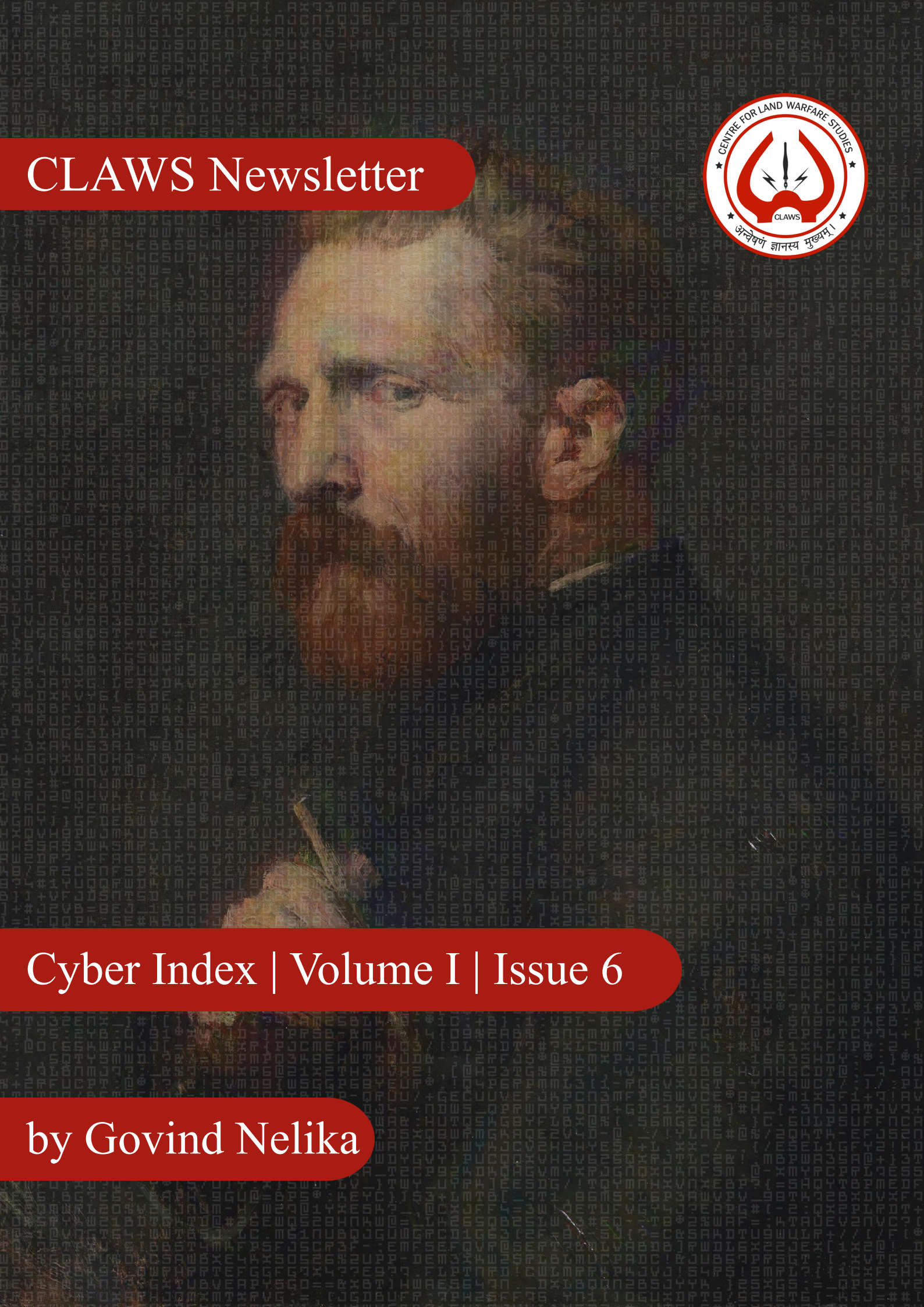
CLAWS Newsletter



Cyber Index | Volume I | Issue 6

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

Pakistan- based hackers target Armed Forces' websites, India foils repeated attempts

In the aftermath of the Pahalgam terrorist attack, which resulted in 26 fatalities, India has thwarted multiple cyberattacks targeting its Armed Forces' websites. The attacks were attributed to a Pakistan-based group known as "IOK Hacker" (Internet of Khilafah), aiming to deface pages, disrupt services, and harvest personal information. Four incidents were confirmed, involving the websites of Army Public Schools in Srinagar and Ranikhet, the Army Welfare Housing Organisation, and the Indian Air Force Placement Organisation. India's cybersecurity systems detected and isolated these threats in real-time, ensuring no operational or classified networks were compromised. These cyberattacks coincided with India's decision to ban 16 Pakistani YouTube channels for disseminating provocative and misleading content following the Pahalgam incident.

Read more: https://www.newindianexpress.com/nation/2025/Apr/29/pakistan-based-hackers-target-armed-forces-websites-india-foils-repeated-attempts

China's Huawei Develops New AI Chip, Seeking to Match Nvidia

Huawei has unveiled its most advanced artificial intelligence chip to date—the Ascend 910C—in a bold move to challenge Nvidia's dominance in the high-end AI processor market, particularly as the U.S. tightens export restrictions on advanced chips. Designed to compete with Nvidia's H100, the Ascend 910C is part of Huawei's broader strategy to achieve semiconductor self-sufficiency amidst intensifying geopolitical and trade tensions. Chinese tech giants including ByteDance and Baidu have already tested the chip, with industry sources suggesting that Huawei could receive orders worth over $2 billion. While the chip may still lag behind Nvidia's top offerings in raw performance and efficiency, it represents a major step forward for China's AI hardware capabilities.

To boost its competitiveness, Huawei is also building AI supercomputing systems using its chips, like the CloudMatrix 384, which in some scenarios can outperform Nvidia-powered systems. The Chinese government is actively supporting Huawei's efforts, recognizing domestic chip development as a national priority in light of escalating restrictions on U.S. technology exports. This development signals a potential reshaping of the global AI chip landscape, with Huawei emerging as a key player in China's bid to reduce reliance on foreign semiconductor technologies.

Read more: https://www.wsj.com/tech/chinas-huawei-develops-new-ai-chip-seeking-to-match-nvidia-8166f606

US office that counters foreign disinformation is being eliminated

The U.S. Secretary of State Marco Rubio announced the permanent closure of the State Department's Counter Foreign Information Manipulation and Interference office (R/FIMI), formerly known as the Global Engagement Center (GEC). Established in 2016 during the Obama administration, the GEC aimed to counter foreign propaganda and disinformation from adversaries such as Russia, China, and Iran. However, it faced criticism from conservative figures who accused it of suppressing domestic voices and infringing on free speech. Rubio cited these concerns, along with allegations of taxpayer fund misuse, as reasons for the shutdown.

Read more: https://www.technologyreview.com/2025/04/16/1115256/us-office-that-counters-foreign-disinformation-is-being-eliminated-say-officials/

United States of America (USA)

AMD says US rule on chips to China could cost it $800 mn

Advanced Micro Devices (AMD) has announced that it anticipates a financial impact of up to $800 million due to new U.S. export restrictions on advanced semiconductor sales to China, particularly affecting its MI308 processors. These charges are associated with inventory, purchase commitments, and related reserves. While AMD plans to apply for export licenses, there is no assurance that such licenses will be granted, especially since no licenses for GPU shipments to China have been approved by the U.S. to date. In 2024, China was AMD's second-largest market, contributing over $6.23 billion in revenue, or 24% of total sales. The export restrictions are part of measures introduced by the Trump administration, targeting high-tech trade with China amid ongoing tariff disputes. These regulatory changes have significantly impacted global technology stocks, with AMD and Nvidia shares falling over 5%.

Read more: https://www.france24.com/en/live-news/20250416-amd-says-us-rule-on-chips-to-china-could-cost-it-800-mn

Acting Pentagon CIO Signing Off on New, Faster Cyber Rules for Contractors

The U.S. Department of Defense (DoD) is launching the Software Fast Track (SWIFT) initiative to modernize and accelerate its cybersecurity approval process for software used by military contractors. Announced by Acting Pentagon CIO Katie Arrington, SWIFT aims to replace the outdated Authorization to Operate (ATO) and Risk Management Framework (RMF) processes, which have long been criticized for causing significant delays due to their complexity and heavy documentation requirements. SWIFT will leverage artificial intelligence to automate and expedite the evaluation process. Contractors must submit Software Bills of Materials (SBOMs)—detailed inventories of software components—for both sandbox and production environments. These must be independently certified and uploaded to the Enterprise Mission Assurance Support Service (eMASS), with data also integrated into the Supplier Performance Risk System (SPRS) to monitor cybersecurity compliance and contractor performance.

AI systems will assess these inputs and, if requirements are met, issue provisional ATOs without human intervention—dramatically shortening the time to deployment. Unlike earlier initiatives like the Air Force's 2019 "Fast Track ATO," which focused only on accelerating assessments, SWIFT revises the core criteria for software approval. This effort marks a significant shift in how the Pentagon approaches cybersecurity—prioritizing real-time, data-driven decisions to enhance both security and the speed of technology adoption in defence systems.

Read more: https://www.airandspaceforces.com/acting-pentagon-cio-faster-cyber-rules-contractors/

Exclusive: Every AI Datacenter Is Vulnerable to Chinese Espionage, Report Says

A recent report by Gladstone AI, reviewed by the Trump administration, warns that U.S. AI datacenters are highly susceptible to Chinese espionage and sabotage, posing significant national security risks. The report highlights vulnerabilities in critical infrastructure, including the potential for low-cost attacks to incapacitate datacenters for extended periods. It also notes that many essential components for these facilities are manufactured in China, increasing the risk of supply chain disruptions. Furthermore, the report raises concerns about the security of AI labs and the possibility of advanced AI models exhibiting autonomous behaviors that could escape containment. The authors urge immediate action to enhance the security of AI infrastructure to safeguard against these threats.

Read more: https://time.com/7279123/ai-datacenter-superintelligence-china-trump-report/

The People's Republic of China | China

China States NSA orchestrated sophisticated cyberattacks

Chinese authorities in Harbin said the U.S. National Security Agency (NSA) of orchestrating sophisticated cyberattacks during the February Asian Winter Games. The alleged attacks targeted critical infrastructure in Heilongjiang province, including energy, transportation, and defense sectors. Chinese police named three NSA agents—Katheryn A. Wilson, Robert J. Snelling, and Stephen W. Johnson—as suspects and issued warrants for their arrest. Additionally, the University of California and Virginia Tech were cited as being involved, though specific details were not provided

Read more: https://www.jpost.com/breaking-news/article-850152

ByteDance Sells Nvidia GPUs to Tencent and Alibaba Amid U.S. Export Restrictions

In response to stringent U.S. export controls on advanced AI chips, Chinese tech giants Tencent and Alibaba have procured Nvidia GPUs from ByteDance, the parent company of TikTok. ByteDance had previously amassed a substantial inventory of Nvidia's H20 chips, valued at approximately $13.7 billion, prior to the implementation of the latest U.S. restrictions. The H20 chip, tailored for the Chinese market to comply with U.S. export regulations, has become a critical component for AI development within China. ByteDance's foresight in stockpiling these chips has not only bolstered its own AI initiatives but also positioned it as a key supplier to other major Chinese tech firms. This internal redistribution of AI hardware highlights the collaborative efforts among Chinese technology companies to navigate and mitigate the challenges posed by international trade restrictions. It also underscores the strategic importance of securing essential technological resources to sustain AI innovation and competitiveness in the global arena.

Read more: https://www.techinasia.com/news/tencent-alibaba-buy-nvidia-gpus-bytedance

Baltic subsea cable damage may not be deliberate, say Swedish authorities

Swedish authorities have concluded that the damage to two undersea fiber-optic cables in the Baltic Sea in November 2024 was likely accidental, with no definitive evidence of deliberate sabotage. The cables affected were the BCS East-West Interlink, connecting Gotland, Sweden, to Lithuania, and the C-Lion1 cable, linking Helsinki, Finland, to Rostock, Germany. Investigations revealed that the Chinese bulk carrier Yi Peng 3 was present in the vicinity during the incidents and may have inadvertently damaged the cables by dragging its anchor. However, authorities have not determined whether the damage was intentional or accidental. The investigation remains open, with deliberate sabotage not entirely ruled out.

Read more: https://totaltele.com/no-sign-baltic-subsea-cable-damage-was-deliberate-say-swedish-authorities/

How China's rare-earth curbs complicate West's rare mineral supply chain

China's recent restrictions on rare earth exports have intensified challenges for Western nations striving to diversify their supply chains. As the dominant global supplier, China controls approximately 70% of rare earth extraction and 90% of neodymium magnet production. These materials are critical for technologies such as semiconductors, electric vehicles, and renewable energy systems. In response to escalating trade tensions, China halted exports of seven rare earth elements in April 2025, requiring exporters to obtain licenses—a process that has already disrupted shipments and led to force majeure declarations. This move underscores China's strategic use of its rare earth dominance, previously demonstrated during the 2010 dispute with Japan. The United States and European Union have recognized the vulnerability posed by reliance on Chinese rare earths. Efforts to establish alternative supply chains include partnerships with countries like Ukraine and investments in domestic production. However, experts caution that developing robust nonchains supply chains

could take a decade or more.

Read more: https://asia.nikkei.com/Business/Technology/Tech-Asia/How-China-s-rare-earth-curbs-complicate-West-s-diversification-push

European Union

China-Linked Hackers Lay Brickstorm Backdoors on Euro Networks

Cybersecurity researchers at Belgian firm Nviso uncovered Windows-based variants of the Brickstorm backdoor malware within European critical infrastructure networks. Previously identified in Linux environments, particularly on VMware vCenter servers, Brickstorm is associated with the China-linked threat group UNC5221. This group has been implicated in significant cyber-espionage activities, including a notable breach of the MITRE Corporation's systems. The Windows variants of Brickstorm discovered by Nviso possess capabilities such as file system navigation, file and directory manipulation, and network tunneling to facilitate lateral movement within compromised networks. These functionalities enable attackers to maintain persistent access and potentially exfiltrate sensitive data. Nviso's findings indicate that these Windows-based backdoors have been operational since at least 2022, remaining undetected until recent incident response efforts. The targeted organizations operate in sectors deemed strategically significant to the People's Republic of China, suggesting a focused cyber-espionage campaign aligned with national interests. The prolonged undetected presence of such malware underscores the evolving sophistication of state-sponsored cyber threats and highlights the necessity for enhanced detection and response strategies within critical infrastructure sectors.

Read more: https://www.darkreading.com/vulnerabilities-threats/china-linked-hackers-brickstorm-backdoors-european-networks?

Dutch Military Intelligence and Security Service annual report highlights Russia's alleged attempt to disrupt 2024 European elections.

The Dutch Military Intelligence and Security Service (MIVD) has reported a significant escalation in Russian hybrid warfare targeting the Netherlands and other European nations. According to MIVD's 2024 annual report, Russia attempted to disrupt the 2024 European elections by launching cyberattacks on websites belonging to Dutch political parties and public transport companies, aiming to hinder Dutch citizens' ability to vote. This marks the first known instance of such cyber sabotage by Russian actors within the Netherlands. MIVD Director Vice Admiral Peter Reesink emphasized that the Russian threat against Europe is not diminishing but increasing, even after a potential end to the war with Ukraine. He highlighted the unprecedented speed and potential impact of these developments on European security. The report also notes that Russian military intelligence, particularly the GRU's Unit 29155, is involved in preparing for destructive cyber operations against vital infrastructure and government institutions in Western countries. These operations aim to disrupt Western support for Ukraine, undermine NATO cohesion, and spread pro-Russian sentiment.

Read more: https://www.politico.eu/article/russia-increasing-hybrid-attacks-against-europe-dutch-intel-agency-warns/

'Choose Europe!': Macron invites scientists to work in France amid US funding cuts

French President Emmanuel Macron has launched the "Choose France for Science" initiative, inviting international scientists to work in France or elsewhere in Europe. This move comes amid significant funding cuts to research institutions in the U.S. under President Donald Trump's administration, which has led to layoffs and increased political tensions over academic freedom. The initiative, operated by France's National Research Agency (ANR), offers co-funding to host international researchers in key areas such as health, climate change, artificial intelligence, space, agriculture, low-carbon energy, and digital systems. The ANR empha-

sized France's commitment to defending academic freedom and highlighted the growing global mobility of researchers as an opportunity for Europe to attract top scientific talent. Macron's call has been echoed by European Commission President Ursula von der Leyen, who invited scientists and researchers worldwide to settle in Europe, emphasizing the EU's commitment to freedom of science and open academic debate.

Read more: https://www.france24.com/en/france/20250419-choose-europe-macron-invites-scientists-to-work-in-france-amid-us-funding-cuts

Middle East

Israel using AI to pinpoint Hamas leaders, find hostages in Gaza tunnels — report

Israel is leveraging advanced artificial intelligence (AI) systems—primarily "The Gospel" and "Lavender"—to identify Hamas operatives and uncover hostages hidden within Gaza's complex tunnel networks. These AI tools process vast amounts of surveillance and intelligence data to rapidly detect potential targets. "The Gospel" focuses on locating Hamas-related infrastructure, while "Lavender" compiles profiles of individuals affiliated with the group. Once targets are flagged, human analysts review and authorize any military actions. The integration of AI has significantly accelerated Israel's military response. On the first day of a recent ground offensive, the Israel Defense Forces (IDF) used AI to strike 150 tunnel sites. Since the escalation of conflict on October 7, over 11,000 targets have reportedly been hit in Gaza, with 90% identified through real-time collaboration between AI systems and intelligence teams. However, the growing reliance on AI in warfare has sparked ethical and legal concerns. Critics argue that automated targeting can increase the risk of civilian casualties and complicate accountability. Reports indicate that the IDF employed pre-approved thresholds for civilian casualties depending on the rank of the Hamas target, with higher allowances for senior operatives compared to lower-ranking individuals.

Read more: https://www.timesofisrael.com/israel-using-ai-to-pinpoint-hamas-leaders-find-hostages-in-gaza-tunnels-report/

Russian Federation

Android spyware trojan targets Russian military personnel

Doctor Web's cybersecurity experts have uncovered a sophisticated Android spyware trojan, dubbed Android.Spy.1292.origin, which is specifically targeting Russian military personnel. This malware is concealed within a tampered version of the popular Alpine Quest mapping application, widely used by Russian soldiers in operational zones.The malicious variant masquerades as a free version of Alpine Quest Pro and is disseminated through various channels, including a counterfeit Telegram channel and Russian Android app catalogs. Once installed, the trojan operates covertly, mimicking the legitimate app's functionality to evade detection. This targeted cyber-espionage campaign underscores the increasing use of legitimate-looking applications to infiltrate devices and extract confidential information, highlighting the need for heightened vigilance and robust cybersecurity measures among military personnel

Read more: https://news.drweb.com/show/?i=15006&lng=en

Republic of Korea

Lazarus hackers breach six companies in watering hole attacks

North Korea's Lazarus Group has launched a sophisticated cyber-espionage campaign, dubbed Operation SyncHole, targeting at least six organizations in South Korea's software, IT, finance, semiconductor manufacturing, and telecommunications sectors between November 2024 and February 2025. The attackers employed

a watering hole attack strategy, compromising websites frequented by employees of the targeted sectors. They exploited a known vulnerability in a widely used file transfer client essential for completing various financial and administrative tasks in South Korea. This vulnerability had been previously identified by the software vendor but remained unpatched during the time of the attacks. Kaspersky researchers, who uncovered the campaign, believe that the actual number of affected organizations is likely higher, given the widespread use of the exploited software across different industries. The operation underscores the persistent threat posed by state-sponsored hacking groups and the critical importance of timely software updates and robust cybersecurity measures.

Read more: https://www.bleepingcomputer.com/news/security/lazarus-hackers-breach-six-companies-in-watering-hole-attacks/

Malware & Vulnerabilities

Weaponized Words Uyghur Language Software Hijacked to Deliver Malware

Member's of the World Uyghur Congress were targeted in a spearphishing campaign that delivered malware through a trojanized version of a legitimate Uyghur language word processor. The compromised software, originally developed by a trusted community member, was used to install spyware on Windows systems, enabling remote surveillance of the victims. The malware was embedded in a password-protected archive shared via Google Drive links in emails impersonating a known contact. This attack is part of a broader pattern of digital transnational repression—likely state-backed—aimed at surveilling and intimidating Uyghur diaspora communities through the exploitation of culturally significant software.

Read more: https://citizenlab.ca/2025/04/uyghur-language-software-hijacked-to-deliver-malware/

State-Sponsored Hackers Weaponize ClickFix Tactic in Targeted Malware Campaigns

State-sponsored hacking groups from Iran, North Korea, and Russia have been observed employing the "ClickFix" social engineering tactic to deploy malware in targeted phishing campaigns. The groups involved include TA427 (Kimsuky), TA450 (MuddyWater), UNK_RemoteRogue, and TA422 (APT28). ClickFix, initially associated with cybercriminals, involves deceiving users into executing malicious commands under the guise of resolving technical issues or completing routine tasks. For instance, TA427 targeted individuals in the think tank sector by initiating contact through spoofed emails, leading victims to execute PowerShell commands that ultimately installed the Quasar RAT, a remote access trojan. Similarly, TA450 lured targets to counterfeit embassy websites, prompting them to run scripts that downloaded malware. These campaigns highlight a shift in state-sponsored cyber operations, adopting tactics traditionally used by cybercriminals to enhance the effectiveness of their attacks. The use of ClickFix by multiple nation-state actors within a short timeframe underscores its perceived efficacy and the evolving landscape of cyber threats. This development raises concerns about the increasing sophistication of phishing techniques and the need for heightened awareness and defensive measures against such social engineering attacks.

Read more: https://thehackernews.com/2025/04/state-sponsored-hackers-weaponize.html?

Renewed APT29 Phishing Campaign Against European Diplomats

Check Point Research identified a sophisticated phishing campaign orchestrated by APT29, a Russian state-linked cyber-espionage group also known as Cozy Bear or Midnight Blizzard. This operation targeted European diplomatic entities, including ministries of foreign affairs and foreign embassies within Europe. The attackers impersonated a major European Ministry of Foreign Affairs, distributing emails that invited recipients to wine tasting events. These emails contained links leading to the download of a malicious loader named GRAPELOADER. GRAPELOADER serves as an initial-stage tool, performing system fingerprinting, estab-

lishing persistence, and delivering additional payloads. Subsequently, a new variant of the modular backdoor WINELOADER is deployed in later stages of the attack. Both GRAPELOADER and the updated WINELOADER share similarities in code structure, obfuscation, and string decryption, with GRAPELOADER introducing enhanced stealth techniques. This campaign underscores APT29's continued focus on high-value diplomatic targets and their evolving tactics to bypass security measures. The use of culturally themed lures, such as wine tasting invitations, demonstrates the group's strategic social engineering capabilities. The discovery of this campaign highlights the persistent threat posed by state-sponsored actors to international diplomatic communications and the importance of robust cybersecurity measures within governmental organizations.

Read more: https://research.checkpoint.com/2025/apt29-phishing-campaign/

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.