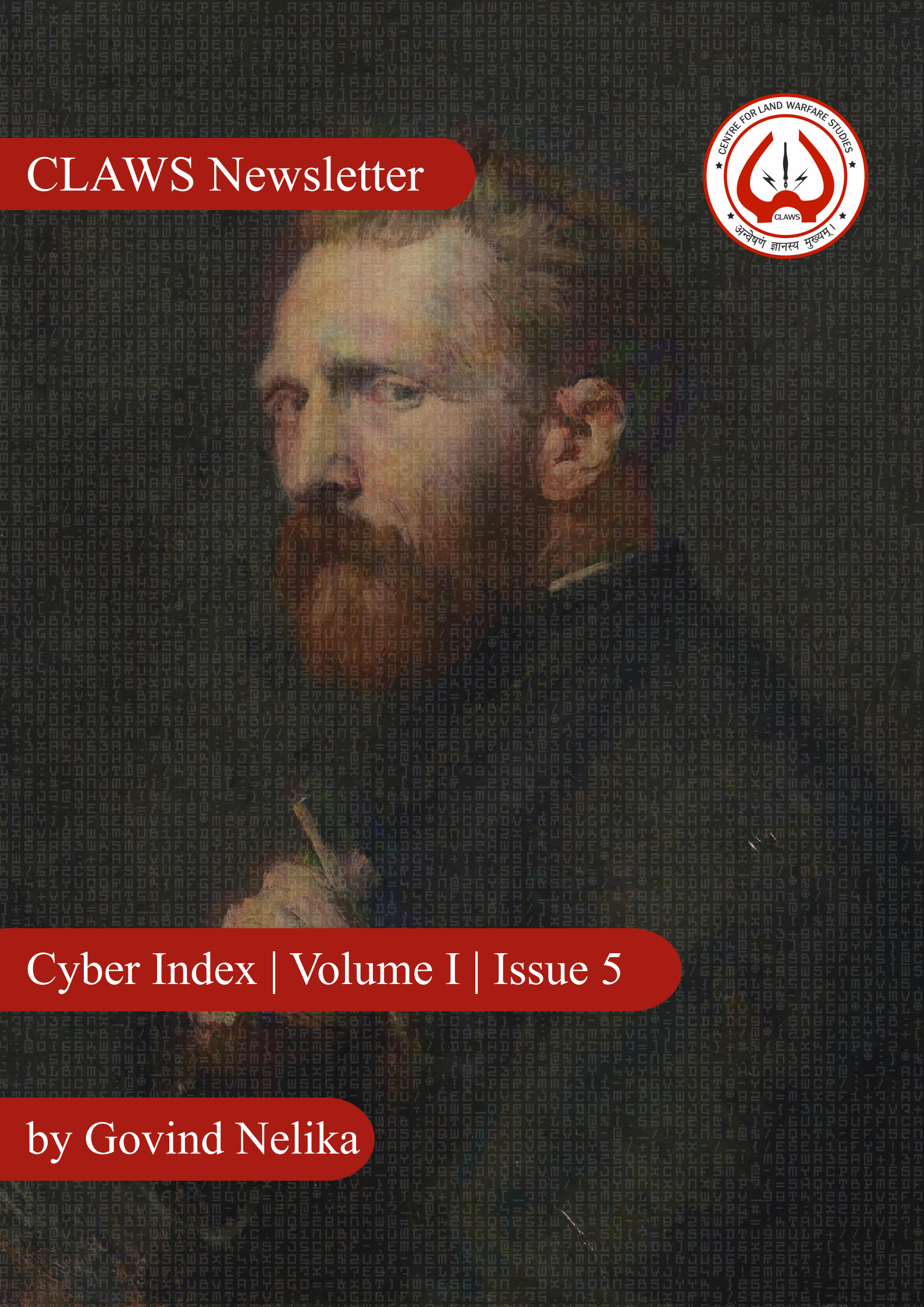
CLAWS Newsletter



Cyber Index | Volume I | Issue 5

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

Attempt to recruit security researchers in bizarre hacking campaign

A mysterious campaign is attempting to recruit cybersecurity professionals to hack Chinese websites, offering up to $100,000 per month. Using fake social media accounts with attractive avatars, the recruiter, known as "Jack," directs targets to a Telegram channel, seeking individuals skilled in exploiting Chinese content management systems to deploy web shells. Jack claims the goal is to obtain "China's traffic" but provides no clear motive or affiliation, inconsistently citing the Indian government and blaming translation errors. Security experts suspect the campaign may be a trolling effort rather than a legitimate threat actor.

Read more: https://techcrunch.com/2025/04/01/someone-is-trying-to-recruit-security-researchers-in-bizarre-hacking-campaign/

Cybersecurity & Cryptography Professor Faced China-Funding Inquiry Before Disappearing, Sources Say

Xiaofeng Wang, a leading cryptography and cybersecurity expert at Indiana University, has come under intense scrutiny following a federal investigation in early 2025. Known internationally for his groundbreaking work in applied cryptography, secure systems, and privacy-preserving technologies, Wang has published extensively and collaborated with major tech companies and government agencies.

His sudden disappearance from the university's website and the FBI's raid on his home sparked speculation, especially amid concerns about potential undisclosed ties to Chinese research programs. Despite the seriousness of the probe, no criminal charges have been filed, and Wang's attorney states he remains safe. He had recently planned a move to a university in Singapore and had requested a leave of absence from IU before his abrupt dismissal.

The situation echoes the now-defunct "China Initiative," raising questions about academic freedom and the treatment of Chinese-born researchers in the U.S, particularly those like Wang, who operate at the intersection of national security and advanced cryptography

Read more: https://www.wired.com/story/xiaofeng-wang-indiana-university-research-probe-china/
https://www.reuters.com/world/us/indiana-university-cybersecurity-professor-has-not-been-arrested-or-detained-2025-04-02/

Stanford releases its AI Index report

The 2025 AI Index Report, published by Stanford's Institute for Human-Centred Artificial Intelligence (HAI), provides an in-depth, data-driven analysis of artificial intelligence's rapid evolution across technical, economic, and societal dimensions. This eighth edition arrives at a critical juncture, highlighting AI's profound impact on global governance, innovation, and daily life. The report delves into significant advancements in model performance, unprecedented levels of private investment, and the increasing integration of AI into sectors such as healthcare, transportation, and education. Additionally, it examines the growing geopolitical dynamics, with nations like China narrowing the gap in AI capabilities, intensifying the global race for AI leadership. Through comprehensive data and analysis, the AI Index equips policymakers, researchers, and the public with essential insights to navigate the complexities of AI's transformative role in society.

Read more: https://hai.stanford.edu/ai-index/2025-ai-index-report

Cyber security and resilience policy statement | United Kingdom of Great Britain and Northern Ireland

The UK's proposed Cyber Security and Resilience Bill aims to strengthen national cyber defences by expand-

ing regulatory oversight to around 1,000 additional organizations, including IT service providers and data centres. It mandates that significant cyber incidents, such as ransomware attacks, must be reported within 72 hours, enhancing threat visibility and response coordination. The bill grants regulators increased powers to enforce compliance, conduct investigations, and recover oversight costs. It also emphasizes the importance of securing digital supply chains and aligns with the EU's NIS 2 directive to ensure consistency in international cyber security standards.

Read more: https://www.gov.uk/government/publications/cyber-security-and-resilience-bill-policy-statement/cyber-security-and-resilience-bill-policy-statement

Paris set to host difficult negotiations on tackling commercial hacking tools

The Pall Mall Process, a joint initiative by the UK and France, convened in Paris to address the global proliferation and misuse of commercial cyber intrusion capabilities (CCICs), such as spyware. The draft agreement proposes measures including regulation of CCIC development and export, domestic oversight mechanisms, vulnerability equity processes, procurement bans on irresponsible vendors, and penalties for misuse. Despite these efforts, key exporting nations like Israel, India, and Austria have been hesitant to participate, though Israel and NSO Group have shown preliminary engagement. The initiative aims to establish a voluntary Code of Practice inspired by international humanitarian standards, but its success depends on broader international commitment.

Read more: https://therecord.media/paris-pall-mall-process-meeting-commercial-hacking-tools

IIT Kanpur and the HQ Central Command, Indian Army signed (MoU) to collaborate for drones and Unmanned Aerial Vehicles (UAVs)

On April 2, 2025, IIT Kanpur and the Indian Army's Central Command signed a Memorandum of Understanding (MoU) to jointly develop an advanced Remote Piloting Training Module (RPTM) and a Software-in-the-Loop Simulator (SITL) for drones and Unmanned Aerial Vehicles (UAVs). This collaboration aims to enhance the Indian Army's training capabilities by integrating advanced simulation technologies, improving efficiency, reducing costs, and minimizing risks. The project, led by IIT Kanpur's UAV Laboratory in collaboration with VU Dynamics Pvt. Ltd., is expected to be completed within six months. The development team, including faculty and students, will create simulations to train operators in real-world drone scenarios, ensuring safety and precision while reducing the need for costly real-time exercises. This initiative underscores IIT Kanpur's aerospace expertise and contributes to India's self-reliance in defence and aerospace innovation.

Read more: https://imoc.iitk.ac.in/iitk-news-single.php?newsid=ODY1

The Republic of China (ROC) | Taiwan

Taiwan says China using generative AI to ramp up disinformation and 'divide' the island

Taiwan has accused China of leveraging generative artificial intelligence (AI) to intensify disinformation campaigns aimed at sowing division within Taiwanese society. The island's National Security Bureau reported that AI-generated content is being utilized to manipulate public opinion and exacerbate internal divisions. This development comes amid heightened tensions, with China recently conducting military exercises near Taiwan and imposing trade sanctions, actions that Taiwan views as efforts to coerce acceptance of Beijing's sovereignty claims. Taiwan continues to reject these claims, emphasizing its commitment to democratic principles and national sovereignty.

Read more: https://www.reuters.com/world/asia-pacific/taiwan-says-china-using-generative-ai-ramp-up-disinformation-divide-island-2025-04-08/

The People's Republic of China | China

China accuses US of launching 'advanced' cyberattacks, names NSA agents

Chinese authorities in Harbin have accused the U.S. National Security Agency (NSA) of conducting sophisticated cyberattacks during the February 2025 Asian Winter Games. According to China's state news agency Xinhua, the attacks targeted critical infrastructure, including energy, transportation, and defence institutions in Heilongjiang province, with the alleged intent to disrupt China's information systems and steal confidential data. Chinese police have named three individuals Katheryn A. Wilson, Robert J. Snelling, and Stephen W. Johnson as suspected NSA agents involved in these operations. Additionally, the University of California and Virginia Tech were cited as being implicated, though specific details were not provided. The U.S. Embassy in China has not commented on these allegations.

Read more: https://www.reuters.com/technology/cybersecurity/chinas-harbin-says-us-launched-advanced-cyber-attacks-winter-games-2025-04-15/

Police Arrest Tibetans for Internet, Phone Use | Human Rights Watch

Chinese authorities have intensified surveillance and repression in Tibet by arresting individuals for their online and phone activities. According to Human Rights Watch, Tibetans have been detained for sharing information deemed politically sensitive, including content related to the Dalai Lama and discussions about human rights. These arrests underscore the Chinese government's ongoing efforts to suppress dissent and control information flow within the region. Human Rights Watch has called on the Chinese government to respect freedom of expression and end the criminalization of peaceful online activities.

Read more: https://www.hrw.org/news/2025/04/13/china-police-arrest-tibetans-internet-phone-use?

Apple chip engineer returns to China, joins Fudan University amid push for talent

Kong Long, a former Apple chip engineer, has returned to China to join Fudan University's School of Microelectronics as a researcher and doctoral adviser. With over seven years of experience at Apple's California headquarters, Kong specialized in wireless semiconductors, contributing to the development of radio frequency chips for devices like the iPhone, Apple Watch, and AirPods. His new role at Fudan focuses on radio frequency integrated circuit system design, digital-analog hybrid computing chips, and high-speed data interface ICs. Kong's move reflects China's broader initiative to attract top semiconductor talent amid efforts to enhance domestic chipmaking capabilities and reduce reliance on foreign technology. He holds a degree in microelectronics from Shanghai Jiao Tong University and earned his PhD in electrical engineering from the University of California, Los Angeles, in 2016.

Read more: https://www.scmp.com/tech/tech-trends/article/3304607/apple-chip-engineer-returns-china-joins-fudan-university-amid-push-talent

Microsoft shutters AI lab in Shanghai, signalling a broader pullback from China

Microsoft has closed its IoT & AI Insider Lab in Shanghai's Zhangjiang Hi-Tech Zone, signaling a broader retreat from China amid escalating geopolitical tensions. Established in 2019, the lab aimed to support the development of Internet of Things (IoT) and artificial intelligence (AI) technologies. Reports indicate that the facility ceased operations in January or February 2025, as the premises were found unoccupied with the company's logo removed and equipment cleared out. This closure aligns with Microsoft's recent strategic shifts, including halting projects with its joint venture Wicresoft and laying off approximately 2,000 employees in China, reflecting the company's response to the evolving global business environment.

Read more: https://www.scmp.com/tech/big-tech/article/3304621/microsoft-shutters-ai-lab-shanghai-signalling-broader-pullback-china?

Democratic People's Republic of Korea (North Korea)

North Korea ramps up cyber offensive: New research centre to focus on AI-powered hacking

North Korea has established "Research Center 227" under the military's Reconnaissance General Bureau, focusing on developing artificial intelligence-powered hacking technologies. The center aims to enhance the country's cyber capabilities by creating offensive programs designed to steal information and disrupt adversary networks. Staffed by approximately 90 experts, including graduates from top university and doctoral programs, the facility operates around the clock to respond to real-time intelligence. This initiative reflects North Korea's broader strategy to strengthen its cyber operations, which have included activities like the 'Contagious Interview' campaign, where fake job adverts are used to distribute malware. The establishment of Research Center 227 underscores the regime's commitment to advancing its cyber warfare capabilities amid escalating global cyber tensions.

Read more: https://www.dailynk.com/english/n-korea-ramps-up-cyber-offensive-new-research-center-to-focus-on-ai-powered-hacking/

Russia – Ukraine

CERT-UA reports attacks in March 2025 targeting Ukrainian agencies with WRECKSTEEL Malware

In March 2025, Ukraine's Computer Emergency Response Team (CERT-UA) identified three cyberattacks targeting state agencies and critical infrastructure, attributed to the threat actor UAC-0219. These attacks employed the WRECKSTEEL malware, delivered via phishing emails containing links to file-sharing services like DropMeFiles and Google Drive. The malware, implemented in both VBScript and PowerShell, executed PowerShell scripts to search for sensitive files, capture screenshots, and exfiltrate data using cURL. Notably, the attackers used NSIS installers with decoy files and the IrfanView image viewer to disguise their activities. CERT-UA emphasized that WRECKSTEEL lacks persistence mechanisms, urging organizations to report any indicators of compromise promptly to facilitate timely cyber protection measures.

Read more: https://securityaffairs.com/176181/cyber-warfare-2/cert-ua-reports-attacks-in-march-2025-targeting-ukrainian-agencies-with-wrecksteel-malware.html

United Kingdom of Great Britain and Northern Ireland

Russian spy sensors found hidden in UK waters

Russian spy sensors have been discovered hidden in UK waters, potentially aimed at monitoring the country's nuclear submarines. The devices were found both underwater and washed ashore, prompting national security concerns. While the UK government has not officially confirmed the reports, the Ministry of Defence has acknowledged the evolving threat landscape and is enhancing efforts to safeguard critical offshore infrastructure. The discovery underscores the growing risks associated with undersea surveillance and the need for robust defense measures to protect vital national assets.

Read more: https://www.telegraph.co.uk/news/2025/04/06/russian-spy-sensors-hidden-uk-waters/

Rebooting Copyright: How the UK Can Be a Global Leader in the Arts and AI

In an era where artificial intelligence is reshaping the boundaries of creativity, the UK stands at a pivotal crossroads: will it become a global leader in aligning copyright with technological innovation? The Tony Blair Institute's latest report, Rebooting Copyright: How the UK Can Be a Global Leader in the Arts and AI, lays out a bold vision for navigating this intersection. Arguing that current copyright frameworks risk stifling both

artistic expression and AI development, the report proposes a forward-looking solution introducing a text and data mining (TDM) exception with an opt-out for rights holders. This approach aims to protect the interests of creators while providing the legal clarity necessary for responsible AI advancement. By embracing this balanced, pragmatic model, the UK has an opportunity not only to lead transatlantic debates on digital rights but to set a global standard for how innovation and culture can thrive together.

Read more: https://institute.global/insights/tech-and-digitalisation/rebooting-copyright-how-the-uk-can-be-a-global-leader-in-the-arts-and-ai

United States of America (USA)

Pentagon's 'SWAT team of nerds' resigns en masse

The Defence Digital Service (DDS), established in 2015 as the Pentagon's rapid-response tech unit, is set to dissolve by the end of April 2025 following the mass resignation of its 14-member team. This decision comes amid pressures from the Elon Musk-led Department of Government Efficiency (DOGE), which has been restructuring various government tech initiatives. DDS, often referred to as the Pentagon's "SWAT team of nerds," played a pivotal role in developing technological solutions during critical events, including the Afghanistan withdrawal and the coordination of aid to Ukraine. Director Jennifer Hay and her team cited marginalization and a lack of integration into DOGE's AI-focused reforms as primary reasons for their departure. The Pentagon announced that DDS's functions will be absorbed by the Chief Digital and Artificial Intelligence Office

Read more: https://www.politico.com/news/2025/04/15/pentagons-digital-resignations-00290930

The Limits of Chip Export Controls in Meeting the China Challenge

The CSIS report titled "The Limits of Chip Export Controls in Meeting the China Challenge" examines the effectiveness of U.S. semiconductor export restrictions aimed at curbing China's technological and military advancements. While these controls have disrupted China's access to advanced chips and manufacturing equipment, they have also spurred China to accelerate its domestic semiconductor development and reduce reliance on U.S. technology. This unintended consequence risks diminishing U.S. influence in global tech supply chains and could undermine the competitiveness of American firms. The report emphasizes the need for a more nuanced and multilateral approach to export controls, balancing national security concerns with the potential economic and strategic repercussions.

Read more: https://www.csis.org/analysis/limits-chip-export-controls-meeting-china-challenge

Trump fires NSA director in national security purge, sources say

President Donald Trump dismissed General Timothy Haugh from his position as Director of the National Security Agency (NSA) and Commander of U.S. Cyber Command. The reasons for Haugh's removal remain undisclosed, but sources suggest it may be linked to his perceived ties to former Joint Chiefs Chairman General Mark Milley, a known critic of Trump. Haugh's ousting is part of a broader purge within U.S. national security agencies, which has also seen the dismissal of several White House National Security Council staff members and military leaders. Critics, including Democratic lawmakers, have condemned these actions as politically motivated and detrimental to the nonpartisan nature of U.S. intelligence and military institutions.

Read more: https://www.reuters.com/world/us/us-nsa-director-timothy-haugh-fired-washington-post-reports-2025-04-04/

The Commonwealth of Australia

Australia monitoring Chinese vessel off south coast

In March 2025, Australia began monitoring the Chinese research vessel Tan Suo Yi Hao as it moved along the country's southern coast. While the vessel, equipped with deep-sea submersibles, operated within international waters following a joint survey with New Zealand, its presence has raised concerns among Australian officials and analysts. Some fear the ship may be mapping ocean floors near sensitive infrastructure like submarine cables and naval bases, potentially supporting future military operations. The incident follows increased Chinese naval activity in the region, prompting ongoing scrutiny and reaffirming Australia's focus on protecting its maritime interests., while Chinese media had alleged those as baseless accusations.

Read more: https://www.abc.net.au/news/2025-03-31/australia-monitoring-chinese-research-vessel-off-south-coast/105117188

https://www.globaltimes.cn/page/202504/1331355.shtml

Vulnerabilities

Pipemagic Exploitation of CLFS zero-day

In April 2025, Microsoft disclosed the active exploitation of a zero-day vulnerability in the Windows Common Log File System (CLFS), designated as CVE-2025-29824. This flaw enables attackers with standard user privileges to escalate to system-level access, facilitating ransomware deployment. The exploitation process involves leaking kernel addresses to user mode via the NtQuerySystemInformation API. Notably, Windows 11 version 24H2 mitigates this attack vector by restricting access to certain system information classes to users with SeDebugPrivilege. The ransomware observed in these attacks employs typical evasion techniques, such as disabling recovery options and deleting system logs. Microsoft released security updates on April 8, 2025, to address this vulnerability and recommends that customers apply these updates promptly to protect their systems.

Read more: https://www.microsoft.com/en-us/security/blog/2025/04/08/exploitation-of-clfs-zero-day-leads-to-ransomware-activity/

Suspected China-Nexus Threat Actor Actively Exploiting Critical Ivanti Connect Secure Vulnerability (CVE-2025-22457)

A critical vulnerability in Ivanti Connect Secure (ICS) VPN appliances, identified as CVE-2025-22457, has been actively exploited by the suspected China-nexus espionage group UNC5221. This buffer overflow flaw, present in ICS versions 22.7R2.5 and earlier, allows for remote code execution. Exploitation began in mid-March 2025, following the release of a patch in February. Upon successful exploitation, attackers deployed two new malware families TRAILBLAZE, an in-memory dropper, and BRUSHFIRE, a passive backdoor alongside components from the previously reported SPAWN malware ecosystem. Ivanti has urged all customers to upgrade to ICS version 22.7R2.6 or later to mitigate risks associated with this vulnerability.

Read more: https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-exploiting-critical-ivanti-vulnerability

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.