China in deep sea race as key research vessel ages

Japan's deep-sea exploration capabilities are at a critical juncture as its primary manned submersible, Shinkai 6500, approaches the end of its operational lifespan. Commissioned in 1989, Shinkai 6500 has conducted approximately 1,800 dives, reaching depths of up to 6,500 meters and contributing significantly to marine science, including earthquake research and deep-sea biodiversity studies. However, with its support vessel, Yokosuka, also aging, there are concerns about Japan's future in manned deep-sea exploration. Compounding the issue, the expertise required to construct such specialized vessels has diminished over time, making the development of a successor both challenging and uncertain. While the government plans to focus on unmanned submersibles, researchers emphasize the irreplaceable value of crewed missions for real-time observations and complex tasks. Without timely investment in new manned submersibles, Japan risks losing its competitive edge in deep-sea research, especially as other nations continue to advance their capabilities.

Read more : https://asia.nikkei.com/Business/Science/Japan-losing-to-China-in-deep-sea-race-as-key-research-vessel-ages

Vulnerabilities This week

Cellebrite zero-day exploit used to target phone of Serbian student activist

Amnesty International's Security Lab has uncovered the misuse of a zero-day exploit developed by Cellebrite to unlock the phone of a Serbian student activist. This exploit targets vulnerabilities in Android's USB kernel drivers, allowing unauthorized access to locked devices. The investigation revealed that Serbian authorities have continued their surveillance of civil society, even after previous reports highlighted such abuses. In response to these findings, Cellebrite announced on February 25, 2025, the suspension of its product use by certain customers in Serbia. The vulnerabilities exploited are not limited to specific devices, potentially affecting over a billion Android users. Amnesty International collaborated with industry partners, including Google's Threat Analysis Group, leading to the identification and patching of several vulnerabilities in the Linux kernel.
Read more : https://securitylab.amnesty.org/latest/2025/02/cellebrite-zero-day-exploit-used-to-target-phone-of-serbian-student-activist/

Sticky Werewolf Uses Undocumented Implant to Deploy Lumma Stealer in Russia and Belarus

The threat actor known as Sticky Werewolf has been linked to targeted cyberattacks in Russia and Belarus, deploying the Lumma Stealer malware through a previously undocumented implant. The attack sequence begins with spear-phishing emails containing malicious attachments, which initiate a complex, multi-stage process to deploy the Lumma Stealer. This malware collects extensive data from infected devices, including browser-stored banking details and cryptocurrency wallet files. Notably, Sticky Werewolf utilizes readily available malicious tools from darknet forums, focusing their efforts on crafting targeted phishing emails and delivery mechanisms, rather than developing proprietary malware.

Read more : https://thehackernews.com/2025/02/sticky-werewolf-uses-undocumented.html

Silk Typhoon hackers now target IT supply chains to breach networks

Chinese state-sponsored cyber-espionage group 'Silk Typhoon' has shifted its tactics to target IT supply chains, focusing on remote management tools and cloud services to infiltrate downstream customer networks. This approach has led to breaches across multiple sectors, including government, healthcare, defence, and energy. The group exploits unpatched applications to escalate privileges within targeted organizations, subsequently using stolen credentials to access customer networks and abuse various deployed applications, including Microsoft services. This tactic allows them to achieve their espionage objectives while minimizing detection.

Read more : https://www.bleepingcomputer.com/news/security/silk-typhoon-hackers-now-target-it-supply-chains-to-breach-networks/

Cybersecurity officials warn against potentially costly Medusa ransomware attacks

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) have issued a warning about the Medusa ransomware, which has been active since 2021 and has recently impacted hundreds of individuals. Medusa uses phishing campaigns to steal credentials and operates on a double extortion model, encrypting victim data while threatening to release it publicly if the ransom is not paid. The ransomware's data-leak site lists victims and offers a countdown to data release, with the option to delay the timer for a $10,000 cryptocurrency payment. To mitigate the risk, officials recommend updating operating

systems, software, and firmware, employing multifactor authentications for all services, and using long, secure passwords. Medusa has targeted over 300 victims in various sectors, including medical, education, legal, insurance, technology, and manufacturing.

Read more: https://apnews.com/article/fbi-cisa-gmail-outlook-cyber-security-email-6ed749556967654f-f41a629a230973e6

Microsoft Patches 57 Security Flaws, Including 6 Actively Exploited Zero-Days

In March 2025, Microsoft released security updates addressing 57 vulnerabilities across its software portfolio, including six zero-day flaws actively exploited in the wild. Among these, six were rated Critical, with 23 identified as remote code execution vulnerabilities and 22 as privilege escalation issues. Notably, the actively exploited zero-days encompass:

- CVE-2025-24983: A use-after-free vulnerability in the Windows Win32 Kernel Subsystem allowing local privilege escalation.

- CVE-2025-24984: An information disclosure flaw in Windows NTFS that permits attackers with physical access to read portions of heap memory via a malicious USB drive.

- CVE-2025-24985: An integer overflow in the Windows Fast FAT File System Driver enabling local code execution.

- CVE-2025-24991: An out-of-bounds read in Windows NTFS leading to local information disclosure.

- CVE-2025-24993: A heap-based buffer overflow in Windows NTFS facilitating local code execution.

- CVE-2025-26633: An improper neutralization vulnerability in Microsoft Management Console allowing local security feature bypass.

These updates underscore the importance of promptly applying patches to mitigate potential security risks.

Read more: https://thehackernews.com/2025/03/urgent-microsoft-patches-57-security.html

OBSCURE#BAT Malware Highlights Risks of API Hooking

Researchers have identified a malware campaign named "OBSCURE#BAT" that employs heavily obfuscated batch files and PowerShell scripts to deliver the "r77" rootkit. This rootkit utilizes user-mode API hooking to conceal files, registry entries, and processes, effectively evading detection by standard Windows tools. The attack initiates with social engineering tactics, such as fake software updates, leading users to execute malicious scripts that establish persistence and facilitate unauthorized access. This development underscores the evolving sophistication of malware techniques aimed at bypassing traditional security measures.

Read more: https://www.darkreading.com/vulnerabilities-threats/obscurebat-malware-highlights-api-hooking

About the Author

Govind Nelika is the Researcher /Web Manager 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.