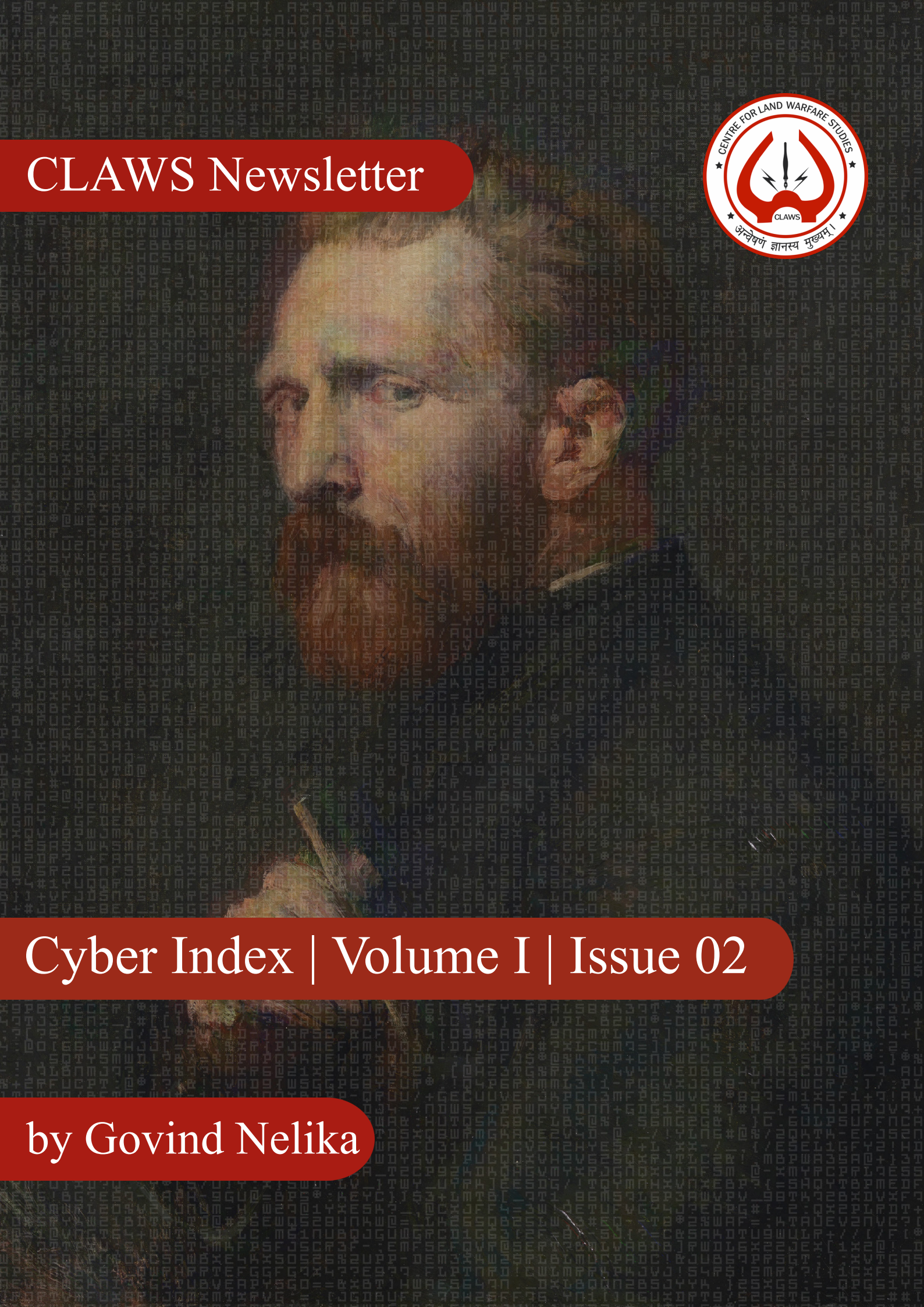
CLAWS Newsletter



Cyber Index | Volume I | Issue 02

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 Bulletin

Munich Cyber Security Conference

Ukrainian cyber officials have reported that Russia is increasingly leveraging artificial intelligence (AI) to enhance its cyber-espionage activities. According to Ihor Malchenyuk, director of the cyberdefence department at Ukraine's State Service of Special Communications and Information Protection (SSCIP), Russian hackers employ machine learning models to sift through vast amounts of exfiltrated data, identifying critical information to craft highly targeted phishing campaigns. These sophisticated attacks have recently targeted Ukrainian military personnel on encrypted messaging platforms like Signal, using personalized messages to deceive recipients into clicking malicious links, thereby compromising sensitive information. Natalia Tkachuk, head of cyber and information security at Ukraine's National Security and Defence Council, highlighted the growing collaboration between Russian state-backed hackers and cybercriminal groups, where financially motivated hackers infiltrate systems to steal funds and subsequently share access and stolen data with state-sponsored operatives. This data is then analysed using AI to further refine cyber-espionage efforts

Read More: https://therecord.media/russia-ukraine-cyber-espionage-artificial-intelligence

The Paris AI Action Summit

The Paris AI Action Summit (Feb 2025) highlighted the divide between AI policies in the Global North and the concerns of the Global South. While the EU pushed for regulations, the US warned against overregulation, prioritizing Big Tech dominance. The Global South was largely excluded, raising concerns about digital colonialism. However, emerging decentralized AI models in Brazil, South Africa, and India aim to reduce reliance on Western AI. The summit lacked focus on AI for public interest, instead centering on economic competition. A more inclusive AI future requires Global South participation, alternative models, and data sovereignty.
Read More : https://techglobalinstitute.com/announcements/blog/a-birds-eye-view-of-the-paris-ai-action-summit-regulation-power-and-alternatives/

India to play key role in AI

Infosys co-founder and chairman Nandan Nilekani emphasized that while artificial intelligence (AI) is advancing rapidly, it cannot replace essential human qualities such as empathy, leadership, collaboration, and creativity. Speaking at an All India Management Association (AIMA) event, Nilekani highlighted the importance of these traits in the workplace, stating, "You can have all the AIs in the world, but if you can't get five people to work together and collaborate, then you cannot go anywhere." Nilekani advised focusing on developing adaptable skills that AI cannot replicate, such as first-principles thinking. He noted that while AI might automate certain tasks, it will also enhance human productivity and create new job opportunities. Regarding India's AI landscape, Nilekani predicted significant advancements in the coming year, driven by initiatives like the India AI Mission.

Read more : https://timesofindia.indiatimes.com/technology/tech-news/infosys-co-founder-nandan-nilekani-you-can-have-all-the-ais-in-the-world-but-/articleshow/118519337.cms

Pegasus spyware infections found on several private sector phones

The mobile security firm iVerify reported detecting Pegasus spyware infections on 11 out of 18,000 devices tested in December. Notably, these infections affected private sector individuals in industries such as real estate, logistics, and finance, as well as a European government official. Victims were located in countries including Switzerland, Poland, Bahrain, Spain, the Czech Republic, and Armenia. This finding indicates that Pegasus spyware, developed by Israel's NSO Group, is more widely used than previously understood, impacting business executives in addition to civil society members. iVerify's detection methods involve scanning for malware signatures and utilizing machine learning to identify spyware infections. The company emphasized

the need for enhanced security measures, noting that many victims were unaware of the infections until tested.

Read more : https://therecord.media/pegasus-spyware-infections-iverify

United States of America (USA)

U.S. CISA has frozen all of its election security work

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has paused all election security activities and initiated a comprehensive review of its efforts over the past eight years. This decision, outlined in an internal memo by acting director Bridget Bean, responds to President Donald Trump's executive order on "ending federal censorship." The review encompasses all positions and programs related to election security and countering misinformation, with a completion target of March 6. During this period, funding for the Elections Infrastructure Information Sharing & Analysis Center has been suspended. This move reflects the administration's stance on alleged online censorship and aims to refocus CISA's mission on core cybersecurity and physical security tasks. State and local election officials, who have relied on CISA's support to secure voting infrastructure, may face challenges due to this suspension.

Read more : https://www.wired.com/story/cisa-election-security-freeze-memo/

CISA and FBI: Ghost ransomware breached orgs in 70 countries

The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) issued a joint advisory revealing that the Ghost ransomware group has compromised organizations across more than 70 countries since early 2021. The affected sectors include critical infrastructure, healthcare, government, education, technology, manufacturing, and numerous small and medium-sized businesses. The attackers exploit unpatched vulnerabilities in internet-facing services, such as those in Fortinet, ColdFusion, and Microsoft Exchange systems. To mitigate the risk of Ghost ransomware attacks, organizations are advised to regularly update and patch systems, implement phishing-resistant multi-factor authentication, and maintain offline backups of critical data.

Read more : https://www.bleepingcomputer.com/news/security/cisa-and-fbi-ghost-ransomware-breached-orgs-in-70-countries/

Meta's chief AI scientist says US-based researchers may look abroad as Trump tries to freeze funding

Meta's chief AI scientist, Yann LeCun, expressed concern over potential U.S. research funding cuts proposed by the Trump administration, particularly targeting the National Institutes of Health (NIH). LeCun warned that such reductions could prompt U.S.-based scientists to seek opportunities abroad, leading to a significant brain drain. He suggested that European institutions could capitalize on this by offering attractive research environments to draw top talent. LeCun emphasized that to retain and attract researchers, institutions must provide access to funding, top-tier students, competitive salaries, research freedom, state-of-the-art facilities, collaborative opportunities, and minimal administrative burdens. These concerns arise amidst legal challenges to the proposed funding cuts, with a judge temporarily blocking them as lawsuits proceed.

Read more : https://www.businessinsider.com/meta-yann-lecun-scientists-look-abroad-amid-trump-funding-cuts-2025-2

Peoples Republic of China (PRC) | China

China to tighten grip on rare earth mining for non-state firms

China plans to ban non-state companies from mining rare earth elements, allowing only large state-owned enterprises to engage in mining, smelting, or separating these minerals. This move, outlined in draft rules by the Ministry of Industry and Information Technology, aims to tighten control over a sector vital to various technologies and has been central to trade tensions with the U.S. Companies will be required to submit monthly production data to the ministry. This proposal follows China's recent export bans on materials like germanium and gallium, countering U.S. technology restrictions. China currently produces about 70% of the world's rare earths and dominates their processing.

Read more : https://www.mining.com/web/china-to-tighten-grip-on-rare-earth-mining-for-non-state-firms/

China's Xi Jinping to hold high-level meeting on Monday with top tech entrepreneurs

Chinese President Xi Jinping convened a high-profile meeting with leading technology entrepreneurs, including Alibaba's Jack Ma, on February 17, 2025, at Beijing's Great Hall of the People. This assembly, a shift from the regulatory crackdowns of recent years, aimed to rally private sector support amid economic challenges and intensifying technological competition with the United States. Xi emphasized the critical role of private enterprises in driving innovation and economic growth, urging business leaders to align with national development goals. Notable attendees included Huawei's Ren Zhengfei, BYD's Wang Chuanfu, and Xiaomi's Lei Jun. The meeting underscored China's strategic focus on self-sufficiency in key technologies and the importance of public-private collaboration in achieving this objective.

Read more : https://www.scmp.com/business/article/3298742/chinas-xi-jinping-hold-high-level-meeting-monday-top-tech-entrepreneurs

The Republic of China (ROC) | Taiwan

Taiwan pledges chip talks and investment to mollify Trump

In response to U.S. President Donald Trump's recent criticisms and tariff threats, Taiwan's President Lai Ching-te has pledged to engage in discussions with the United States to address concerns over the semiconductor industry. Lai emphasized the importance of the global semiconductor supply chain and expressed Taiwan's commitment to increasing investments in the U.S., boosting imports from the country, and enhancing defense spending. These measures aim to strengthen Taiwan's economic and security ties with the United States amidst ongoing trade tensions

Read more : https://www.reuters.com/world/taiwan-president-meet-senior-officials-us-tariffs-sources-say-2025-02-14/

Taiwan's digital ministry uses AI to combat online fraud and deep fakes

Taiwan's Ministry of Digital Affairs (MODA) announced the deployment of artificial intelligence (AI) and machine learning (ML) technologies to combat online fraud and deepfakes. The National Centre for Cybersecurity Technology (NICS), established by MODA, has developed advanced tools such as "fraud keyword extraction" and "data mining deepening." These innovations leverage natural language processing, big data analytics, AI, and ML to enable continuous, automated inspections for early-stage fraud detection. As of May 2024, the system was analyzing approximately 30,000 cases daily, identifying 5,000 to 10,000 suspected fraudulent activities, with a total monthly inspection volume exceeding 900,000 cases. This approach has significantly reduced the reliance on manual inspections and enhanced the efficiency of anti-fraud operations. Additionally, MODA has implemented a platform that integrates multiple deepfake detection methods, allow-

ing agencies to swiftly identify and analyze potential threats.

Read more : https://govinsider.asia/intl-en/article/taiwans-digital-ministry-uses-ai-to-combat-online-fraud-and-deep-fakes

China urges US to 'correct its mistakes' after website removes Taiwan independence reference

In February 2025, the U.S. State Department updated its website's Taiwan fact sheet, removing previous language stating that the U.S. does not support Taiwan's formal independence. The revised page emphasizes opposition to unilateral changes to the status quo by either Taiwan or China and highlights Taiwan's collaboration with the Pentagon on technology and semiconductor projects. The update also expresses U.S. support for Taiwan's membership in international organizations "where applicable." A State Department spokesperson described the changes as routine updates to inform the public about the unofficial U.S.-Taiwan relationship, reaffirming commitment to the one-China policy and the preservation of peace and stability in the Taiwan Strait. Taiwan's Foreign Minister, Lin Chia-lung, welcomed the revisions, appreciating the positive stance on U.S.-Taiwan relations. Conversely, China's Foreign Ministry criticized the changes, urging the U.S. to "correct its mistakes" and accusing it of sending a "seriously wrong message" to Taiwan independence forces

Read more : https://www.straitstimes.com/asia/east-asia/us-says-website-update-routine-after-removal-of-reference-to-taiwan-independence

European Union

Sweden suspects sabotage after new undersea cable damage

Swedish authorities have initiated a sabotage investigation following damage to an undersea fiber-optic cable in the Baltic Sea near Gotland Island, within Sweden's exclusive economic zone. The cable, connecting Finland and Germany, sustained minor damage that did not affect its functionality, as reported by Finnish telecom operator Cinia. This incident, first recorded on February 20, marks the third occurrence of damage to this cable in a short period. Swedish Prime Minister Ulf Kristersson emphasized the seriousness of these events, especially given the current security climate. In response to multiple cases of damaged infrastructure in the region, NATO has increased its presence in the Baltic Sea by deploying additional patrol vessels to deter potential sabotage. While some officials link these incidents to hybrid attacks and Russia's "shadow fleet," others in the U.S. and European intelligence communities consider them accidental.

Read More : https://kyivindependent.com/sweden-suspects-sabotage-after-new-undersea-cable-damage/

U.S Vice President J D Vance's week of waging war on EU tech law

U.S. Vice President JD Vance embarked on a European tour, delivering sharp critiques of the European Union's technology regulations. At the Paris AI Action Summit, Vance argued that EU tech laws hinder artificial intelligence development and stifle innovation. Later, at the Munich Security Conference, he intensified his rhetoric, comparing EU policies on disinformation and illegal online content to Soviet-era censorship and labeling EU officials enforcing these laws as "commissars." These statements represent a significant escalation in U.S. opposition to European tech regulations, aligning with recent criticisms from President Donald Trump and tech industry leaders like Elon Musk and Mark Zuckerberg, who have equated EU fines on tech companies to "tariffs."

This transatlantic tension over digital policy is further exemplified by Vice President Vance's confrontation with British Prime Minister Keir Starmer during a meeting in the Oval Office. Vance challenged Starmer over the UK's perceived infringements on free speech, citing instances such as the fining of a British Army veteran for praying outside an abortion clinic. Starmer defended the UK's commitment to free speech, emphasizing

its longstanding tradition

Read More : https://www.politico.eu/article/jd-vance-waging-war-eu-tech-law-msc-ai-summit/

The Commonwealth of Australia

Nation State Hackers Target Australian Organizations (Greyzone)

Australian organizations are increasingly targeted by nation-state hackers and hacktivist groups, with a notable rise in cyberattacks linked to geopolitical tensions. In November 2024, over 60 Distributed Denial-of-Service (DDoS) attacks were reported against 39 Australian entities, including government institutions, transportation, financial, legal, educational, and insurance sectors. Pro-Russian groups, such as NoName057(16), Cyber Army of Russia Reborn, and Z-Pentest, were responsible for more than half of these attacks, motivated by Australia's military support for Ukraine. Additionally, pro-Palestinian hacktivists, including RipperSec and the Pro-Palestinian Hacker Movement, targeted Australian organizations due to perceived support for Israel. The Australian Security Intelligence Organisation (ASIO) has also highlighted the complex security landscape, revealing state-sponsored plots from countries like Russia and Iran aimed at eliminating critics within Australia. These threats encompass espionage, politically motivated violence, and cyber sabotage, with critical infrastructure sectors, such as defence, being prime targets. ASIO warns of intensified foreign interference and influence campaigns, utilizing advanced technologies like AI and deepfakes to manipulate information and undermine public trust

Read more : https://www.defenceconnect.com.au/joint-capabilities/15527-nation-state-hackers-continue-to-target-australian-orgs-as-greyzone-operations-intensify-year-on-year

'Mayhem': Trump tariff threat forces Australia to pause big tech levy

In February 2025, the Australian government paused its plans to implement a levy on major U.S. tech companies, such as Meta and Google, due to concerns over potential trade retaliation from the Trump administration. This decision came after President Donald Trump threatened reciprocal tariffs on countries imposing taxes on U.S. goods, which could impact Australian exports. Ambassador Kevin Rudd has been actively engaging with U.S. officials to prevent a trade conflict and advise Australian ministers on proceeding without provoking U.S. backlash. The proposed levy, known as the News Bargaining Initiative, aimed to charge digital platforms that refused to compensate local media outlets for news content. Despite the delay, the Australian government remains committed to ensuring fair compensation for Australian publishers.

Read more : https://www.smh.com.au/politics/federal/mayhem-trump-tariff-threat-forces-australia-to-pause-big-tech-levy-20250214-p5lc9z.html

Kaspersky Banned on Australian Government Systems

Australia's Department of Home Affairs issued Direction 002-2025, mandating the removal of all Kaspersky Lab products and services from government systems by April 1, 2025. This decision stems from concerns over potential foreign interference, espionage, and sabotage, given Kaspersky's Russian origins. Kaspersky has refuted these allegations, attributing the ban to geopolitical tensions and asserting that no technical assessment was conducted to justify the decision. This move aligns Australia with other nations, such as the United States, which expanded its ban on Kaspersky products in 2024.

Read more : https://www.securityweek.com/kaspersky-banned-on-australian-government-systems/

United Kingdom of Great Britain and Northern Ireland

MI5 'probes use of Chinese tech in clean power'

The UK's domestic security agency, MI5, is investigating the integration of Chinese green technology into the nation's energy infrastructure due to potential security concerns. This review is part of a broader government "China audit" assessing Beijing's influence on critical sectors. The focus is on technologies such as solar panels, industrial batteries, and wind turbines supplied by Chinese companies, which are essential for the UK's decarbonization goals. Officials are particularly concerned about the possibility of sensitive data being shared with the Chinese government and the potential control over strategic energy assets. The Ministry of Defence has also expressed apprehension regarding the use of Chinese-manufactured equipment in wind farms, citing risks of espionage. Balancing the urgency of transitioning to renewable energy with national security considerations presents a complex challenge, as Chinese companies currently dominate global supply chains for many green technologies

Read more : https://renews.biz/98820/mi5-probes-use-of-chinese-tech-in-clean-power/

What the U.K. Wants from Apple Will Make Our Phones Less Safe

Apple announced the removal of its Advanced Data Protection (ADP) feature for UK users following a secret order from the British government demanding backdoor access to encrypted iCloud data. This move has sparked controversy, with privacy advocates warning that such government mandates could weaken overall cybersecurity and set a dangerous precedent for other nations. Apple, known for its strong stance on user privacy, opted to withdraw the feature rather than compromise encryption integrity, emphasizing that it would not create backdoors or master keys for its products. Critics argue that mandatory backdoor access not only threatens individual privacy but also increases the risk of security vulnerabilities that could be exploited by malicious actors. This decision highlights the ongoing global debate between national security interests and digital privacy rights, raising concerns about whether other governments may follow the UK's lead in pressuring tech companies to weaken encryption standards

Read more : https://foreignpolicy.com/2025/02/25/apple-united-kingdom-adp-back-door-less-safe/

Tackling AI security risks to unleash growth and deliver Plan for Change

On February 14, 2025, during the Munich Security Conference, UK Technology Secretary Peter Kyle announced the transformation of the AI Safety Institute into the AI Security Institute. This rebranding emphasizes the UK's commitment to addressing AI-related national security and crime risks, aligning with the government's Plan for Change. The Institute's expanded focus includes preventing AI's use in developing chemical and biological weapons, conducting cyber-attacks, and facilitating crimes such as fraud and child sexual abuse. A new criminal misuse team, in collaboration with the Home Office, will research these threats, particularly the creation of AI-generated child sexual abuse material. Additionally, the Institute will partner with entities like the Defence Science and Technology Laboratory to assess frontier AI risks. In parallel, the UK government has secured an agreement with AI firm Anthropic to explore AI-driven economic growth opportunities, furthering the objectives of the Plan for Change.

Read more : https://www.gov.uk/government/news/tackling-ai-security-risks-to-unleash-growth-and-deliver-plan-for-change

TechUK demands that Britain's chip strategy is crisped up

In February 2025, TechUK, a leading trade association, released a report urging the UK government to accelerate and enhance its National Semiconductor Strategy, originally introduced in May 2023. The strategy had allocated £1 billion over a decade, focusing on the UK's strengths in chip design, research and development,

and compound semiconductors. However, TechUK contends that progress since its inception has been merely "incremental" and advocates for more decisive actions. Key recommendations include establishing national bodies to facilitate collaboration among chipmakers, securing financing, accessing export markets, and designating semiconductor fabrication plants as critical national infrastructure. These measures aim to solidify the UK's position in the global semiconductor landscape and attract necessary investments.

Read more : https://www.theregister.com/2025/02/17/techuk_semiconductor_strategy/

The Federal Republic of Germany

German Election targeted by alleged Russian Disinformation

German security services have identified an alleged Russian disinformation campaign targeting the upcoming federal elections. Fake videos are circulating on social media, falsely depicting ballot manipulation, such as the exclusion of the Alternative for Germany (AfD) party from ballots or the destruction of AfD-marked ballots. Authorities attribute these actions to a group known as Storm-1516, previously linked to interference in the 2024 U.S. presidential election. The Interior Ministry emphasizes that this campaign aims to influence the election outcome and undermine democratic processes.

Researchers have also uncovered a network of over 700 fake social media accounts disseminating pro-Russian narratives and attacking conservative frontrunner Friedrich Merz. This orchestrated effort seeks to sway public opinion and disrupt the electoral process. In response to these threats, Germany's domestic intelligence service (BfV) has established a special task force to counter potential cyberattacks, espionage, sabotage, and disinformation campaigns ahead of the federal election. The BfV emphasizes the need to protect democracy in the digital space against foreign influence

Read more : https://therecord.media/german-election-targeted-by-russian-disinformation

Republic of Korea (ROK)

South Korea aims to secure 10,000 GPUs for national AI computing centre

South Korea has announced plans to acquire 10,000 high-performance graphics processing units (GPUs) within this year to bolster its national AI computing capabilities. Acting President Choi Sang-mok emphasized that as global competition in the AI industry intensifies, the focus is shifting from corporate battles to national innovation ecosystems. The government aims to secure these GPUs through public-private collaboration to expedite the launch of services at its national AI computing center. While specific GPU models and budget details are yet to be finalized, decisions are expected by September. This initiative comes in the context of recent U.S. regulations on AI chip exports, from which South Korea is exempt, allowing it to advance its AI infrastructure plans without facing export restrictions.

Read more : https://www.reuters.com/technology/artificial-intelligence/south-korea-aims-secure-10000-gpus-national-ai-computing-centre-2025-02-17/

South Korea suspends DeepSeek AI over privacy concerns

South Korea's Personal Information Protection Commission (PIPC) has temporarily suspended new downloads of the Chinese AI chatbot DeepSeek due to concerns over its handling of personal data. The suspension affects downloads from Apple and Google app stores, though the chatbot remains accessible via web browsers. The PIPC stated that the suspension will continue until DeepSeek ensures compliance with South Korea's privacy laws. In response, DeepSeek is working to address these concerns by appointing a legal representative in South Korea and updating its policies to meet local requirements.This action follows reports from South Korea's National Intelligence Service (NIS) accusing DeepSeek of excessively collecting personal data, in-

cluding keyboard input patterns that could identify individuals. The NIS warned that chat records might be transferred to Chinese servers, potentially compromising user privacy.

Read more : https://san.com/cc/south-korea-suspends-deepseek-ai-over-privacy-concerns/

Nippon-koku (Japan)

Japan & Australia to Bolster IT

Japan and Australia have launched the Pacific Digital Development Initiative to enhance telecommunications infrastructure and digital resilience in Pacific Island nations. This collaboration aims to provide funding and technology for projects like installing submarine cables, improving connectivity, and strengthening cybersecurity. The initiative reflects both countries' commitment to supporting the region's digital development and countering potential security risks associated with reliance on certain foreign technologies.

Read more : https://asia.nikkei.com/Business/Technology/Japan-Australia-to-bolster-IT-personnel-of-Pacific-island-nations

Other Focus

Economic cyber-espionage: a persistent and invisible threat

Economic cyber-espionage, defined as state-sponsored theft of sensitive business information through cyber means for commercial gain, poses an invisible yet persistent threat to national economies. Despite a 2015 G20 agreement condemning cyber-enabled intellectual property (IP) theft for commercial purposes, incidents have quadrupled since then. Notably, the focus of these cyber-espionage activities has shifted from advanced economies to emerging ones, with countries in South Asia, Southeast Asia, and Latin America increasingly targeted. Many of these nations, rapidly expanding in sectors like biotechnology, advanced manufacturing, and digital services, often lack robust recognition of or defence against such threats. Efforts to combat economic cyber-espionage require a comprehensive approach, including political acknowledgment, international cooperation, and the development of cybersecurity capacities tailored to protect IP-intensive industries

Read more : https://www.aspistrategist.org.au/economic-cyber-espionage-a-persistent-and-invisible-threat/

Meta confirms 'Project Waterworth,' a global subsea cable project spanning 50,000 kilometers

Meta has unveiled Project Waterworth, an ambitious initiative to construct a 50,000-kilometer subsea cable system connecting the United States, India, Brazil, South Africa, and other regions. This multibillion-dollar project aims to enhance global internet connectivity and support the company's AI advancements. The cable will feature 24 fiber pairs, significantly increasing data transmission capacity. To ensure resilience, the system will be installed at depths of up to 7,000 meters and employ enhanced burial techniques in shallow, high-risk areas to protect against potential hazards. This development underscores Meta's commitment to bolstering digital infrastructure and facilitating technological growth across multiple continents.

Read more : https://techcrunch.com/2025/02/14/meta-confirms-project-waterworth-a-global-subsea-cable-project-spanning-50000km/

Revealed: Google facilitated Russia and China's censorship requests

An investigation by the Observer has revealed that Google has been cooperating with autocratic regimes, including Russia and China, by facilitating their censorship requests. Since 2011, Google has engaged with

approximately 150 countries, responding to requests to remove content, including those from democratic governments, dictatorships, and regimes accused of human rights abuses. The company has taken down content such as YouTube videos of anti-state protesters or content criticizing political figures upon requests from countries like Russia and China. Google's data indicates that there are 5.6 million items "named for removal" due to government requests, with requests doubling since 2020. Russia accounted for more than 60% of these requests, often involving sensitive political content. In China, Google took down over 200 videos requested by the Ministry of Public Security. Critics argue that Google's actions raise concerns about its role in controlling public information and the lack of transparency and regulation over their censorship decisions. Despite claims of assessing the legitimacy of requests, Google's transparency reports provide only partial insights into its decision-making processes.

Read more : https://www.theguardian.com/world/2025/feb/15/google-helped-facilitate-russia-china-censorship-requests

How China is making waves in the AI race

China's artificial intelligence (AI) landscape experienced a significant transformation, with Hangzhou emerging as a pivotal hub for AI innovation. The city, already renowned as the headquarters of tech giant Alibaba, has become home to several AI startups, notably DeepSeek, which have been instrumental in challenging Silicon Valley's dominance in AI technology.

DeepSeek's rapid ascent has been marked by the development of advanced AI models that rival Western counterparts in performance while being more cost-effective. Their flagship model, DeepSeek-R1, has gained widespread adoption, particularly in China's home appliance industry. Companies such as Haier, Hisense, and TCL Electronics have integrated DeepSeek's AI into products like televisions, refrigerators, and robotic vacuum cleaners, enhancing their functionality and user interaction.

The success of DeepSeek has not only bolstered national pride but also prompted other Chinese tech giants to accelerate their AI initiatives. Tencent, for instance, introduced its AI model, Hunyuan Turbo S, which claims faster response times and cost efficiency compared to DeepSeek-R1. This competitive environment underscores China's commitment to advancing its AI capabilities and reducing reliance on Western technologies.
In summary, Hangzhou's emergence as a center for AI innovation, spearheaded by companies like DeepSeek, signifies a strategic shift in the global AI landscape. China's focus on developing competitive, cost-effective AI solutions is reshaping industry dynamics and challenging established players in Silicon Valley.

Read more: https://www.afr.com/world/asia/china-s-ai-dragons-take-on-silicon-valley-20250204-p5l9ig

Malware

North Korea exploits vulnerabilities in U.S. cybersecurity systems

In a recent statement, Kathleen Fisher, director of DARPA's Information Innovation Office, highlighted that North Korea exploits vulnerabilities in U.S. cybersecurity systems to fund its nuclear weapons program through ransomware attacks. She emphasized that while existing technologies can prevent such breaches, bureaucratic hurdles, particularly the Authority to Operate (ATO) process, delay their deployment. Fisher stressed the urgency of implementing these solutions to enhance software security and prevent inadvertently financing adversarial weapon development.

Read more : https://breakingdefense.com/2025/02/us-cyber-vulnerabilities-fuel-n-koreas-nuclear-arsenal-but-solutions-are-near-darpa-official/

Russia-linked cyberattacks by Storm-2372 targeting governments, NGOs, critical infrastructure

Alleged Russian state-sponsored hackers, identified as Storm-2372, have been conducting a global phishing campaign targeting various sectors, including government, defence, telecommunications, healthcare, education, energy, and non-governmental organizations. Active since at least August 2024, the group employs device code phishing techniques to compromise accounts. This method involves tricking victims into entering authentication codes on legitimate sign-in pages, allowing attackers to obtain access tokens and infiltrate email and cloud storage services without needing passwords. The campaign has affected entities across Africa, Europe, the Middle East, and North America.
In a related development, the alleged Russian hackers have also targeted government officials worldwide by compromising their WhatsApp accounts through spear-phishing attacks. The group, known as Star Blizzard and linked to Russia's Federal Security Service (FSB), sends emails impersonating U.S. government officials, enticing recipients to click on malicious QR codes that grant access to their WhatsApp messages. These attacks have primarily focused on diplomats, defence policymakers, and researchers involved in Russia-related matters

Read more : https://industrialcyber.co/ransomware/microsoft-details-russia-linked-cyberattacks-by-storm-2372-targeting-governments-ngos-critical-infrastructure/

Lumma Stealer Spread By Reemergent Angry Likho APT

Advanced persistent threat (APT) group known as Angry Likho, also called Sticky Werewolf, has resurfaced, targeting high-profile organizations in Russia and Belarus, among other countries. The group employs spear-phishing emails with malicious RAR attachments to deploy the Lumma Stealer malware. Once activated, this malware extracts system data, software details, personal information, browser-stored data, and cryptocurrency wallets. Notably, Angry Likho utilizes a new method involving a self-extracting archive named FrameworkSurvivor.exe, created with the Nullsoft Scriptable Install System, indicating a shift toward more covert operations

Read more: https://www.msspalert.com/brief/lumma-stealer-spread-by-reemergent-angry-likho-apt

A Tale of Two Typhoons: Properly Diagnosing Chinese Cyber Threats

Erica Lonergan and Michael Poznansky authored an article in War on the Rocks titled "A Tale of Two Typhoons: Properly Diagnosing Chinese Cyber Threats," analyzing two significant Chinese cyber operations: Volt Typhoon and Salt Typhoon. While both intrusions involved unauthorized access to U.S. critical infrastructure, the authors emphasize their distinct objectives and recommend tailored policy responses.

Salt Typhoon: This operation is characterized as a large-scale espionage effort. Chinese actors infiltrated major U.S. telecommunications networks, including Verizon and AT&T, accessing sensitive data from high-profile individuals such as President-elect Donald Trump and Vice President-elect JD Vance. The primary aim was intelligence gathering for national security purposes. For such espionage activities, the authors suggest that policymakers should prioritize incident response and bolster future defense and resilience measures.
Volt Typhoon: This breach is identified as operational preparation of the environment. Chinese operatives embedded themselves within U.S. critical infrastructure, potentially positioning cyber assets for activation during a crisis or conflict. This preemptive strategy could disrupt U.S. military operations and civilian life in the event of hostilities. To counteract such threats, the authors recommend focusing on deterring war, preventing attacks on civilian targets, and enhancing resilience for military assets.

Read more : https://warontherocks.com/2025/02/a-tale-of-two-typhoons-properly-diagnosing-chinese-cyber-threats/

Winos 4.0 Malware Targets Taiwan With Email Impersonation

The Winos 4.0 malware is targeting organizations in Taiwan through phishing emails that impersonate le-

gitimate sources. This tactic aims to deceive recipients into opening malicious attachments or links, leading to system compromises. Fortinet experts have raised alarms about this campaign, emphasizing the need for heightened vigilance and robust cybersecurity measures to counter such sophisticated threats.

Read more : https://www.infosecurity-magazine.com/news/winos-40-malware-targets-taiwan/

Palo Alto Networks' Unit 42 have discovered a new Linux backdoor named Auto-Color

Researchers at Palo Alto Networks' Unit 42 have discovered a new Linux backdoor named Auto-Color, active between November and December 2024. This malware is designed with advanced evasion techniques to avoid detection. It disguises itself under benign file names such as "door" or "egg" to blend in with legitimate system files. Additionally, Auto-Color hides its command-and-control (C2) connections, using methods similar to the Symbiote malware family, making it difficult for security tools to detect its communications. It also employs proprietary encryption to secure its configuration and data transfers, further complicating analysis. Once installed, the malware provides attackers with full remote access to the compromised system, allowing them to execute commands stealthily. The initial infection method remains unknown, but researchers have found it targeting universities and government offices in North America and Asia. Due to its sophisticated design, removing Auto-Color from infected systems requires specialized security measures.

Read more : https://unit42.paloaltonetworks.com/new-linux-backdoor-auto-color/

CERT-UA Warns of UAC-0173 Attacks Deploying DCRat to Compromise Ukrainian Notaries

The Computer Emergency Response Team of Ukraine (CERT-UA) has identified a resurgence of cyberattacks by the group UAC-0173, targeting Ukrainian notaries since mid-January 2025. These attacks utilize phishing emails, purportedly from the Ministry of Justice of Ukraine, prompting recipients to download an executable file hosted on Cloudflare's R2 storage service. Once executed, this file installs the DCRat (DarkCrystal RAT) malware, granting attackers remote access to compromised systems. Subsequently, additional tools like RDPWRAPPER are deployed to facilitate parallel RDP sessions, and utilities such as FIDDLER, NMAP, and XWorm are used for intercepting authentication data, network scanning, and data theft, respectively. Compromised systems are also exploited to disseminate further phishing emails using the SENDMAIL utility.

Read more : https://thehackernews.com/2025/02/cert-ua-warns-of-uac-0173-attacks.html

CISA Adds Microsoft and Zimbra Flaws

The Cybersecurity and Infrastructure Security Agency (CISA) has added two new vulnerabilities to its Known Exploited Vulnerabilities Catalogue due to active exploitation. The first, CVE-2024-49035, is an improper access control vulnerability in Microsoft Partner Center, while the second, CVE-2023-34192, is a cross-site scripting (XSS) vulnerability in Synacor's Zimbra Collaboration Suite (ZCS). These vulnerabilities are actively being exploited and pose significant risks, particularly to federal enterprises. Under Binding Operational Directive 22-01, Federal Civilian Executive Branch (FCEB) agencies are required to remediate these vulnerabilities by the specified due date to protect their networks from cyber threats. Although this directive is mandatory for federal agencies, CISA strongly advises all organizations to address these vulnerabilities promptly as part of their cybersecurity and vulnerability management strategies

Read more : https://www.cisa.gov/news-events/alerts/2025/02/25/cisa-adds-two-known-exploited-vulnerabilities-catalog

Chinese Hackers Exploit Windows Tool to Install Backdoors

The Chinese state-sponsored hacking group Mustang Panda is exploiting a legitimate Microsoft tool, MA-

VInject.exe, to install backdoors on government systems in the Asia-Pacific region. By abusing MAVInject, the group can inject malicious code into trusted processes, effectively evading antivirus detection. This tactic underscores the evolving strategies of threat actors in leveraging legitimate tools for malicious purposes, highlighting the need for enhanced monitoring of system utilities to detect and prevent such sophisticated attacks.

Read more : https://www.govinfosecurity.com/chinese-hackers-exploit-windows-tool-to-install-backdoors-a-27555

New Golang-Based Backdoor Uses Telegram Bot API for Evasive C2 Operations

Netskope Threat Labs have uncovered a new Golang-based backdoor that leverages the Telegram Bot API for command-and-control (C2) communications. Believed to be of Russian origin, this malware operates by injecting itself into the "C:\Windows\Temp\svchost.exe" directory upon execution. It utilizes an open-source Golang library to interact with Telegram, allowing it to receive commands from an attacker-controlled chat. Currently, the backdoor supports three implemented commands: executing PowerShell commands (/cmd), relaunching itself for persistence (/persist), and self-deletion (/selfdestruct). Notably, while a screenshot capture function (/screenshot) is listed, it remains unimplemented. The malware sends the output of these commands back to the Telegram channel, facilitating covert operations and evasion of traditional detection mechanisms.

Read more: https://thehackernews.com/2025/02/new-golang-based-backdoor-uses-telegram.html?

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.