

CLAWS Newsletter



Cyber Index | Volume I | Issue 01

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 defence policies and military preparedness.

The CLAWS Fortnightly Newsletter is a newly initiated series under the leadership of Dr. Tara Kartha, Director Research & Academic. 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.

WhatsApp says spyware company Paragon targeted users

Meta's recent confirmation of a zero-click vulnerability in WhatsApp underscores the evolving risks posed by sophisticated spyware. The exploit, discovered by Citizen Lab, allowed attackers—allegedly linked to spyware company Paragon—to infiltrate users' devices without any interaction from the target. This method is particularly concerning as it bypasses traditional security awareness measures, such as avoiding suspicious links or attachments.

The attack specifically targeted high-risk individuals, including journalists, human rights activists, and political dissidents, reflecting the increasing weaponization of spyware for surveillance and repression. While Meta has patched the vulnerability, the incident raises broader concerns about the persistent vulnerabilities in widely used communication platforms and the capabilities of private-sector spyware firms.

This case highlights the need for continuous software updates, proactive security measures, and policy-level discussions on the regulation of spyware technologies. As zero-click exploits become more prevalent, both users and organizations must adopt robust cybersecurity strategies, including the use of encrypted messaging, device monitoring, and threat intelligence to mitigate risks.

For further details : <https://thehackernews.com/2025/02/meta-confirms-zero-click-whatsapp.html?m=3n%2e009a%2e3581%2eoc0ao452lz%2e2loi>

Foreign Influence and the Digital Manipulation of Sectarian Divides in Syria

The Defence & Security Information Analysis (DISA) Center's report sheds light on the growing impact of foreign influence and disinformation campaigns in post-Assad Syria, revealing how geopolitical actors exploit sectarian tensions to further destabilize the country. By leveraging social media and digital platforms, these actors engage in propaganda efforts designed to manipulate public opinion, incite violence, and deepen societal fractures.

The study outlines key tactics used in these operations, including the spread of fake news, the amplification of inflammatory narratives through bots and trolls, and the strategic use of disinformation to erode trust in institutions. Given Syria's prolonged conflict and fragile social fabric, such campaigns pose a significant threat to national reconciliation efforts and long-term stability.

Addressing these challenges requires a multi-faceted approach. The report underscores the urgency of media literacy programs, civil society empowerment, and inter-communal dialogue as critical tools to counter disinformation. Additionally, it highlights the necessity of tackling the root causes of sectarianism and fostering inclusive governance to build a more resilient Syrian state. Without such measures, foreign actors will continue to exploit existing divisions, prolonging instability and hindering post-conflict reconstruction.

For further details : <https://disa.org/foreign-influence-and-disinformation-campaigns-exacerbating-sectarian-instability-in-post-assad-syria/>

The Rise of "Crazy Evil" and the Evolution of Social Media Scams

The emergence of the cybercriminal group "Crazy Evil" highlights the increasing sophistication of social media scams and their impact on unsuspecting users. As reported by Security Affairs, the group operates at least 10 highly specialized fraud schemes, leveraging tactics such as fake giveaways, phishing campaigns, and romance scams to deceive victims into divulging sensitive information or transferring money.

What sets Crazy Evil apart is its strategic use of social engineering techniques, making scams appear legitimate and difficult to detect. The article underscores the financial and psychological toll these schemes impose

on victims, many of whom are manipulated into making irreversible transactions. As social media continues to be a primary channel for digital interactions, cybercriminals are refining their methods, exploiting both technological vulnerabilities and human psychology.

Countering such threats requires a two-pronged approach: user awareness and platform accountability. Individuals must remain cautious by verifying accounts, questioning too-good-to-be-true offers, and safeguarding personal data. At the same time, social media companies must implement stronger fraud detection mechanisms, enhance user reporting systems, and proactively remove malicious accounts before they cause harm. Without these measures, groups like Crazy Evil will continue to exploit the digital landscape for financial gain.

For further details : <https://securityaffairs.com/173784/cyber-crime/crazy-evil-runs-10-social-media-scams.html>

Germany's Proactive Strategy Against Social Media Election Interference

As concerns over election security grow worldwide, Germany is taking a proactive stance against potential social media interference ahead of its federal election. According to Politico, German authorities are implementing a multi-layered defense strategy to combat disinformation and manipulation on platforms like TikTok, Meta, and X (formerly Twitter).

Key measures include collaborations with social media companies to swiftly identify and remove misleading content, as well as public awareness campaigns to educate citizens about online manipulation tactics. Additionally, the establishment of a dedicated task force signals a heightened commitment to monitoring and responding to emerging threats in real time.

This approach reflects a broader acknowledgment of the growing vulnerability of democratic processes to digital interference. By fostering cooperation between government agencies and tech platforms, Germany is positioning itself as a model for election integrity efforts in the digital age. However, the effectiveness of these measures will ultimately depend on their ability to adapt to evolving threats and ensure that disinformation campaigns are neutralized before they influence public opinion and voter behavior.

For further details : <https://www.politico.eu/article/german-authorities-prepared-social-media-election-interference-tiktok-meta-x/>

Poland's Pegasus Scandal and the Threat to Democratic Integrity

The arrest of former Polish Justice Minister Zbigniew Ziobro marks a major turning point in the ongoing spyware controversy that has shaken Poland's political landscape. As reported by The Record, Ziobro—an influential figure in the ruling Law and Justice party—is accused of authorizing the illegal use of Pegasus spyware to surveil political opponents and journalists. This development not only exposes the potential for government overreach but also raises pressing concerns about the erosion of privacy rights and democratic norms in Poland.

The revelations surrounding Pegasus spyware have already fueled public outrage and intensified calls for greater accountability. The case underscores broader international concerns about the unchecked use of surveillance technology by governments and the lack of legal safeguards to prevent abuse. While Poland's handling of this scandal will be closely watched, it also serves as a warning to other nations about the dangers of weaponizing digital surveillance for political gain.

Moving forward, the situation highlights the urgent need for stronger regulatory frameworks, increased transparency, and independent oversight to ensure spyware tools are not misused against civil society and political opposition. As scrutiny over state surveillance intensifies globally, this case could have far-reaching implications for how democracies regulate spyware and protect fundamental rights.

For further details : <https://therecord.media/poland-spyware-former-justice-minister-arrested>

Japan's Export Controls and the Global Tech Power Struggle

Japan's decision to tighten export controls on semiconductors and quantum computing technology signals a strategic shift in the global race for technological supremacy. As reported by Bloomberg, these restrictions—though not explicitly naming China—are widely perceived as a response to concerns over Beijing's advancements and potential military applications of cutting-edge technologies.

This move aligns with a broader global trend in which nations are imposing stricter controls on critical technologies to safeguard national security. Similar measures have been taken by the U.S. and its allies, reflecting increasing concerns about the weaponization of emerging technologies and supply chain vulnerabilities. However, such restrictions could also have economic repercussions, as Japanese tech firms may face limited market access and reduced revenue opportunities in key regions.

Japan now faces the challenge of balancing economic interests with national security priorities, navigating a geopolitical landscape where technological innovation is increasingly intertwined with defense strategies. The effectiveness of these export controls will depend on international cooperation and whether they truly curb adversarial technological advancements—or simply accelerate the drive for domestic alternatives in restricted markets.

For further details : <https://www.bloomberg.com/news/articles/2025-01-31/japan-plans-to-curb-exports-of-chips-quantum-computing-tech>

US Government websites are disappearing in real time

The unexplained disappearance of U.S. government websites raises serious concerns about data security, transparency, and public service continuity. As Wired reports, the sudden vanishing of these sites—without official explanations—has fueled speculation about potential technical failures, cyber threats, or systemic mismanagement.

Government websites serve as critical infrastructure, providing citizens with access to essential services, legal resources, and public records. Their disappearance poses immediate risks, including data loss, service disruptions, and diminished public trust in government institutions. Whether due to cyberattacks, budget cuts, or poor oversight, the lack of transparency surrounding these incidents only exacerbates public concern.

This situation highlights the urgent need for greater accountability in how government agencies maintain, secure, and communicate changes to digital platforms. Proactive measures—such as regular audits, public disclosure of downtime causes, and stronger cybersecurity policies—are essential to prevent further disruptions and safeguard public access to critical information.

Without swift action, these disappearances risk undermining confidence in digital governance and leaving gaps in services that millions of citizens rely on daily.

For further details : <https://www.wired.com/story/us-government-websites-are-disappearing-in-real-time/>

China's Pushback Against Japan's High-Tech Export Controls

China's strong opposition to Japan's planned export restrictions on semiconductors and quantum computing components underscores the geopolitical and economic stakes in the ongoing global tech race. As reported by the South China Morning Post, Beijing has urged Tokyo to reconsider, warning that these measures could strain bilateral relations and disrupt supply chains.

Japan's move mirrors U.S.-led efforts to curb China's access to critical technologies, reinforcing a broader Western strategy to limit Beijing's advancements in strategic sectors. While framed as a national security measure, the restrictions also carry significant economic risks for Japanese companies that rely on Chinese markets for revenue and supply chain stability.

This standoff raises concerns about accelerating tech decoupling between China and the West, potentially leading to fragmented supply chains and increased competition for technological self-sufficiency. If Japan proceeds with these restrictions, it may deepen existing economic and diplomatic tensions, pushing China to further invest in domestic alternatives and strategic alliances to counterbalance Western controls.

Ultimately, the situation highlights the delicate balance between national security, economic interests, and geopolitical stability—a challenge that will continue shaping global technology policies in the years ahead.

For further details : <https://www.scmp.com/news/china/diplomacy/article/3296983/china-urges-japan-re-think-planned-hi-tech-export-bans>

The Risks of Adopting DeepSeek AI for Australian Companies

While DeepSeek is gaining attention for its affordability and accessibility, the Australian Strategic Policy Institute (ASPI) Strategist warns that businesses must approach it with caution. The lack of transparency surrounding this open-source AI model raises concerns about data integrity, security vulnerabilities, and potential biases.

One of the key risks is the uncertainty about the dataset and training methodology behind DeepSeek. Without clear oversight, companies may unknowingly integrate an AI model that carries hidden biases, security loopholes, or even backdoor vulnerabilities. The article underscores the growing concerns over AI governance, particularly when adopting models from lesser-known or unverified sources.

To mitigate these risks, due diligence and robust security measures must be prioritized. Australian companies are urged to evaluate AI tools carefully, ensuring they align with ethical standards, cybersecurity best practices, and regulatory compliance. While open-source AI presents cost advantages, businesses must weigh these benefits against the potential for unintended consequences—ranging from data breaches to flawed decision-making.

This case highlights the broader challenge of balancing AI innovation with security and trust, a critical issue as businesses increasingly integrate machine learning into core operations.

For further details : <https://www.aspistrategist.org.au/deepseek-may-be-cheap-ai-but-australian-companies-should-beware/>

The Strategic Risks of North Korea Leveraging DeepSeek AI

North Korea's growing cyber capabilities and history of aggressive digital warfare raise serious concerns about its potential use of China's open-source AI model, DeepSeek, for military and cyber operations. As NK News highlights, access to advanced AI tools could enable Pyongyang to conduct more sophisticated cyberattacks, enhance intelligence operations, and refine its propaganda strategies.

DeepSeek's open-source nature makes it an attractive asset for authoritarian regimes, allowing North Korea to develop AI-driven cyber weapons with minimal oversight or external restrictions. This could amplify the scale and efficiency of cyber espionage, ransomware campaigns, and disinformation efforts, posing a significant threat to global security.

The proliferation of powerful AI tools among state-sponsored cyber actors underscores the urgent need for

international cooperation. Nations must work together to monitor AI weaponization, strengthen cybersecurity defenses, and implement regulatory frameworks that prevent hostile entities from exploiting cutting-edge technologies. As AI continues to reshape cyber warfare and intelligence strategies, the global community must stay ahead of emerging threats to prevent rogue states like North Korea from leveraging AI for malicious geopolitical agendas.

For further details : <https://www.nknews.org/pro/how-north-korea-could-leverage-chinas-deepseek-ai-model-for-military-cyber-ops/>

The Converging Threat Landscape in U.S. Homeland Security for 2025

The 2025 Homeland Security Threat Forecast, as outlined by Small Wars Journal, highlights the growing intersection of terrorism, cyber warfare, and internal security risks, creating a multi-faceted challenge for U.S. security agencies.

One of the key takeaways is the increasing sophistication of terrorist organizations in leveraging cyber tactics for recruitment, propaganda dissemination, and attack coordination. The report also underscores the vulnerability of critical infrastructure, warning that cyberattacks could have severe national security and public safety consequences—potentially disrupting power grids, financial systems, and emergency response networks.

To counter these evolving threats, the article stresses the need for a comprehensive, integrated approach, involving government collaboration with the private sector and local communities. It calls for increased investment in cybersecurity, enhanced intelligence-sharing mechanisms, and proactive community engagement to strengthen national resilience.

As threats become more interconnected and unpredictable, adaptive security strategies—including AI-driven threat detection, cross-agency cooperation, and robust public-private partnerships—will be crucial in safeguarding the U.S. homeland against emerging dangers.

For further details : <https://smallwarsjournal.com/2025/02/03/2025-homeland-security-threat-forecast-the-converging-nature-of-terrorism-cyber-and-internal-threats/>

DeepSeek's Role in Shaping the US-China Tech War

As China's DeepSeek AI advances, its success could undermine U.S. efforts to restrict China's technological rise, intensifying the ongoing US-China tech war, according to The Financial Times. This development underscores the geopolitical stakes of AI supremacy, particularly in areas such as autonomous weapons, cyber capabilities, and military strategy.

The lack of international regulations on AI-powered warfare raises concerns about an unchecked arms race, where AI-driven decision-making could escalate conflicts without human oversight. DeepSeek's open-source nature further complicates control efforts, as it could enable adversarial states to develop advanced AI applications outside Western regulatory influence.

This situation highlights the urgent need for global dialogue on AI governance, particularly regarding autonomous weapons and ethical safeguards. Without international cooperation, the militarization of AI could lead to destabilizing consequences, making conflict less predictable and more dangerous.

Ultimately, DeepSeek's impact extends beyond technological competition—it represents a shifting power dynamic that could reshape global security policies and challenge the U.S.-led efforts to contain China's AI development.

For further details : <https://www.ft.com/content/3549cc33-e04d-41da-8c58-525d5bb2ba4c>

Strengthening Global AI Collaboration Beyond the AI Action Summit

The AI Action Summit, as analyzed by the OECD AI blog, underscores the critical need for international cooperation in addressing both the challenges and opportunities presented by artificial intelligence. The post outlines three key steps to enhance global AI collaboration:

1. **Building Trust Through Transparency & Accountability.** The foundation of effective AI governance lies in ensuring transparency and accountability. By fostering open dialogue among stakeholders, nations can establish shared principles that promote responsible AI deployment while mitigating risks such as bias, misinformation, and unethical applications.
2. **Encouraging Innovation Through Data Sharing & Open Science,** While AI progress relies on data accessibility and collaborative research, it must be balanced with strong privacy protections and cybersecurity measures. The article advocates for cross-border data-sharing frameworks that respect ethical and legal boundaries while fueling AI advancements.
3. **Bridging the Digital Divide for Inclusive AI Development.** The disparity in AI capabilities between nations poses risks of inequitable progress.

To ensure that AI benefits all societies, efforts must be made to democratize access, reduce algorithmic biases, and integrate diverse perspectives into AI policymaking.

Ultimately, the summit's call for continued dialogue reflects the urgency of establishing a global AI framework that prioritizes human-centered development. By harmonizing innovation with responsibility, international stakeholders can collectively shape AI's future for the benefit of humanity while mitigating its most pressing risks.

For further details : <https://oecd.ai/en/work/the-ai-action-summit-and-beyond-3-steps-to-strengthen-global-ai-collaboration>

Cybersecurity Risks Surrounding Musk's Dogecoin Development Team

As The Economic Times reports, concerns are growing over cybersecurity vulnerabilities linked to Elon Musk's Dogecoin development team. Experts warn that the lack of transparency and security expertise within the team could expose Dogecoin's decentralized network to potential attacks.

Key concerns include:

1. **Weak Security Oversight** – Without independent audits and rigorous security protocols, vulnerabilities in Dogecoin's code could be exploited by hackers, phishing schemes, or 51% attacks.
2. **Decentralization Risks** – While decentralization is a core strength of cryptocurrencies, it also presents challenges in enforcing security standards, especially if key developers lack expertise in preventing exploits and breaches.
3. **Accountability & Transparency** – The Dogecoin community lacks the formal security governance seen in Bitcoin or Ethereum, raising questions about who is responsible for maintaining and securing the network.

The article stresses the urgent need for independent security audits and greater accountability within the Dogecoin ecosystem. Without these safeguards, Dogecoin users could face increased exposure to fraud, theft, and systemic risks—potentially undermining its credibility and long-term viability.

For further details : <https://economictimes.indiatimes.com/news/international/global-trends/musks-doge-team-raises-major-cyber-security-concerns/articleshow/118197137.cms?from=mdr>

China announces measures against Google, other US firms, as trade tensions escalate

China's State Administration for Market Regulation (SAMR) has launched an anti-monopoly investigation into Google's business practices, signalling a renewed effort to regulate foreign tech firms amid escalating US-China trade tensions, according to Reuters. While the specific details of the probe remain unclear, it highlights Beijing's increasing scrutiny of Big Tech companies, particularly foreign firms operating within China. The investigation could lead to fines, operational restrictions, or market access limitations, adding further uncertainty to Google's already challenging presence in the country.

This move appears to be part of a broader strategic response to U.S. restrictions on Chinese tech giants, such as Huawei and TikTok. As Washington enforces stricter export controls on semiconductors and AI technologies, Beijing is leveraging regulatory pressure to push back against American firms. Google, which has already faced government censorship and stiff competition from domestic rivals like Baidu and Tencent, now faces additional barriers that could further limit its role in the Chinese market.

The investigation underscores the growing fragmentation of global technology markets, as both China and the U.S. tighten regulations on foreign firms in an increasingly competitive landscape. With trade tensions escalating, multinational tech companies are caught in the crossfire of geopolitical manoeuvring, facing greater regulatory scrutiny, market restrictions, and potential operational challenges. The outcome of China's probe into Google will be closely watched, as it could set a precedent for future regulatory actions against other U.S. tech firms.

For further details : <https://www.reuters.com/technology/china-anti-monopoly-regulator-launches-probe-into-google-2025-02-04/>

The AEC's Battle Against AI-Driven Misinformation: A Complex and Ongoing Challenge

The Australian Electoral Commission (AEC) is confronting a growing threat: the use of artificial intelligence (AI) and misinformation to influence elections. While the commission is taking steps to mitigate these risks, the challenge extends beyond traditional regulatory measures due to the decentralized and covert nature of online misinformation.

A key difficulty lies in identifying and countering misleading content, especially when it is produced by advanced AI systems capable of generating convincing yet false narratives. The rapid evolution of these technologies raises concerns about the effectiveness of current monitoring mechanisms and the ethical implications of regulating digital speech. Striking a balance between combating misinformation and avoiding undue censorship remains a pressing issue.

Addressing this problem requires a multi-faceted strategy. The article argues that a collaborative effort—bringing together government agencies, technology companies, and civil society organizations—is essential. This approach should prioritize media literacy initiatives, enhanced fact-checking processes, and the establishment of ethical guidelines for AI's role in political campaigns.

Ultimately, safeguarding democratic integrity in the digital age demands a proactive and adaptive response. As misinformation tactics become more sophisticated, so too must the strategies to counter them, ensuring that electoral processes remain transparent and trustworthy.

For further details : <https://theconversation.com/the-aec-wants-to-stop-ai-and-misinformation-but-its-up-against-a-problem-that-is-deep-and-dark-248773>

Tech Espionage and National Security: The Risks of Insider Threats

A recent investigation by The Bureau of Investigative Journalism highlights a serious case of alleged corporate

espionage involving a former Google engineer. The individual is accused of accessing and attempting to sell sensitive supercomputing data to a foreign government, raising significant concerns about data security and national security risks.

This case underscores the growing threat of insider breaches within major tech companies. With corporations like Google handling vast amounts of proprietary algorithms and strategic data, the potential for exploitation by bad actors—whether for financial gain or geopolitical leverage—is a critical issue. The incident also exposes vulnerabilities in existing cybersecurity protocols, emphasizing the need for stronger internal safeguards and monitoring mechanisms to detect and prevent unauthorized access.

Beyond corporate concerns, the broader implications of such breaches extend to economic competitiveness and national security. As global competition in AI and computing intensifies, securing intellectual property becomes crucial not just for individual companies but for maintaining technological leadership on a national scale. The report ultimately raises urgent questions about how tech firms and governments can collaborate to strengthen defenses against insider threats, ensuring that sensitive innovations remain protected from foreign exploitation.

For further details : https://www.thebureau.news/p/former-google-staffer-accused-of?r=fx5&utm_medium=ios&triedRedirect=true

Global AI Governance at a Crossroads: Key Debates at the Paris Summit

As world leaders and AI experts gather for the Paris AI Summit, discussions around the responsible development and regulation of artificial intelligence are taking center stage. This high-profile event comes amid growing concerns over AI's potential risks, including job displacement, algorithmic bias, and its misuse in disinformation and security threats.

One of the key points of contention is the differing regulatory approaches between major global players. While the United States favors a more market-driven, hands-off approach to AI governance, the European Union continues to push for stricter oversight to mitigate risks. This divide underscores the ongoing challenge of establishing a unified global framework for AI regulation.

Adding to the debate is the emergence of “DeepSeek,” a newly published research paper advocating for AI safety through interpretability—an approach that emphasizes making AI decision-making processes more transparent. The report has drawn significant attention, including from former US President Donald Trump, further fueling discussions on AI's societal and geopolitical impact.

With AI's influence rapidly expanding across industries, the Paris Summit represents a pivotal moment for international cooperation. The outcome of these discussions could shape future policies, balancing innovation with safeguards to ensure AI remains a tool for progress rather than a source of unchecked risk.

For further details : <https://www.reuters.com/technology/artificial-intelligence/trump-deepseek-focus-nations-gather-paris-ai-summit-2025-02-05/>

Cracking Down on Cybercrime: The Impact of Sanctions on ZServers

The US and UK have imposed sanctions on ZServers, a Russian-based hosting provider accused of offering “bulletproof” services to cybercriminals, particularly in connection with the LockBit ransomware group. This move marks a significant escalation in international efforts to dismantle the infrastructure supporting cybercrime.

ZServers has allegedly played a key role in enabling ransomware operations, data breaches, and other illicit online activities by providing hosting that is resistant to law enforcement takedowns. By targeting the infra-

structure behind cyberattacks rather than just individual perpetrators, these sanctions signal a shift towards a more systemic approach to combating digital crime.

However, enforcing such measures remains a challenge, especially when dealing with entities operating in jurisdictions with weak cybersecurity regulations or government complicity. The effectiveness of these sanctions will depend on international cooperation and the ability to disrupt financial and operational networks tied to cybercriminal activities.

Ultimately, the action against ZServers underscores a growing global resolve to curb cyber threats at their source. It sends a clear message that nations are willing to take aggressive steps to hold not only hackers but also their enablers accountable, reinforcing cybersecurity as a top priority in international security policy.

For further details : <https://therecord.media/zservers-russia-bulletproof-hosting-us-uk-sanctions?>

The Dark Side of AI: Malicious ML Models Exploiting Hugging Face's Platform

A recent investigation has uncovered malicious machine learning (ML) models on Hugging Face, a widely used platform for AI collaboration. These models, designed to generate harmful content—including hate speech, phishing attacks, and malware—leveraged vulnerabilities in the Pickle format to evade detection. This discovery raises serious concerns about the potential misuse of AI technology for malicious purposes.

The incident highlights a critical challenge in AI security: the ease with which harmful models can be uploaded, shared, and deployed without adequate safeguards. As AI becomes more accessible, the risk of its exploitation by bad actors increases, necessitating stronger oversight and detection mechanisms.

This case underscores the need for platforms like Hugging Face to enhance their security protocols, ensuring that malicious models are identified and removed before they can cause harm. Responsible AI development requires proactive risk mitigation, including better screening processes, transparency in model deployment, and collaboration with cybersecurity experts.

Ultimately, this serves as a stark reminder that AI, while a powerful tool for innovation, can also be weaponized. To prevent its misuse, the AI community must adopt stricter security standards and remain vigilant against emerging threats in the evolving landscape of machine learning.

For further details: <https://thehackernews.com/2025/02/malicious-ml-models-found-on-hugging.html>

A New Front in the Tech War: China's Counter-Sanctions on US Biotech

China's recent counter-sanctions on US biotech firms mark a pivotal moment in the intensifying technological rivalry between the two superpowers. By targeting companies involved in cutting-edge gene-editing technologies like CRISPR, Beijing is signaling a shift from defensive measures to direct retaliation against US restrictions on its technological progress.

This move could have far-reaching consequences, particularly in the fields of scientific collaboration and innovation. As restrictions tighten on both sides, global research efforts may face significant disruptions, limiting the exchange of knowledge and slowing advancements in critical areas like biotechnology. The sanctions also underscore a broader trend of escalating competition for supremacy in emerging technologies, including artificial intelligence and semiconductors.

Beyond the immediate impact on biotech firms, this development raises concerns about the long-term fragmentation of the global technology landscape. As geopolitical tensions increasingly shape technological policies, the risk of creating parallel, non-cooperative research ecosystems grows. This division could stifle international scientific progress and reshape economic power dynamics in unforeseen ways.

Ultimately, China's counter-sanctions signal that the tech war is entering a new phase—one where both nations are willing to leverage high-stakes industries as tools of geopolitical strategy. The outcome of this stand-off will likely shape the future of innovation, global trade, and international relations for years to come.

For further details : <https://www.scmp.com/news/china/science/article/3297609/chinas-1st-counter-sanction-us-biotech-industry-marks-turning-point-tech-war?>

SmokeLoader Malware: A Cyber Weapon in the Ukraine Conflict

The resurgence of SmokeLoader malware in cyberattacks against Ukraine highlights the evolving digital battlefield amid the ongoing war with Russia. This sophisticated malware, known for its adaptability, is being deployed across multiple industries to distribute ransomware, steal sensitive data, and enable remote access for further exploitation.

SmokeLoader's recent attacks exploit a vulnerability in a widely used file archiver, allowing threat actors to infiltrate systems and execute malicious payloads undetected. Given its ability to serve as a gateway for more destructive malware, cybersecurity experts warn that its deployment could significantly disrupt Ukraine's critical infrastructure, amplifying the broader impact of the conflict.

Beyond the immediate technical threat, this wave of cyberattacks underscores the growing role of state-sponsored hacking operations in modern warfare. As Ukraine and its allies work to counter these incursions, international cooperation in intelligence sharing, threat mitigation, and cybersecurity resilience becomes increasingly crucial. Ultimately, the use of SmokeLoader in politically motivated cyberattacks highlights the need for enhanced digital defenses. As cyber warfare tactics become more sophisticated, proactive threat detection and global collaboration will be essential in safeguarding national security and preventing further escalation in the digital domain.

For further details : <https://therecord.media/smokeloader-malware-ukraine-russia?>

The Growing Threat of Supply Chain Attacks: Lessons from the VeraCore Zero-Day Exploits

The recent exploitation of zero-day vulnerabilities in VeraCore underscores the increasing danger of supply chain attacks, where cybercriminals infiltrate widely used third-party software to compromise entire networks. By injecting malicious code into VeraCore's platform, attackers were able to distribute compromised software updates, potentially impacting numerous downstream organizations.

This incident highlights the critical need for stronger security measures throughout the software development lifecycle. Companies must adopt rigorous code reviews, continuous vulnerability scanning, and secure update mechanisms to minimize the risk of exploitation. Additionally, organizations relying on third-party software must implement robust vetting processes and layered security controls to detect and mitigate potential threats.

The VeraCore breach serves as a stark reminder that even trusted software platforms are not immune to exploitation. As supply chain attacks become more sophisticated, the cybersecurity community must prioritize proactive defence strategies, fostering collaboration between software vendors, security researchers, and enterprises to strengthen resilience against these evolving threats.

For further details : <https://www.cybersecuritydive.com/news/veracore-zero-day-vulnerabilities-exploited-in-supply-chain-attacks/739784/>

Kimsuky's Evolving Tactics: PowerShell and Dropbox in Cyber Espionage

The latest cyberattack campaign by Kimsuky, a North Korean state-sponsored hacking group, demonstrates the increasing sophistication of nation-state cyber threats. By exploiting PowerShell and Dropbox, the at-

tackers have devised a stealthy method to infiltrate targeted systems, evade detection, and establish long-term access for intelligence gathering.

This campaign highlights how adversaries are leveraging trusted cloud services like Dropbox to mask malicious activity. By disguising malware as legitimate files and using PowerShell to execute it, Kimsuky effectively bypasses conventional security defenses, making detection and mitigation more challenging for targeted organizations.

The attack underscores the critical need for enhanced cybersecurity measures, particularly for entities involved in Korean affairs and other high-risk sectors. Organizations must adopt proactive defense strategies, such as restricting PowerShell usage, strengthening endpoint monitoring, and implementing multi-factor authentication for cloud services.

As Kimsuky continues to refine its tactics, this incident serves as a reminder that state-sponsored cyber threats are evolving rapidly. A multi-layered security approach, combining threat intelligence, user awareness, and advanced detection mechanisms, is essential to countering these persistent threats.

For further details : <https://www.msspalert.com/brief/ongoing-kimsuky-attack-campaign-exploits-powershell-dropbox>

Nobelium's Latest Tactic: Exploiting Microsoft Exchange to Hijack Accounts

The resurgence of Nobelium, the Russian state-backed hacking group behind the infamous SolarWinds attack, highlights the evolving nature of cyber threats. Their latest campaign exploits a newly discovered Microsoft Exchange Server vulnerability, CVE-2025-0298, allowing them to bypass authentication mechanisms and gain unauthorized remote access to critical systems.

Once inside, Nobelium can steal sensitive data, deploy malware, and potentially disrupt business operations, reinforcing the high stakes of state-sponsored cyberattacks. This incident underscores the need for organizations to prioritize cybersecurity vigilance, especially when dealing with widely used enterprise software like Microsoft Exchange.

Microsoft has responded swiftly with security updates to patch the vulnerability, but the attack serves as a crucial reminder that advanced threat actors continuously adapt their techniques. Organizations must implement robust defense strategies, including timely patch management, multi-factor authentication, and continuous monitoring, to mitigate risks from such sophisticated adversaries.

As cyber warfare tactics grow more advanced, proactive security measures and global cooperation remain essential in defending against nation-state actors like Nobelium.

For further details: <https://thehackernews.com/2025/02/microsoft-russian-linked-hackers-using.html?>

DeepSeek and the Future of AI in China: Balancing Innovation and Ethics

The recent publication of the DeepSeek research paper has sparked a complex debate within China's AI community, highlighting tensions between technological advancement and ethical responsibility. By emphasizing interpretability and transparency in AI systems, DeepSeek challenges China's traditional focus on achieving rapid technological dominance, introducing new questions about responsible development.

While the paper has gained traction among researchers and industry leaders, its reception by the Chinese government has been more measured. Given the sensitivity surrounding AI safety and concerns over foreign influence, policymakers are carefully weighing DeepSeek's implications for national security and global competitiveness. This cautious stance reflects broader geopolitical tensions, where AI is not just a tool for progress

but also a strategic asset in global power dynamics.

The long-term impact of DeepSeek on China's AI development remains uncertain. However, its emergence has ignited an important conversation about the trade-offs between innovation and accountability. As China continues to shape its AI strategy, the balance it strikes between these competing priorities will influence not only its technological trajectory but also the global discourse on ethical AI governance.

For further details: <https://chinamediaproject.org/2025/02/10/deepseeking-truth/>

Disinformation as a Strategic Threat to the Quad's Unity

The growing wave of disinformation targeting the Quadrilateral Security Dialogue (Quad) poses a serious challenge to the alliance's cohesion and effectiveness. By exploiting societal divisions, distorting the Quad's objectives, and amplifying pro-China narratives, adversaries seek to weaken trust among member nations—Australia, India, Japan, and the United States—and erode public support for the partnership.

These tactics reflect a broader strategy of information warfare, where digital platforms become battlegrounds for geopolitical influence. Misinformation about the Quad's role, particularly portrayals of it as a destabilizing force or a tool of Western hegemony, risks undermining cooperation on critical security issues, including Indo-Pacific stability and maritime security.

To counter this threat, the article calls for a unified response, emphasizing media literacy, increased platform accountability, and intelligence-sharing among Quad members. Strengthening resilience against disinformation is not just about safeguarding the alliance—it is essential for maintaining regional stability in the face of evolving geopolitical challenges.

As information warfare intensifies, the Quad's ability to counter malign influence campaigns will play a crucial role in shaping its long-term success. Proactive strategies to combat disinformation will ensure that the alliance remains a credible and effective force in the Indo-Pacific.

For further details: <https://www.aspistrategist.org.au/undermining-unity-disinformation-as-a-threat-to-the-quad/>

Strengthening U.S. Cyber Defenses: A Bipartisan Push for a Dedicated Cyber Force

As cyber threats from nation-state actors and criminal organizations continue to escalate, U.S. lawmakers are uniting to push forward a bipartisan effort to establish a dedicated cyber force within the military. This initiative reflects a growing consensus in Congress on the need for a more robust and coordinated approach to national cybersecurity.

The proposed legislation aims to create a unified cyber command structure, enhance training and recruitment of cybersecurity professionals, and improve collaboration between government agencies and the private sector. Recent high-profile cyberattacks have underscored the urgency of this effort, raising concerns about the vulnerability of critical infrastructure and national security.

Despite strong bipartisan support, the initiative faces an uncertain legislative path. However, its advancement represents a significant step toward modernizing U.S. cyber defenses and addressing the increasingly complex threats in cyberspace. If successfully implemented, the creation of a dedicated cyber force could mark a turning point in the nation's ability to deter and respond to cyberattacks effectively.

For further details: <https://www.politico.com/newsletters/weekly-cybersecurity/2025/02/10/lawmakers-unite-to-push-forward-cyber-force-00203283>

Legal Threats as a Tool to Suppress Security Research

A growing concern in the global tech landscape is the use of legal threats by Chinese companies to silence independent researchers who expose security vulnerabilities. The New York Times reports on how firms like Dahua Technology, a major surveillance technology provider, have issued cease-and-desist letters to academics who published findings on flaws in their facial recognition systems.

This tactic represents a broader effort to control the narrative around Chinese technology and deter scrutiny of its security implications. By leveraging legal pressure, these companies create a chilling effect on academic research, discouraging critical analysis that could otherwise inform public policy and consumer awareness.

The article underscores the risks such practices pose to transparency and responsible AI development. If unchecked, this trend could weaken global cybersecurity efforts and limit independent assessments of emerging technologies. Addressing this issue will require a concerted effort from governments, academic institutions, and the cybersecurity community to safeguard research integrity and promote accountability in AI and surveillance technology.

For further details: <https://www.nytimes.com/2025/02/11/technology/chinese-company-legal-threats-researchers.html?>

Sandworm's Latest Cyber Espionage Campaign: A Growing Threat to Western Organizations

The alleged Russian state-sponsored hacking group Sandworm has been caught engaging in cyber espionage, stealing credentials and sensitive data from organizations in the U.S. and U.K., according to The Register. Known for its destructive cyberattacks, Sandworm continues to evolve its tactics, leveraging advanced phishing techniques and malware to infiltrate networks and exfiltrate valuable information.

The report underscores the persistent danger posed by state-backed hacking groups and their ability to adapt to cybersecurity defenses. Organizations are urged to implement robust security measures, including multi-factor authentication, employee training, and intelligence-sharing initiatives to counteract these threats.

With cyberwarfare becoming an increasingly central tool in geopolitical conflicts, Sandworm's activities signal a continued escalation in digital espionage. The article warns that without international cooperation and proactive defense strategies, such threats will only grow more sophisticated and pervasive.

For further details: https://www.theregister.com/2025/02/12/russias_sandworm_caught_stealing_credentials/

Alexander Vinnik's Release: A Geopolitical Bargain with Cybercrime Implications

The reported release of Alexander Vinnik, a Russian cybercriminal convicted of money laundering, as part of a U.S.-Russia prisoner swap, raises significant geopolitical and cybersecurity concerns. According to The Record Media, Vinnik, who allegedly operated the BTC-e cryptocurrency exchange—linked to illicit financial activities—was exchanged for a Russian pilot convicted of drug trafficking.

This development underscores the complexity of diplomatic negotiations amid ongoing tensions between Washington and Moscow. It also raises questions about the future of cybercrime investigations, as Vinnik's release could hinder efforts to dismantle cryptocurrency-enabled financial crime networks.

With no official confirmation from either government, the circumstances of the exchange remain unclear. However, the case highlights the delicate balancing act between law enforcement priorities and geopolitical manoeuvring, particularly as cybercriminals continue to exploit cryptocurrencies for money laundering and ransomware operations.

For further details: <https://therecord.media/alexander-vinnik-reported-released-prisoner-swap-russia-us>

China's Semiconductor Surge Challenges Korean Market Leadership

A Financial Times report examines the rapid growth of China's semiconductor industry, which is increasingly threatening South Korea's dominance in the sector. The article highlights how China's leading chipmakers, buoyed by state subsidies, domestic demand, and technological advancements, are aggressively expanding production. This "snowballing" growth has raised alarms among Korean industry leaders, particularly in the memory chip market, where Samsung and SK Hynix have traditionally held a commanding presence.

The article explores China's strategic push for self-sufficiency, accelerated by U.S. export controls on advanced semiconductor technology. With Chinese firms rapidly improving their capabilities, Korean companies face mounting pressure to innovate and maintain their competitive edge. The report also discusses the potential for increased geopolitical tensions, as the U.S. and its allies seek to curb China's rise in chip manufacturing.

The article concludes by emphasizing that the global semiconductor landscape is shifting, and South Korea must adapt swiftly to retain its leadership amid China's relentless growth in the sector.

For further details: <https://www.ft.com/content/b6f89d2b-5fe2-4a8f-a7cc-c75989e27544>

China's Salt Typhoon Hackers Persist in Telecom Breaches Despite Sanctions

A TechCrunch report highlights the continued cyber espionage activities of Salt Typhoon, a Chinese hacking group allegedly linked to China's Ministry of State Security, despite U.S. sanctions aimed at curbing its operations. The group remains highly active, breaching global telecommunications firms to steal sensitive data and intellectual property.

The article details Salt Typhoon's evolving tactics, including:

- Spear-phishing campaigns targeting telecom employees.
- Malware infections to establish long-term access to networks.
- Exploiting vulnerabilities in telecom infrastructure to exfiltrate data.

Despite international sanctions, law enforcement struggles to hold state-sponsored cyber actors accountable, as attribution remains complex, and enforcement mechanisms are limited. The article underscores the ongoing cybersecurity threat posed by Salt Typhoon and similar groups, stressing the need for stronger international collaboration to counter these persistent cyberattacks.

For further details: https://techcrunch.com/2025/02/13/chinas-salt-typhoon-hackers-continue-to-breach-telecom-firms-despite-us-sanctions/?utm_source=dlvr.it&utm_medium=bluesky

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.



All Rights Reserved 2025 Centre for Land Warfare Studies (CLAWS)

No part of this publication may be reproduced, copied, archived, retained or transmitted through print, speech or electronic media without prior written approval from C L A W S.

The views expressed and suggestions made are solely of the author in his personal capacity and do not have any official endorsement. Attributability of the contents lies purely with author.