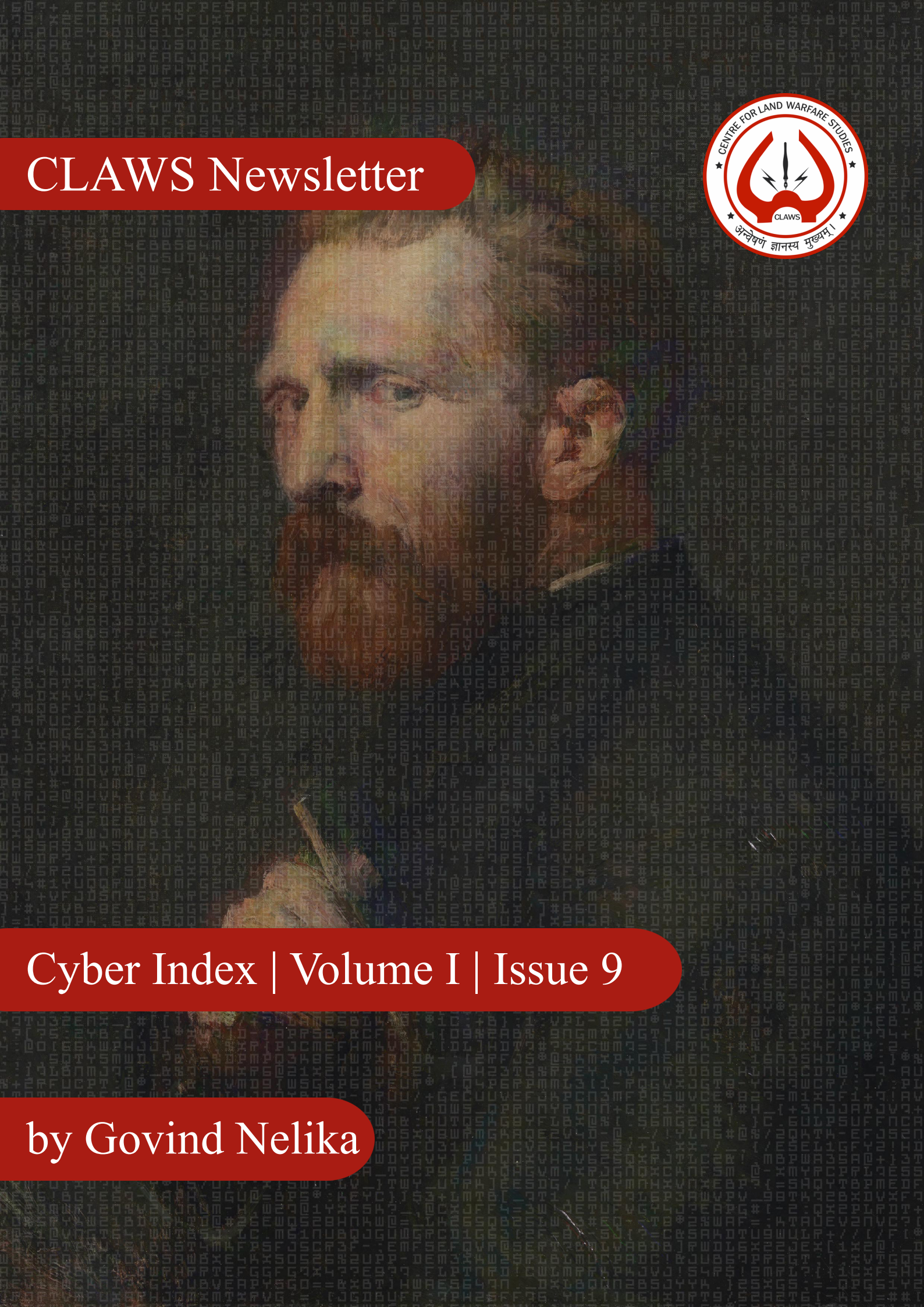
CLAWS Newsletter



Cyber Index | Volume I | Issue 9

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

Global brief

Japan, US vow to spur cybersecurity cooperation amid rising threats

Japan and the United States, responding to a surge in cyber threats, have committed to intensifying their cybersecurity partnership. Framed against the backdrop of escalating cyberattacks targeting critical infrastructure and digital supply chains, both governments assert that bolstering joint defences is essential to uphold national security and economic stability. The cooperation extends beyond mere information sharing it includes coordinated responses to incidents, shared defensive standards, and joint efforts in developing resilient technologies. Politically and strategically, the move underscores a broader commitment by both allies to assert a proactive cyber posture, countering not just isolated criminal hacking but also state linked cyber operations that threaten democratic institutions and industrial control systems. Legally, this emerging framework signals a deeper normalization of cyber diplomacy—establishing common norms of behaviour, potential incident response treaties, and possibly shared attribution mechanisms to deter malicious cyber activity.

At a deeper level, the article identifies key actors: the U.S. Cybersecurity and Infrastructure Security Agency (CISA), Japan's National Center of Incident Readiness and Strategy for Cybersecurity (NISC), as well as political leadership in both Tokyo and Washington. Their roles converge around defining policy architecture, allocating resources, and aligning legislative systems to enable more fluid, timely collaboration.

A clear cause and effect logic emerges mounting cyber threats—ranging from ransomware attacks on business and energy sectors to intrusions into government databases—have pressured both nations to transcend siloed national strategies. In turn, this has catalysed institutional integration: agreeing on shared intelligence systems, joint cyber exercises, and legal harmonization. The broader significance is twofold: geopolitically, Japan endeavours to anchor itself more robustly within U.S.-led deterrence architectures—mirroring partnerships like AUKUS—and domestically, it must adapt its legal and regulatory regimes to support rapid, cross-border cyber cooperation.

Societally, enhanced cybersecurity coordination promises strengthened protections for citizens against digital fraud, service interruptions, and potential civil liberties intrusions, though it also raises legal policy questions about surveillance boundaries and transparency. Strategically, this trilateral alignment may embolden Japan and the U.S. to more confidently push back against malicious cyber behaviour from adversaries, reinforcing a rules based international cyber order.
In essence, the article's core message is that the intensifying digital threat environment is forging a closer, more systemic cyber alliance between Japan and the U.S. That alliance carries weighty geopolitical, legal, and societal implications—it reshapes how nation states defend critical systems, codify cyber norms, and confront adversarial states and criminal actors in the digital domain.

Read more: https://mainichi.jp/english/articles/20250531/p2g/00m/0na/031000c

South Korea election hit by misinformation

South Korea's recent presidential election (held on June 3, 2025) was significantly affected by a wave of misinformation campaigns involving state-backed and partisan actors. Social media platforms widely circulated fake news, including fabricated endorsements (such as claims that former US President Donald Trump had publicly backed fringe candidates) . These deliberate disinformation efforts exploited heightened geopolitical tensions—with an eye on both internal political polarization and looming threats from regional rivals—as well as technological vulnerabilities in election infrastructure and online platforms.The tactics deployed included AI-generated messages and deepfakes—leveraging tools capable of creating convincing audio, images, and text—to manipulate public opinion.

These deceptions were amplified through coordinated bot networks and inauthentic social-media accounts, strategically timed to coincide with the campaign's final weeks . Although South Korea implemented a legal

ban on deepfakes and mandated disclosure for AI-generated political content—including possible criminal penalties up to seven years in prison and fines for violations within 90 days of the vote—monitoring showed over a hundred flagged deepfake-related infractions in just a fortnight before the legislative elections in 2024.

The National Election Commission faced sharp criticism from voters at campaign rallies, with demands for greater accountability amid perceptions that existing measures had proven insufficient. Meanwhile, content-tracking efforts by domestic tech firms (like Naver) and startups (such as those specializing in deepfake detection) proved helpful in identifying and flagging manipulated content. Yet enforcement challenges remain—particularly involving foreign-hosted platforms and the use of VPNs, which obscure the origin of malicious campaigns Strategically, this surge in election-related disinformation amplifies national security concerns: it undermines public trust in electoral integrity, deepens domestic polarization, and opens a pathway for external influence—whether by geopolitical rivals or non-state actors. The situation underscores a global trend: the struggle to regulate AI enabled misinformation, prevent covert influence in democratic processes, and build resilient systems that can withstand adversarial technological tactics without eroding free expression.

Read more: https://www.france24.com/en/live-news/20250601-south-korea-election-hit-by-misinformation

United States of America (USA)

Cyber cuts are freaking out China watchers

The U.S. federal government's proposed reductions to cybersecurity funding, provoking alarm among China-focused analysts. Key actors include the U.S. Department of Homeland Security, relevant congressional oversight committees, and private cybersecurity firms advising on critical infrastructure defense. This comes amid heightened concern over cyber threats originating from China, India, Russia, and other nation-states.

In recent months, analysts have flagged the "cyber cuts," where budget allocations meant to bolster election systems, power grids, water supplies, and emergency services are being diminished. These funds had previously supported threat monitoring, incident response drills, and real-time intelligence-sharing partnerships between federal and state authorities. Experts warn that scaling back these programs hinders readiness against advanced Chinese cyber operators believed to be probing U.S. networks daily, as well as reducing preparedness for ransomware and supply chain attacks tied to nation-state proxies.

Technically, the reductions affect funding for log aggregation systems, continuous monitoring platforms, and public–private fusion centers. The changes may slow down the deployment of intrusion detection systems and delay upgrades to critical network segmentation, increasing detection latency for breaches. Observers also note that these cuts could reduce investment in zero-trust architectures and limit ongoing tabletop exercises—simulated cyber-attack scenarios essential to maintaining response capabilities. Such operational readiness measures have been emphasized since major incidents like SolarWinds and the Colonial Pipeline attack.

The broader context is a geopolitical tug-of-war in cyberspace. The U.S. government is balancing fiscal constraints with a mandate to deter state-backed digital aggression. Any degradation of domestic cyber defenses could embolden adversaries, especially China, which has increasingly leveraged cyber operations to probe weaknesses, collect intellectual property, and conduct surveillance. In turn, this could undermine U.S. credibility in cybersecurity assistance offered to allies and partners worldwide.

Strategically, the issue spotlights the tension between budgetary restraint and national security. The cybersecurity ecosystem thrives on real-time detection, continuous training, and layered defenses—elements put at risk by funding cuts. If current proposals proceed, they may slow the momentum towards more resilient, adaptive systems, weaken deterrence, and increase the probability of high-impact intrusions with cross-border

consequences.

Read more: https://www.politico.com/newsletters/digital-future-daily/2025/06/05/cyber-cuts-are-freaking-out-china-watchers-00390703?

US still reigns over China in tech race, but gaps are quickly closing: Harvard report

The ongoing technological competition between the United States and China remains a central dynamic in global power relations, with both nations investing heavily in frontier technologies to secure long-term strategic dominance. The key actors involved are the U.S. and Chinese governments, alongside research institutions and technology firms backed by each state. A recent analysis by Harvard's Belfer Center highlights that while the U.S. maintains an overall lead in critical technologies such as advanced semiconductors, AI foundation models, and aerospace systems, China is rapidly closing the gap—particularly in quantum communication, electric vehicles, 5G infrastructure, and clean energy technologies.

The report outlines China's strategic state-backed approach, which combines industrial policy, targeted investments, and human capital development to accelerate domestic capabilities and reduce reliance on Western technologies. In areas such as battery technology, rare earth processing, and solar panel manufacturing, China has already achieved global leadership. Conversely, the U.S. retains its edge in chip design, software ecosystems, and high-performance computing—areas safeguarded by export controls, intellectual property regimes, and complex global supply chains.

Specific developments include China's efforts to build a vertically integrated chip supply chain, heavy funding for AI research through national labs and commercial giants like Huawei and Baidu, and parallel ambitions in space exploration and satellite-based communications. The U.S., meanwhile, is doubling down on reshoring semiconductor production, investing in public-private partnerships like CHIPS Act-funded fabs, and strengthening alliances with democratic tech partners through initiatives like the Quad and AUKUS.

Strategically, this evolving rivalry is reshaping global innovation flows, regulatory frameworks, and security doctrines. As technological superiority becomes synonymous with geopolitical leverage, the narrowing gap between the U.S. and China raises critical questions about the future balance of power, the risk of tech bifurcation, and the resilience of global supply chains in an era of increasing strategic decoupling.

Read more: https://www.scmp.com/news/china/science/article/3313212/us-still-reigns-over-china-tech-race-gaps-are-quickly-closing-harvard-report?

Anthropic launches new Claude service for military and intelligence use

The U.S. government's adoption of a specialized version of Anthropic's Claude AI model—named Claude-Gov—marks a significant development in the integration of artificial intelligence into federal operations, including defense and national security. The key actors in this initiative include Anthropic, a leading AI safety-focused company, and various U.S. government agencies, notably those operating in civilian and military sectors. This move aligns with broader efforts to modernize governmental infrastructure and decision-making processes through AI-driven tools, while also enhancing strategic autonomy amid intensifying global AI competition, especially with China.

Claude-Gov is a tailored version of Anthropic's Claude 3 large language model (LLM), designed to meet U.S. government requirements for privacy, reliability, and compliance with federal standards. It will be hosted on dedicated government infrastructure rather than public cloud platforms, a move intended to reduce security vulnerabilities and limit exposure to commercial data leaks or external manipulation. This configuration allows agencies to use advanced AI capabilities—including document summarization, secure query handling, and scenario modeling—within a controlled and auditable environment.

Anthropic's Claude models are known for their constitutional AI framework, which prioritizes safety, non-ma-

nipulative behavior, and interpretable reasoning. This makes them particularly suitable for use in sensitive government contexts where predictability, transparency, and value alignment are paramount. The Claude-Gov deployment is part of a broader push by the U.S. to ensure that its public sector, particularly the Department of Defense and intelligence agencies, remains technologically competitive while minimizing reliance on commercially exposed AI systems.

Strategically, this development signals a maturing phase in AI-government collaboration, where trustworthiness and national control take precedence over general-purpose AI adoption. As global adversaries pursue militarized or state-controlled AI strategies, the deployment of Claude-Gov reflects the U.S. response: securing advanced AI capacity under sovereign control to mitigate risks of exploitation, maintain operational superiority, and shape the future rules of engagement in AI-driven global affairs.

Read more: https://www.theverge.com/ai-artificial-intelligence/680465/anthropic-claude-gov-us-government-military-ai-model-launch?

Peoples Republic of China – PRC

Leaked files reveal how China is using AI to erase the history of the Tiananmen Square massacre

The Chinese government has intensified efforts to erase public memory of the 1989 Tiananmen Square massacre through the deployment of advanced artificial intelligence and enhanced censorship tools. The key actors include state-controlled propaganda departments, cybersecurity regulators, and Chinese tech firms that collaborate with authorities to enforce digital information control. This campaign operates within the broader context of the Chinese Communist Party's (CCP) long-standing policy of narrative control, aimed at maintaining political legitimacy and suppressing dissent. The suppression has evolved from manual censorship to automated, AI-driven content filtering systems capable of identifying and removing politically sensitive material—including text, images, videos, and even encrypted references—across social media platforms, messaging services, and search engines.

Recent developments include the use of large language models and computer vision tools to detect oblique or coded references to the massacre, including memes, altered images, and historical allusions that once evaded automated moderation. Chinese platforms like WeChat, Weibo, and Douyin have reportedly adopted more sophisticated models trained to flag not only explicit keywords, but also contextual and behavioural patterns associated with dissent. These tools operate in real time, allowing censors to pre-empt viral content and shut down discussions almost instantaneously.

This heightened digital repression was particularly visible during the anniversary of the crackdown on June 4, with virtual private networks (VPNs), cloud storage, and AI-generated memorial art also being actively targeted or disrupted. Additionally, public commemorations in Hong Kong—once a haven for remembrance—have been silenced under Beijing's expanded national security laws.

The strategic implications are twofold. Domestically, the CCP's deployment of AI-enhanced censorship represents a scalable model for authoritarian control over historical narrative and dissent, reinforcing state power. Internationally, it raises alarms about the export of surveillance and censorship technology to other regimes, setting a precedent for digital authoritarianism that challenges norms of free expression, historical accountability, and human rights in the global information space.

Read more: https://www.abc.net.au/news/2025-06-04/beijing-ai-and-censors-erase-tiananmen-square-massacre/105370772

China is gaining ground in the global race to develop AI agents

China's artificial intelligence sector is undergoing rapid localization as domestic technology companies accel-

erate the development of homegrown AI agents in response to regulatory restrictions and geopolitical pressures. The primary actors in this shift include major Chinese firms such as Baidu, Alibaba, and Tencent, as well as emerging startups and state-backed research institutions. This development is driven by China's strategic imperative to reduce dependency on Western AI systems—particularly those from U.S.-based companies like OpenAI—amid tightening export controls, rising tech rivalry, and digital sovereignty concerns.

Recent developments involve the large-scale deployment of Chinese-language AI agents across consumer and enterprise applications, including education, customer service, content moderation, and smart home technologies. These AI systems are built on large-scale transformer architectures trained on domestic datasets and designed to operate in alignment with state censorship protocols. Their deployment is tightly integrated with China's existing digital governance model, ensuring ideological conformity and compliance with national content standards. Technical limitations such as access to high-performance computing infrastructure and diverse training data remain challenges; however, government subsidies and a massive domestic user base are helping to overcome these barriers.

One notable feature of this movement is the clear distinction between Chinese AI agents and their Western counterparts: the former are optimized not only for linguistic relevance but also for political reliability. This ensures that interactions conform to state narratives and avoid politically sensitive content. The agents are also embedded in a range of state and private platforms, effectively forming a parallel AI ecosystem that excludes foreign competitors.

Strategically, China's drive for AI self-sufficiency represents a critical milestone in the global bifurcation of digital technologies. It highlights the emergence of ideologically segmented AI ecosystems, where technology is both shaped by and reinforces the governing political order. This trajectory raises concerns about digital authoritarianism, fragmented internet governance, and the potential use of AI as a tool of state control and geopolitical influence.

Read more: https://restofworld.org/2025/china-ai-agent-openai/

Follow the Smoke | China-nexus Threat Actors Hammer at the Doors of Top Tier Targets

The cybersecurity landscape is facing heightened threats from a coordinated group of China-nexus threat actors actively targeting high-value global institutions across sectors such as government, defence, telecommunications, and technology. These state-aligned groups are part of a broader cyberespionage ecosystem supported by China's intelligence apparatus, with campaigns designed to extract sensitive data, conduct long-term infiltration, and undermine the strategic advantages of rival states. The activity occurs within the context of intensifying geopolitical rivalry, particularly between China and the United States, and is aligned with Beijing's objectives to bolster technological self-reliance, monitor dissidents, and acquire foreign intellectual property.

Recent investigations have uncovered a pattern of persistent intrusions involving sophisticated tactics, techniques, and procedures (TTPs), including living-off-the-land (LotL) methods, fileless malware, custom loaders, and advanced command-and-control (C2) infrastructures. The threat actors leverage legitimate system tools to blend in with normal network activity, enabling long-term espionage while evading detection. Credential harvesting, exploitation of zero-day vulnerabilities, and lateral movement across interconnected networks are common methods used to establish and maintain access.

Targets have included government agencies, military contractors, aerospace firms, and strategic infrastructure providers. In several cases, attackers utilized custom backdoors and shellcode loaders that mimic legitimate software components, allowing them to bypass endpoint protection and retain persistence. These campaigns often involve coordinated phishing operations and watering-hole attacks to gain initial access, followed by privilege escalation and data exfiltration over encrypted channels.

The strategic implications of these operations are significant. They illustrate China's continued investment

in offensive cyber capabilities as a pillar of its national strategy and reflect a growing normalization of state-sponsored cyberespionage as a tool of great-power competition. These campaigns threaten not only the confidentiality and integrity of critical information systems but also the resilience of democratic institutions and commercial innovation pipelines. They underscore the urgency for robust cyber defence collaboration among allied nations, enhanced threat intelligence sharing, and sustained investment in cybersecurity resilience across sectors.

Read more: https://www.sentinelone.com/labs/follow-the-smoke-china-nexus-threat-actors-hammer-at-the-doors-of-top-tier-targets/

Russia – Ukraine

Pro-Ukraine hacker group Black Owl poses 'major threat' to Russia, Kaspersky says

A new cyber actor known as Black Owl, a pro-Ukraine hacktivist collective, has emerged as a significant threat to Russian digital infrastructure amid the ongoing Russia-Ukraine conflict. Comprised of highly skilled individuals, Black Owl represents a shift from conventional cyber activism to more coordinated and operationally sophisticated campaigns. The group reportedly operates with a blend of cyber sabotage, espionage, and psychological operations aimed at degrading Russia's internal stability and military command capabilities. Black Owl's operations have targeted a range of Russian digital assets, including government databases, military logistics platforms, and public-facing websites. Utilizing a combination of custom malware, data wipers, credential-harvesting tools, and social engineering techniques, the group has successfully infiltrated several sensitive networks. Their campaigns are distinguished by carefully timed attacks designed to disrupt Russian civil and military coordination, as well as to embarrass state authorities by leaking confidential data. Among their notable actions are breaches into regional administration servers, destruction of local backup systems, and the defacement of propaganda channels with pro-Ukrainian messaging.

The group's public communications, often disseminated via Telegram and dark web forums, display a strategic understanding of information warfare and its impact on national morale. Unlike other loosely affiliated hacktivist entities, Black Owl exhibits a disciplined operational structure, suggesting possible support or collaboration with state-aligned or intelligence-connected actors on the Ukrainian side, though no direct attribution has been confirmed.

Strategically, Black Owl's rise reflects the broader weaponization of cyberspace in the Russia-Ukraine war, where non-state cyber actors increasingly play pivotal roles in shaping the battlespace. Their success in penetrating Russian systems highlights persistent vulnerabilities in Moscow's cyber defences and raises concerns over retaliatory escalations. More broadly, it underscores how modern conflict now includes asymmetrical digital campaigns that blur the lines between civilian and military targets, complicating traditional security frameworks and norms in cyberspace.

Read more: https://therecord.media/pro-ukraine-hacker-group-black-owl-major-threat-russia?

'Spider's Web' warning: The US must prioritize drone defense to avoid Russia's fate

The United States faces increasing pressure to accelerate the development and deployment of counter-drone capabilities amid the rapidly evolving threat landscape shaped by advancements in unmanned aerial systems (UAS). The central concern, raised by military analysts and defence strategists, centres on the U.S. military's current vulnerabilities to mass drone assaults, particularly in light of lessons drawn from the ongoing Russia-Ukraine conflict. Key actors in this context include the U.S. Department of Defence, defence contractors, and policymakers within NATO-aligned defence circles.

The strategic backdrop is defined by the growing accessibility and lethality of drone swarms, which can be

deployed in coordinated, low-cost, and high-volume attacks to overwhelm traditional air defences. Ukraine's use of both commercial and military drones to degrade Russian Armor, logistics, and air defences has demonstrated the disruptive power of decentralized drone warfare. Russia's failure to adequately defend against these swarms has been attributed to gaps in electronic warfare, radar coverage, and kinetic countermeasures—shortcomings the U.S. is now racing to avoid.

Specific concerns highlighted include the lack of a unified, scalable counter-UAS architecture across U.S. military branches. Although numerous systems exist—ranging from jammers and directed energy weapons to net-based interceptors—they remain siloed and limited in interoperability. The growing threat includes not only tactical drones on battlefields but also strategic risks to homeland infrastructure, forward-deployed bases, and maritime assets. The complexity of defending against AI-powered drones, capable of autonomous targeting and swarming behaviour, adds urgency to the problem.

Strategically, the proliferation of low-cost drone warfare technologies signals a shift in the global balance of military power, lowering the entry barrier for asymmetric actors and state adversaries alike. If the U.S. fails to adapt its doctrine, procurement, and R&D priorities accordingly, it risks strategic surprise in future conflicts. The situation underscores the imperative for integrated drone defence as a pillar of modern deterrence and force protection in an increasingly unmanned battlespace.

Read more: https://breakingdefense.com/2025/06/spiders-web-warning-the-us-must-prioritize-drone-defense-to-avoid-russias-fate/?

Europe

Chinese spying on Dutch industries 'intensifying': Dutch defence minister

Chinese state-backed espionage targeting Dutch high-tech industries has intensified, according to Dutch defence and intelligence authorities. The primary actors involved are Chinese intelligence agencies, which have increasingly focused on acquiring sensitive Dutch technologies through covert means. The Netherlands, home to globally significant firms such as ASML—crucial to semiconductor manufacturing—has emerged as a key target due to its strategic role in global supply chains and its expertise in advanced technologies, particularly those with dual-use military and civilian applications.

The Dutch Defence Ministry has raised concerns over growing cyber and human intelligence operations originating from China, specifically aimed at penetrating sectors such as aerospace, quantum computing, and semiconductor manufacturing. These espionage activities often involve cyber intrusions, social engineering, and the recruitment of insiders to exfiltrate proprietary knowledge. In recent years, the Dutch General Intelligence and Security Service (AIVD) has detected multiple attempts to bypass export controls and exploit scientific collaboration agreements, signalling a systematic effort to siphon critical technology for Beijing's geopolitical ambitions.

This trend unfolds amid broader geopolitical tensions between China and Western democracies, particularly as governments increasingly view technological supremacy as a national security priority. In response, the Netherlands has moved to strengthen export restrictions, enhance cybersecurity frameworks, and deepen cooperation with NATO and EU partners to mitigate the threat. The ongoing espionage underscores the vulnerabilities inherent in open innovation ecosystems and the risks posed by asymmetric intelligence tactics targeting small yet technologically advanced nations.

The strategic implications are profound. Unchecked espionage could erode the technological edge of key Western industries, disrupt supply chain resilience, and compromise national defence capabilities. The situation reflects a larger global pattern wherein authoritarian regimes leverage intelligence operations to close

strategic gaps, raising the urgency for coordinated counterintelligence measures and policy responses across allied nations.

Read more: https://www.reuters.com/business/aerospace-defense/chinese-spying-dutch-industries-intensifying-dutch-defence-minister-2025-05-31/

EU, Southeast Asia aim to boost security for undersea cables

State-sponsored sabotage of undersea infrastructure has become a growing threat in both Europe and Asia, with increasing incidents linked to Chinese and Russian-affiliated vessels operating under opaque ownership—often referred to as "shadow fleets." These incidents, concentrated in the Baltic Sea and around Taiwan, suggest a coordinated pattern of grey-zone activity targeting critical subsea cables and pipelines vital for communication, energy, and military coordination.

In the Baltic region, a series of cable and power line disruptions between November 2024 and January 2025 affected key assets such as the BCS East–West Interlink, C-Lion1 data cable, and the Estlink-2 power cable. These incidents impacted Finland, Estonia, Germany, and Sweden. Investigations pointed to suspicious vessel activity, particularly the Chinese-flagged Yi Peng 3 and the Eagle S, a Cook Islands–registered ship tied to Russian operators. Satellite and maritime data placed these vessels near damaged cables, and Finnish special forces boarded the Eagle S after it was spotted loitering above Estlink-2. Although sabotage remains unproven due to legal and evidentiary hurdles, the deliberate dragging of anchors over cable routes raised strong suspicions.

A parallel pattern is unfolding in the Indo-Pacific. Taiwanese authorities intercepted the Hongtai, a Chinese-crewed ship under a Togolese flag, after a cable to the Penghu islands was severed. The ship's proximity and evasive maneuvers heightened concerns about deliberate interference—especially near militarized zones. In response, NATO launched "Operation Baltic Sentry," deploying drones, divers, minehunters, and AI-aided surveillance to patrol critical underwater corridors. Similarly, the EU and regional navies, including Estonia's, are expanding patrols and enhancing satellite monitoring. In Asia, the U.S., Japan, Australia, and India are collaborating on cable resilience, aiming to increase redundancy and rapid-repair capabilities.

Technically, the attacks exploit physical methods like anchor-dragging, often conducted under civilian cover, making attribution and response challenging. The broader implication is clear: undersea cables are becoming strategic targets in hybrid warfare, with significant consequences for national security, global connectivity, and geopolitical stability.
Ask ChatGPT

Read More: https://www.dw.com/en/eu-southeast-asia-sabotage-undersea-cables-china-nato-baltic-russia/a-72841922

Middle East

BladedFeline: Whispering in the dark

A coordinated cyber-espionage campaign involving Iranian state-linked threat actors has intensified across the Middle East, with particular focus on the Kurdish region of Iraq. The operation, attributed to a subgroup of Iran's OilRig (APT34) cluster—codenamed BladedFeline—demonstrates a sophisticated and persistent effort to infiltrate government and diplomatic networks for intelligence collection. Key targets have included the Kurdistan Regional Government (KRG), entities within the central Iraqi administration, and even a telecommunications provider in Uzbekistan, signalling a broader regional agenda. This activity reflects Iran's strategic objective of monitoring Kurdish political movements, assessing regional diplomatic alignments, and gathering intelligence on energy and security affairs vital to Tehran's interests.

Technically, the attackers have employed a multi-phase intrusion approach, leveraging spear-phishing emails to compromise Microsoft Exchange webmail services, and deploying custom malware such as Whisper, Shahmaran, and PrimeCache. These tools enable long-term persistence, remote command execution, and encrypted data exfiltration. For example, Whisper uses email attachments as covert command-and-control (C2) channels, while PrimeCache, linked to the broader OilRig toolkit, supports credential harvesting and lateral movement across compromised networks. In several instances, attackers have also deployed the Flog webshell to maintain access to external-facing infrastructure. Malware components are modular, stealthy, and tailored to evade detection within government systems.

This campaign underscores the growing sophistication of Iranian cyber operations, combining traditional espionage tradecraft with advanced technical capabilities. The focus on Kurdish and Iraqi infrastructure suggests an intent to shape or pre-empt political developments in territories of strategic concern to Iran, while the expansion into Central Asia reflects a broader ambition to project digital influence beyond immediate borders. Regionally, the implications are profound: as cyber-enabled intelligence becomes a central instrument of statecraft, governments in the Middle East face escalating threats that demand enhanced cyber defence, intergovernmental cooperation, and more resilient digital governance frameworks.

Read more: https://www.welivesecurity.com/en/eset-research/bladedfeline-whispering-dark/

Malware & Vulnerabilities

International operation takes down crypting sites used for testing malware

An international law enforcement coalition has dismantled the infrastructure behind "Cryptor," a cybercriminal service used to conceal malicious software from antivirus detection. Key actors in the operation included Europol, Eurojust, and law enforcement agencies from 19 countries, including the United States, United Kingdom, Germany, and Ukraine. This coordinated effort targeted a criminal ecosystem that provided crypting tools—software obfuscators designed to help malware developers evade security defences—for use in deploying remote access trojans (RATs), ransomware, and other malicious payloads.

The takedown involved the seizure of multiple domains and servers associated with the Cryptor service, along with the arrest of several individuals suspected of developing and distributing the tools. Technical analysis revealed that Cryptor-enabled malware had been used in a wide range of cyber operations, from credential theft and espionage to financial fraud. The service functioned on a subscription model, offering tiered pricing and customer support to cybercriminals, thereby professionalizing and scaling malware distribution in underground markets.

Investigators traced digital infrastructure through forensic analysis of traffic patterns, server logs, and cryptocurrency transactions, ultimately enabling coordinated raids and digital asset seizures. One notable aspect of the operation was its emphasis on dismantling the service's backend and customer database, potentially exposing thousands of users worldwide and opening avenues for further prosecutions.

This enforcement action reflects a broader international trend toward targeting the cybercrime-as-a-service economy, where threat actors increasingly rely on third-party providers for specialized tools. Strategically, the operation underscores a growing consensus among allied nations that transnational cybercrime requires multilateral, intelligence-driven responses. It also demonstrates the increasing technical sophistication and global reach of law enforcement bodies in countering digital threats, raising the stakes for cybercriminals operating behind obfuscation services. By disrupting the supply chain of obfuscation technology, authorities aim to degrade the capabilities of malware operators and restore a measure of deterrence in cyberspace.

Read more: https://therecord.media/international-operation-takes-down-cryptor

Microsoft and CrowdStrike Launch Shared Threat Actor Glossary to Cut Attribution Confusion

Microsoft and CrowdStrike have launched a joint cybersecurity initiative to enhance real-time threat intelligence sharing in response to the growing sophistication and frequency of cyberattacks targeting critical infrastructure and enterprises. The collaboration involves the creation of a shared threat data exchange framework aimed at improving the speed and accuracy of detecting advanced persistent threats (APTs), ransomware operations, and state-backed cyber intrusions. Both companies—leaders in endpoint security and cloud-based threat detection—will integrate their security telemetry and analytic capabilities, enabling cross-platform correlation of indicators of compromise (IOCs), behavioural patterns, and attack techniques.

This development is set against the backdrop of intensifying cyber warfare, with state-affiliated threat actors exploiting software vulnerabilities, supply chain weaknesses, and identity systems to conduct espionage, sabotage, and financially motivated attacks. By combining Microsoft's vast telemetry across its Windows ecosystem, Azure cloud, and identity management infrastructure with CrowdStrike's Falcon platform—known for its behavioural analytics and threat hunting tools—the partnership aims to deliver faster threat containment and improved forensics across diverse IT environments.

A key technical element of the initiative is the use of standardized APIs and secure data-sharing protocols that allow for near-instant dissemination of threat intelligence across both firms' platforms without compromising user privacy or system integrity. This real-time integration also supports machine learning-driven detections and automated response mechanisms to neutralize active threats more effectively. It represents a move away from siloed security tools toward a federated defence model better suited to counter coordinated, multi-vector attacks.

The strategic implications are significant. In an era where cyberattacks can cripple national infrastructure and disrupt global commerce, the Microsoft-CrowdStrike alliance exemplifies the private sector's increasing role in collective cyber defence. It reflects a broader industry trend of collaborative security ecosystems designed to outpace agile and well-resourced adversaries, particularly those backed by nation-states with geopolitical motivations.

Read more: https://thehackernews.com/2025/06/microsoft-and-crowdstrike-launch-shared.html?

About the Author

Govind Nelika is the Researcher / Web Manager / Outreach Coordinator 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.