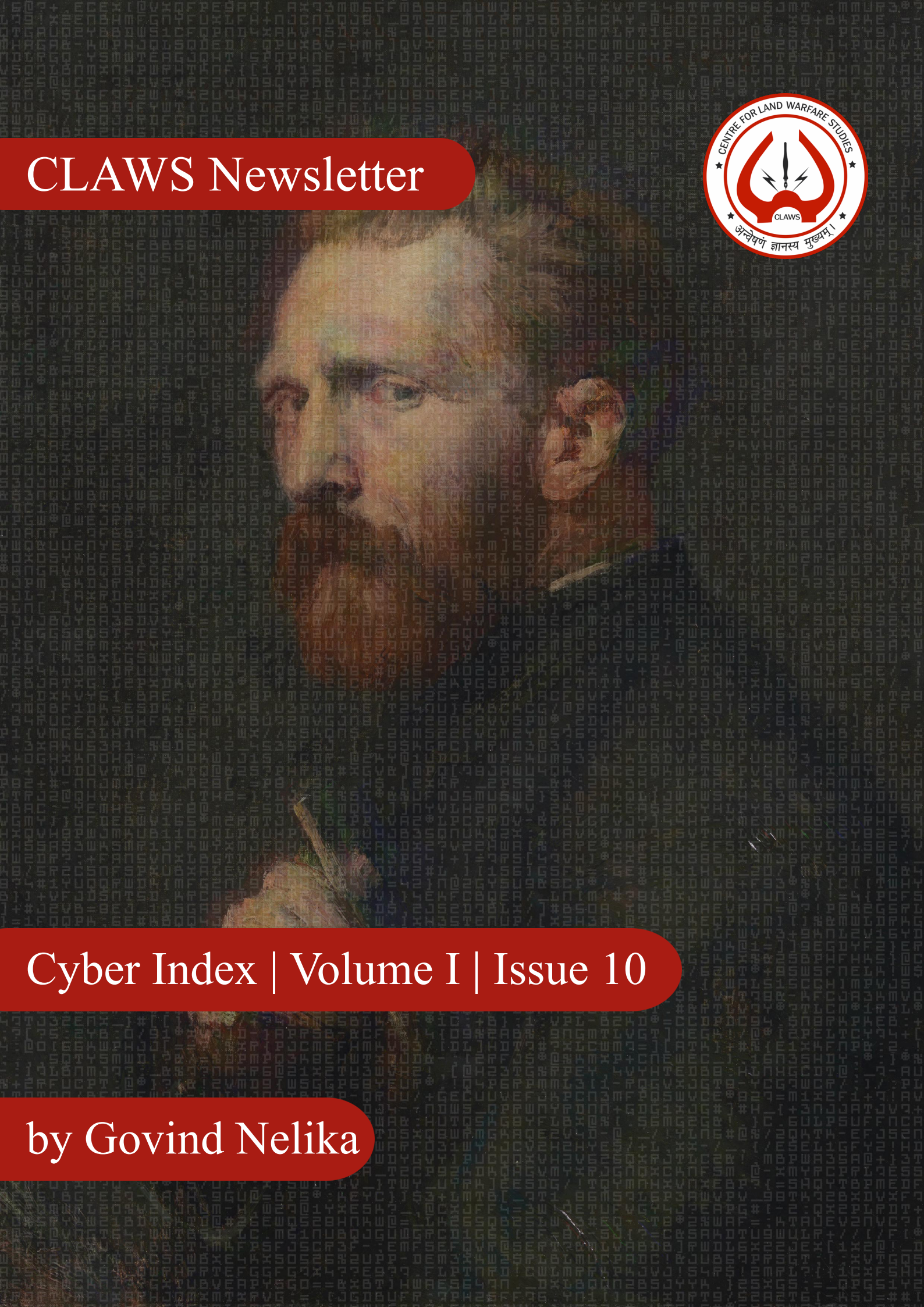
CLAWS Newsletter



Cyber Index | Volume I | Issue 10

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

NATO's Communications and Information Agency (NCI Agency) signs contract with Planet Labs

U.S.-based Earth observation company Planet Labs has secured a new contract with NATO's Communications and Information Agency (NCI Agency) to provide commercial satellite imagery and geospatial intelligence to support the alliance's intelligence and operational planning efforts. This development reflects a broader strategic shift within NATO toward leveraging commercial satellite capabilities to enhance situational awareness, particularly amid heightened geopolitical tensions with Russia and increased activity in contested regions such as Eastern Europe and the Arctic. The contract builds on a 2022 agreement and significantly expands Planet's role in supplying imagery derived from its fleet of high-revisit, medium- and high-resolution Earth observation satellites.

Under the new agreement, Planet will deliver persistent monitoring and rapid imagery updates to NATO and allied analysts, enabling near real-time assessments of military activities, infrastructure developments, and environmental changes in strategic theatres. The data will be integrated into NATO's intelligence systems to support operations ranging from force posture evaluation to humanitarian response and critical infrastructure monitoring. The satellites use a combination of optical and near-infrared sensors to capture imagery with frequent revisit rates critical for tracking fast-changing developments on the ground.

This partnership underscores the growing reliance on commercial providers for tactical and strategic intelligence, a trend accelerated by the war in Ukraine, which demonstrated the operational value of high-frequency satellite imagery in open-source intelligence (OSINT) and battlefield awareness. It also illustrates NATO's effort to enhance intelligence-sharing interoperability among member states while reducing dependence on traditional state-run assets. The expanded contract strengthens transatlantic defence ties through public-private collaboration and highlights the increasing role of dual-use technologies in modern defence postures. Strategically, it reflects NATO's recognition of the evolving nature of surveillance and reconnaissance in a multipolar world where space-based assets are central to information dominance and rapid decision-making in crisis scenarios.

Read more : https://www.satellitetoday.com/government-military/2025/06/16/planet-wins-new-nato-intelligence-deal/

https://investors.planet.com/news/news-details/2025/NATO-Selects-Planet-for-Landmark-Seven-Figure-Contract-for-Advanced-Daily-Monitoring-and-Early-Warning-Capabilities/default.aspx

Nuclear risks grow as new arms race looms new SIPRI Yearbook

The Stockholm International Peace Research Institute (SIPRI) has issued a stark assessment of the growing risks of nuclear conflict and the resurgence of global arms competition, citing renewed investment in nuclear arsenals and a breakdown of arms control regimes. The key actors driving this shift include the United States, Russia, China, and several other nuclear-armed states such as India, Pakistan, North Korea, and Israel. Against a backdrop of escalating geopolitical tensions including the ongoing war in Ukraine, deteriorating U.S.-China relations, and mounting instability in the Middle East these nations are expanding or modernizing their nuclear capabilities while dialogue on disarmament continues to stall.

SIPRI's findings highlight a marked increase in the number of operational nuclear warheads and the development of new delivery systems, such as hypersonic glide vehicles, intercontinental ballistic missiles (ICBMs), and submarine-launched ballistic missiles (SLBMs). Russia and the United States together still hold approximately 90% of the world's nuclear weapons, but China is rapidly expanding its stockpile and diversifying its strategic forces, including the construction of new missile silos and improvements to its command and control systems. India and Pakistan are similarly advancing their dual-capable delivery systems, while North Korea continues to refine its weapons and launch technologies, signalling ambitions for full-spectrum deterrence.

A key concern identified is the weakening of multilateral frameworks that once mitigated nuclear risks. The collapse of the Intermediate-Range Nuclear Forces (INF) Treaty, the uncertain future of New START, and the lack of progress on the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) review process have eroded norms and guardrails. As arms control mechanisms falter and trust between major powers diminishes, the potential for miscalculation or unintended escalation increases.

Strategically, this trend signals a shift toward a more volatile international security environment where nuclear weapons are more central to national defence postures. It reflects a dangerous move away from transparency, restraint, and dialogue, raising the spectre of a new global arms race with profound implications for global stability and crisis management.

Read more: https://www.sipri.org/media/press-release/2025/nuclear-risks-grow-new-arms-race-looms-new-sipri-yearbook-out-now

Kier Giles Russia Researcher at Chathamhourse targeted in Cyber Espionage campaign in Coordinated Email Breach

A recent cyber intrusion targeting Keir Giles, a prominent Russia and Eurasia security expert affiliated with Chatham House, underscores the persistent and personalized nature of espionage-focused cyber operations linked to state-aligned actors. The incident involved unauthorized access to multiple email accounts, suggesting a deliberate and methodical attempt to gather intelligence on Giles' communications and professional activities. Given Giles' specialization in Russian military and information warfare strategies, the breach carries significant implications and aligns with established patterns of cyber targeting against individuals involved in national security discourse, policy advising, or public commentary on authoritarian regimes.

The attack methodology appears consistent with advanced persistent threat (APT) tactics frequently employed by Russian state-backed groups such as APT29 (Cozy Bear) or APT28 (Fancy Bear), known for credential harvesting, phishing, and long-term infiltration of personal and institutional communications. While technical details of the intrusion remain limited, the compromise of multiple accounts indicates a coordinated effort likely involving credential stuffing or spear-phishing techniques. These methods exploit password reuse, weak authentication, or social engineering to gain unauthorized access, often circumventing multi-factor authentication in cases where such protections are inconsistently applied.

This event reflects the broader strategic objectives of hostile cyber actors who target experts, journalists, and analysts to collect sensitive information, map professional networks, and potentially manipulate or disrupt policy-relevant discourse. Such intrusions not only compromise the privacy and safety of individuals but also risk undermining public trust in institutions and intellectual independence in matters of national and international security. From a geopolitical perspective, the targeting of non-governmental experts highlights the widening scope of cyber espionage beyond traditional state and military systems. It underscores the need for robust cyber hygiene and institutional support for individuals operating at the intersection of security analysis and foreign policy. The incident fits into a broader trend of information warfare wherein cyber operations are used to intimidate, surveil, or neutralize perceived adversaries of authoritarian regimes.

Read more: https://www.linkedin.com/posts/keir-giles-499a489_hack-alert-several-of-my-email-accounts-activity-7339380839400546305-A6EK?

https://citizenlab.ca/2025/06/russian-government-linked-social-engineering-targets-app-specific-passwords/?

Felicity Oswald, COO UK NSCSC to leave the Agency

Felicity Oswald, currently Chief Operating Officer (COO) at the United Kingdom's National Cyber Security Centre (NCSC), will depart the agency in September to assume the role of Chief Executive at Girlguiding UK, Britain's preeminent youth organisation for girls with over 300,000 members. Since joining GCHQ and then the NCSC, she has held pivotal leadership roles, including serving as interim CEO in 2024, helping to set

strategy, manage organisational risk, and drive cyber policy response domestically and internationally.

Oswald's tenure at NCSC coincided with major national cybersecurity reforms and heightened threat awareness. She played a key leadership role in briefing incoming government ministers on cyber vulnerabilities and pushing forward legislative initiatives including the Cyber Security and Resilience Bill and shaping Britain's updated national security strategy with a stronger cybersecurity focus. Her legacy includes contributions to GCHQ/NCSC outreach initiatives such as the CyberFirst Girls Competition, aimed at expanding diversity in the cyber workforce by inspiring girls and young women to pursue STEM careers.

At Girlguiding, Oswald brings over two decades of public service experience and a demonstrated commitment to promoting gender equality in technology and leadership. In her new position, she will oversee the charity's ambitious "Girls Can Do Anything" strategy, aimed at doubling its membership and further embedding inclusion initiatives for underrepresented groups by 2035. Her cybersecurity leadership and focus on digital transformation are expected to strengthen Girlguiding's infrastructure and advance its mission to foster confidence and agency among girls nationwide.Strategically, this transition highlights a shift of a seasoned cyber leader from national security architecture to youth empowerment and STEM advocacy. Oswald's move represents a unique fusion of public sector cyber expertise and social impact leadership, reinforcing the importance of role models in technology while broadening influence beyond traditional security domains.

Read more: https://therecord.media/felicity-oswald-ncsc-coo-uk

United States of America (USA)

Commercial remote sensing: The critical U.S. National Security Space imperative

The evolving role of commercial remote sensing firms in national security has become a strategic imperative for the United States, with the Department of Defence (DoD), intelligence agencies, and allied partners increasingly integrating commercial Earth observation capabilities into defence planning and real-time operations. Key actors in this shift include U.S. government agencies such as the National Reconnaissance Office (NRO), National Geospatial-Intelligence Agency (NGA), and Space Systems Command, alongside a rapidly expanding private sector of satellite imaging providers. This development is driven by a confluence of factors, including intensifying geopolitical competition with China and Russia, the proliferation of anti-satellite capabilities, and the need for resilient, distributed intelligence-gathering architectures in contested environments.

Recent initiatives underscore the urgency of incorporating commercial space-based sensing into national defence strategies. The NRO has been tasked with integrating commercial electro-optical, radar, and hyperspectral imagery into U.S. reconnaissance systems, expanding beyond traditional classified satellites. Meanwhile, the U.S. Space Force's Commercial Space Office is working to ensure that commercial assets are interoperable and survivable in conflict scenarios, including through protective measures and diversification of data sources. These efforts aim to ensure uninterrupted access to global situational awareness, even under conditions of electronic warfare, kinetic attacks, or space-based interference.

Commercial providers contribute by offering high-revisit imagery, persistent monitoring, and rapid data delivery capabilities that enhance early warning, target tracking, and crisis response. Technologies employed include synthetic aperture radar (SAR) that can penetrate cloud cover and operate at night, as well as multi-sensor constellations that allow for fusion of different imaging types. As adversaries develop counterspace weapons and operate in grey zones, commercial remote sensing offers both redundancy and agility, mitigating vulnerabilities inherent in traditional military assets. Strategically, this shift reflects a broader transformation in defence intelligence, where public-private integration is essential to maintaining information superiority and operational readiness in an increasingly contested and data-driven security landscape.

Read more: https://breakingdefense.com/2025/06/commercial-remote-sensing-the-critical-u-s-national-security-space-imperative/?

US critical networks are prime targets for cyberattacks. They're preparing for Iran to strike.

A recent wave of cyberattacks has intensified concerns over the security of U.S. critical infrastructure, as Iranian and Israeli cyber operations increasingly spill beyond their regional rivalry into broader digital domains. The main actors involved are Iranian state-backed hacking groups and Israel-linked cyber operators, both of which have engaged in sustained, retaliatory cyber campaigns. The attacks have escalated in the context of deteriorating geopolitical relations following recent military and intelligence confrontations in the Middle East, including strikes on Iranian facilities and alleged Israeli assassinations of high-ranking Iranian figures. Amid this heightened conflict, cyber operations have emerged as a key tool for signalling, retaliation, and disruption.

In recent incidents, Iranian-linked hackers targeted U.S. water utilities, energy infrastructure, and municipal systems using basic but effective tactics such as ransomware and web server exploitation, exploiting known vulnerabilities in outdated software and weak authentication protocols. In parallel, groups affiliated with or sympathetic to Israel conducted attacks on Iranian institutions, including financial networks and government databases. These operations sometimes leveraged data destruction malware, credential theft, and defacement, suggesting a mix of disruption and psychological impact as primary objectives.

Technical indicators point to overlapping infrastructure and evolving tradecraft on both sides, with attackers increasingly obfuscating origin and intent to complicate attribution. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) and private sector partners have issued advisories to operators of critical infrastructure, warning of spillover effects from this foreign conflict and the potential for cyberattacks on soft targets in the U.S. to serve as proxies in regional disputes.

Strategically, the escalation demonstrates how regional cyber conflicts can have global ramifications, particularly when nation-state actors exploit transnational digital dependencies. The persistent vulnerability of U.S. infrastructure highlights the urgent need for modernization, public-private coordination, and proactive defence postures as adversaries expand the battlespace into civilian networks in peacetime hybrid conflict.

Read more: https://www.politico.com/news/2025/06/17/us-critical-networks-iran-israel-cyber-attack-00411799?

BlackSky to expand constellation to deliver high-cadence, multi-spectral broad area collection capabilities

BlackSky Technology, a U.S.-based commercial space and geospatial intelligence company, has announced plans to significantly expand its satellite constellation to enhance high-cadence, multi-spectral, broad-area imaging capabilities. The key actors involved in this development include BlackSky, its government and defense clients such as the U.S. Department of Defense and intelligence agencies, and strategic industry partners supporting the manufacture and deployment of the new satellite architecture. This expansion is framed by growing global demand for real-time situational awareness in both military and civilian applications, especially amid heightened geopolitical instability, regional conflicts, and the increasing militarization of space.

The new satellite generation, known as Gen-3, will incorporate advanced multi-spectral sensors capable of capturing imagery across visible and near-infrared bands with improved resolution, greater area coverage, and increased revisit rates. These satellites are engineered to enable persistent monitoring of key regions, providing critical insights on patterns of life, infrastructure activity, force movements, and environmental change. This leap in capability allows for dynamic tipping-and-cueing operations where one satellite or sensor triggers another for follow-up imaging facilitating time-sensitive intelligence collection and decision support across domains.

BlackSky's integration of artificial intelligence and machine learning into its Spectra AI platform enables rapid processing and analysis of imagery, allowing customers to receive actionable intelligence minutes after

image acquisition. This capability is especially valuable for defence and security missions, disaster response, and strategic infrastructure monitoring. With this expansion, BlackSky aims to deliver near-persistent global coverage, positioning itself as a critical asset in the commercial ISR (intelligence, surveillance, and reconnaissance) market.

Strategically, the constellation upgrade reflects broader defence and intelligence trends favouring agile, responsive, and commercially sourced geospatial data to supplement traditional national systems. It underscores the increasing reliance of governments on private sector innovation to maintain information superiority and situational awareness in an era defined by rapid geopolitical shifts and accelerated decision cycles.

Read more: https://www.blacksky.com/blacksky-to-expand-constellation-to-deliver-high-cadence-multi-spectral-broad-area-collection-capabilities/

Peoples Republic of China – PRC

Beijing confirms that it has signed a trade agreement with the US

China and the United States have formalized a new bilateral trade agreement aimed at reducing tensions and fostering greater economic cooperation amid a backdrop of geopolitical competition and global economic instability. The key actors in this development are the Chinese Ministry of Commerce and the Office of the United States Trade Representative, which have confirmed the deal following months of quiet negotiations. The agreement, signed in Beijing, addresses a range of contentious issues, including tariff reductions, improved access for U.S. companies to China's financial and technology markets, and commitments from both sides to enhance intellectual property protections. In return, the U.S. has agreed to ease certain export restrictions and reduce tariffs on selected Chinese goods, signaling a measured thaw in trade relations following years of heightened friction triggered by the trade war under the previous U.S. administration.

The deal also contains provisions to boost transparency in regulatory practices and re-establish bilateral working groups to manage disputes more constructively, thereby reducing the likelihood of sudden unilateral trade actions. Although specific figures remain undisclosed, Chinese state media has framed the agreement as "mutually beneficial" and a step toward stabilizing global supply chains. This development comes as both countries seek to balance economic imperatives with strategic competition—especially in areas like advanced semiconductors, green energy technologies, and AI—while contending with domestic economic pressures such as inflation, unemployment, and slowing growth.

Strategically, the agreement represents a calculated detente that may temporarily ease global economic uncertainty, particularly in Asia-Pacific markets and among multinational corporations exposed to Sino-American trade dynamics. However, it does not signal a fundamental resolution of broader geopolitical tensions, including disputes over Taiwan, cybersecurity, and technological supremacy. The deal fits into a broader trend of selective economic engagement between major powers, where economic pragmatism coexists with strategic rivalry, creating an increasingly complex and fragmented global trade environment.

Read more: https://www.euronews.com/business/2025/06/27/beijing-confirms-that-it-has-signed-a-trade-agreement-with-the-us

DeepSeek's Democratic Deficit

China's development of its advanced generative AI model, DeepSeek-V2, underscores the country's rapid progress in artificial intelligence while also raising concerns over transparency, algorithmic accountability, and democratic oversight. The project is spearheaded by DeepSeek, a prominent Chinese AI firm backed by both private investors and supportive government policies aligned with Beijing's broader ambitions to achieve technological self-sufficiency and global leadership in AI. DeepSeek-V2 is positioned as a domestic alternative to leading Western models like OpenAI's GPT-4, featuring capabilities such as multi-modal processing,

autonomous reasoning, and complex task completion key competencies for applications ranging from military planning to state surveillance and large-scale automation.

Despite the model's technical sophistication and the government's endorsement, the development process has been marked by a lack of public oversight, limited peer review, and minimal engagement with civil society or independent ethics bodies. Unlike Western AI ecosystems, where development is increasingly shaped by public debate, academic scrutiny, and emerging regulatory frameworks, China's AI advancement is characterized by a closed-loop system involving government ministries, state research labs, and tightly aligned tech firms. DeepSeek's algorithms, training data, and alignment methodologies remain opaque, raising risks around biased outputs, misuse for censorship or disinformation, and potential violations of privacy and intellectual freedom.

The broader context includes intensifying geopolitical rivalry between China and the West over control of emerging technologies, particularly in dual-use domains where AI can serve both civilian and military ends. As Chinese AI models grow more capable, their integration into state-led governance and surveillance architectures may set precedents for authoritarian uses of machine intelligence. Strategically, DeepSeek-V2 exemplifies China's efforts to decouple from U.S.-led technological ecosystems, signaling a future where rival AI spheres reflect deeper ideological and governance divides. The lack of democratic safeguards in such deployments poses challenges for international norms on responsible AI development and use.

Read more: https://chinamediaproject.org/2025/06/24/deepseeks-democratic-deficit/?

China Backs Digital Yuan and Promotes Multi-Polar Currency System

China's advancement of its central bank digital currency (CBDC), the digital yuan (e-CNY), represents a significant evolution in global financial infrastructure, with far-reaching economic and geopolitical implications. Spearheaded by the People's Bank of China (PBoC), this state-backed initiative has transitioned from domestic pilot programs to broader integration across key urban centers, cross-border trade corridors, and institutional frameworks. The digital yuan initiative is unfolding amid growing tensions with Western powers over technological sovereignty, financial surveillance, and competition over global reserve currency dominance. Recent developments include the expansion of digital yuan applications in retail and wholesale transactions, integration into cross-border trade with nations aligned through the Belt and Road Initiative (BRI), and partnerships with financial infrastructure providers to facilitate interoperability with foreign digital currencies. Technical capabilities of the digital yuan include programmable features, real-time traceability, and offline payment functionality, which distinguish it from conventional electronic payment platforms. The currency operates on a dual-layer architecture where the PBoC issues and commercial banks distribute, enabling centralized oversight while leveraging existing financial institutions for scale.

State-owned banks and major tech platforms such as Alipay and WeChat Pay have been enlisted to embed the e-CNY into daily economic activity, while foreign firms operating in China are increasingly expected to accommodate the digital yuan in transactions, potentially altering the competitive dynamics of cross-border e-commerce and investment. Moreover, China has actively explored multi-CBDC bridge projects with entities like the Bank for International Settlements and central banks in Southeast Asia and the Middle East to establish alternative global payment rails independent of SWIFT.

Strategically, the digital yuan could reduce China's reliance on the U.S. dollar, enhance surveillance over capital flows, and extend Beijing's influence in international finance. Its growth signals a broader shift toward state-controlled digital monetary systems, posing challenges to Western financial dominance and raising concerns over privacy, currency weaponization, and the fragmentation of global monetary standards.

Read more: https://fintechnews.hk/34395/fintechchina/china-digital-yuan-currency-shift/

Japan | Nippon-koku

The underlying risks to Japan's undersea cables

Japan's growing vulnerability to undersea cable sabotage has emerged as a critical national security concern, prompting renewed strategic focus on the resilience of its digital infrastructure. The main stakeholders include the Japanese government, defence and telecommunications sectors, and potential adversarial states such as China and Russia, whose military and intelligence activities in maritime domains have increased in both frequency and sophistication. Japan relies on over two dozen submarine cables to handle more than 95% of its international data traffic, making them vital not only for civilian communications and economic stability, but also for military coordination, intelligence sharing, and crisis response.

Recent geopolitical developments including China's assertive maritime posture in the East and South China Seas, and Russia's increased naval activity in the Pacific have elevated concerns over the intentional targeting of undersea cable systems. Specific vulnerabilities include cables in the Okinawa Trough and near Hokkaido, regions where foreign research vessels and submarines have been detected operating in proximity to critical infrastructure. The dual-use nature of oceanographic research vessels raises suspicions, as such platforms can be outfitted for surveillance, mapping, and even physical disruption of cable routes. Japan's existing protection mechanisms, including monitoring by the Japan Coast Guard and maritime self-defence forces, are limited by jurisdictional gaps and the vast geographic scale of the seafloor cable network. While physical sabotage remains difficult, the risk of covert tampering or intelligence collection via cable interception remains high. Tokyo is now exploring enhanced surveillance technologies, legal reforms to expand protective mandates, and deeper cooperation with allies such as the United States and Australia to secure shared digital arteries.

Strategically, the security of undersea cables is a foundational issue in modern hybrid conflict, where disruption of communications infrastructure can yield asymmetric advantages without crossing conventional thresholds of war. Japan's efforts reflect a broader international trend toward viewing digital infrastructure as a critical component of national defence and economic sovereignty.

Read more: https://www.japantimes.co.jp/news/2025/06/16/japan/explainer-japan-undersea-cables/?

Japan teams with NATO to counter China, Russia cyber threats

Japan has formally deepened its strategic cybersecurity cooperation with NATO to counter mounting cyber threats emanating from China and Russia. The principal actors involved include Japan's Ministry of Defense and Self-Defense Forces, NATO's leadership and cyber defense institutions such as the Cooperative Cyber Defence Centre of Excellence (CCDCOE), alongside Tokyo's national intelligence agencies and allied Indo-Pacific partners. This partnership is shaped by intensifying geopolitical tensions: Russia's war in Ukraine and closer military cooperation between Beijing and Moscow have elevated risks of cyber espionage, sabotage, and disinformation campaigns across both the Euro-Atlantic and Indo-Pacific theaters. Japan's strategic response includes joining NATO cyber exercises, expanding intelligence sharing, and planning joint frameworks for incident response and operational interoperability.

Recent developments include institutionalizing these ties under the 2023–2026 Individually Tailored Partnership Programme (ITPP), which provides a formal framework for collaboration across cyber defence, space security, and hybrid threats. Japan's participation in NATO cyber exercises like Locked Shields and Cyber Coalition is increasing, with Japanese personnel engaging in training and joint planning at CCDCOE in Tallinn. Moreover, Tokyo is positioning itself within broader multilateral partnerships such as the Indo Pacific Four (IP4) alongside Australia, New Zealand, and South Korea, which together enhance cooperative information-sharing and cyber resilience.

Technically, this collaboration involves expanding threat intelligence collaboration, standardizing cyber defence tools and protocols, and supporting interoperability across allied infrastructure. Japan also leverages

NATO's analytics and research from CCDCOE, particularly in countering hybrid cyber tactics including disinformation, malware threats, and supply chain compromises.

Strategically, this deepened partnership reflects a recognition that cyber threats are transnational and that emerging adversarial cyber capabilities threaten democratic resilience and infrastructure stability. By aligning with NATO and adjacent Indo-Pacific partners, Japan strengthens deterrence and resilience, contributing to a broader norms-based security architecture that bridges regional and Euro-Atlantic defence buffers in an increasingly contested global cyber environment.

Read more: https://asia.nikkei.com/Spotlight/Cybersecurity/Japan-teams-with-NATO-to-counter-China-Russia-cyber-threats?

Middle East

Iranian Educated Manticore Targets Leading Tech Academics

Educated Manticore a state-aligned advanced persistent threat group associated with Iran's IRGC Intelligence Organization and tracked by security firms as APT42, Charming Kitten, or Mint Sandstorm has launched a newly intensified spear phishing campaign targeting high-profile tech academics and cybersecurity specialists, particularly in Israel. This activity comes amid escalating Iran–Israel tensions and reflects Tehran's strategic push to surveil expert communities and gather technical intelligence in the cyber and research domains.

The operation employs highly personalized social engineering: attackers impersonate fictitious assistants or employees of cybersecurity firms via email and WhatsApp, using polished, AI-assisted language to gain trust without including malicious links in initial contact. Once rapport is built, victims receive links to fake Google Meet invitations or credential-harvesting pages. These phishing kits are implemented as React-based single-page applications (SPAs), dynamically rendering authentication flows and pre-filling victims' email addresses to enhance realism.

The kits support a full suite of Google's authentication steps from password entry through SMS, email, TOTP, and push verification allowing attackers to relay 2FA tokens in real time. A persistent WebSocket connection also enables passive keylogging of all keystrokes, even if forms are abandoned. Beyond Google, similar phishing infrastructure targets Outlook and Yahoo credentials with comparable design and functionality. Check Point Research has mapped over 100 unique domains, many linked to an infrastructure cluster known as Green Charlie, rapidly deployed and rotated to avoid detection. The precision targeting of Israeli academics and journalists underscores the group's intelligence interest in technology expertise, possibly tied to retaliation or future cyber capability development.

Strategically, the campaign reflects a broader trend of state-aligned actors targeting non-governmental expert communities to extract credentials, build networks, and gain situational awareness. It highlights the sophistication of modern phishing techniques capable of bypassing MFA, the weaponization of trusted collaboration platforms, and the need for heightened vigilance and layered authentication security in high-risk sectors.

Read more: https://research.checkpoint.com/2025/iranian-educated-manticore-targets-leading-tech-academics/

Pro-Israel hackers claim breach of Iranian bank amid military escalation

A pro-Israel hacktivist group known as "Group 13" has claimed responsibility for a cyberattack that disrupted the services of Bank Melli, one of Iran's largest and most strategically significant financial institutions. The key actors in this development include the Iranian state-owned banking sector, Israel-aligned cyber activists, and potentially affiliated intelligence bodies operating in the broader context of intensifying regional cyber

and proxy warfare between Iran and Israel. This incident underscores the escalating trend of retaliatory cyber operations amidst ongoing tensions over Iran's nuclear program, Israeli security concerns, and the broader shadow conflict between the two nations involving both kinetic and digital domains.

According to available details, the attack leveraged a coordinated denial-of-service operation, which rendered Bank Melli's online banking and payment services inoperative for hours. Group 13 also claimed to have exfiltrated sensitive internal data and customer records, though the full extent of the breach remains unverified. The group publicized its operation on social media platforms, releasing images of login panels, internal systems, and employee data, which suggests prior access to internal networks possibly achieved through credential harvesting or exploitation of unpatched vulnerabilities in web-facing infrastructure. This cyber incident follows a broader pattern of tit-for-tat operations between pro-Israeli and pro-Iranian cyber entities, including recent intrusions on critical infrastructure, disinformation campaigns, and leaks aimed at damaging reputations or undermining public trust. Group 13 has previously targeted Iranian logistics and military sectors, aligning its actions with strategic objectives that serve both national security narratives and public influence operations.

The attack highlights the increasing prominence of non-state actors and hacktivist collectives operating in alignment with state interests, blurring the lines between civilian and military spheres in cyberspace. Strategically, this episode reinforces concerns about the vulnerability of financial institutions to asymmetric cyber threats and demonstrates how cyber tools are being wielded as instruments of geopolitical confrontation and psychological warfare in the Middle East.

Read more: https://therecord.media/pro-israel-hackers-claim-attack-on-iranian-bank

Iran Slows Internet to Prevent Cyber Attacks Amid Escalating Regional Conflict

Iran's recent move to significantly restrict domestic internet access represents a major escalation in its digital censorship and information control strategy amid intensifying geopolitical and domestic pressures. Spearheaded by state security and telecommunications authorities, the initiative centers on limiting Iranian users' access to a wide range of foreign platforms including Google, WhatsApp, and Instagram by reconfiguring national connectivity through a state-controlled network infrastructure. This policy shift is supported by technical enforcement mechanisms such as DNS filtering, IP blocking, deep packet inspection (DPI), and the redirection of traffic through government proxies, all coordinated under Iran's broader "National Information Network" (NIN) project.

The restrictions appear to have been triggered by a combination of international tensions, internal dissent, and concerns over foreign influence, especially during politically sensitive periods such as elections, protests, or cyber-related escalations. The state argues these controls are necessary for national security and to protect Iran's "digital sovereignty." However, critics contend the true objective is to tighten surveillance capabilities, suppress dissent, and isolate citizens from uncensored global discourse. Independent observers and civil society groups have noted a rise in forced migration of online activity to domestic alternatives that are easier for authorities to monitor, while also observing widespread disruptions in communication for businesses and civil institutions reliant on international digital services.

Technically, the shift aligns with longstanding ambitions by Iranian authorities to replicate the kind of sovereign internet model seen in countries like China, characterized by extensive censorship, content control, and surveillance integration. The implications of this move are far-reaching. It may deepen Iran's technological isolation from the global internet, restrict civil liberties, and complicate international efforts to engage Iranian society digitally. Strategically, it also signals a trend toward regional internet fragmentation, where authoritarian regimes build national "splinternets" to maintain political control, further fracturing the open internet into ideologically and technologically divided zones.

Read more: https://thehackernews.com/2025/06/iran-restricts-internet-access-to.html?

Israeli officials say Iran exploiting security cameras to guide missile strikes

Iranian state-aligned cyber operators have intensified their espionage efforts against Israeli targets by breaching security camera networks to monitor critical infrastructure and military operations. This operation, attributed to the Iranian-linked group known as Moses Staff, reflects Tehran's broader strategic objective of gathering intelligence on Israeli defense capabilities and operational readiness, particularly in the context of escalating regional hostilities. The campaign reportedly targeted commercial and governmental CCTV systems, allowing persistent remote access to live surveillance feeds. This access enabled operators to collect visual intelligence on sensitive military and civilian locations, including transportation hubs and air defense installations.

The breach involved a combination of credential harvesting, exploitation of unpatched vulnerabilities in surveillance systems, and lateral movement across compromised networks. Notably, the attackers leveraged remote desktop tools and bespoke malware to exfiltrate video streams and still images over prolonged periods. These tools facilitated long-term monitoring of Israeli defense activities without alerting system administrators. The campaign coincides with an uptick in physical attacks against Israeli assets, suggesting a coordinated effort to align cyber reconnaissance with kinetic military operations or sabotage planning.

This development underscores a significant evolution in Iran's cyber-espionage strategy prioritizing real-time situational awareness and exploiting overlooked physical security layers like networked cameras. It also highlights the growing convergence of cyber and physical domains in modern intelligence gathering and warfare. The implications for national security are profound: the breach reveals vulnerabilities in civilian-operated surveillance systems that could be weaponized in geopolitical conflicts, particularly by state actors seeking asymmetric advantages. As regional tensions between Iran and Israel persist, such operations signal a shift toward more integrated and adaptive cyber campaigns, wherein digital intrusions serve as precursors or force multipliers for broader strategic objectives, including missile strikes or sabotage missions. This trend calls for enhanced scrutiny of IoT devices and infrastructure resilience within high-risk geopolitical environments.

Read more: https://therecord.media/iran-espionage-israeli-security-cameras-missile-attacks?

Malware & Vulnerabilities

State Department Targets IRGC-Linked CyberAv3ngers in $10M Reward Initiative

The U.S. Department of State, through its Rewards for Justice (RFJ) program, has issued a reward of up to $10 million for information leading to the identification or location of individuals affiliated with the pro-Iranian threat actor known as CyberAv3ngers. This cyber group is assessed to be linked to the Islamic Revolutionary Guard Corps (IRGC), specifically its cyber-focused arm, the IRGC Cyber Electronic Command. CyberAv3ngers has been implicated in a series of cyber operations targeting critical infrastructure, particularly in the United States and Israel. Their focus has centered on industrial control systems (ICS), including operational technology (OT) used in water utilities, energy infrastructure, and transportation systems.

CyberAv3ngers is known for exploiting vulnerabilities in programmable logic controllers (PLCs), such as Unitronics Vision Series PLCs, to disrupt system operations. They have used publicly available tools, default passwords, and unpatched firmware as entry points into sensitive infrastructure, highlighting persistent lapses in basic cybersecurity hygiene. The group's tactics include defacing human-machine interface (HMI) panels, issuing shutdown commands, and altering display screens with anti-Israeli or pro-Iranian messages. Such operations are not only intended to sabotage but also to send strategic messages aligned with Iran's broader regional influence campaign.

The decision to publicly attribute these attacks and offer a bounty underscores growing U.S. concern over the threat posed by ideologically motivated state-linked cyber actors targeting civilian infrastructure. It also reflects a broader pattern in which state proxies engage in disruptive cyber behaviour without triggering direct military reprisals. Strategically, this development reinforces the imperative for nations to harden critical infra-

structure against increasingly sophisticated and politically driven cyber threats. It also signals the willingness of the U.S. government to adopt aggressive countermeasures, including financial incentives for intelligence, in order to deter malign cyber activity and increase the operational risk for adversarial cyber operatives acting under state direction.

Read more: https://rewardsforjustice.net/rewards/cyberav3ngers/

Malware & Vulnerabilities

Malicious Code Surge: How PyPI, npm, and AI Tools Are Being Weaponized Against DevOps and Cloud Infrastructures

Unicode obfuscation has emerged as a subtle, yet powerful technique used by threat actors to bypass static code analysis and deceive both developers and security tools. The central focus of this issue involves software supply chain security and static application security testing (SAST), with key actors including malicious open-source package maintainers, application security researchers, and vendors of code scanning tools. The context is shaped by growing reliance on open-source dependencies and developer-friendly programming languages particularly JavaScript and Python that can be exploited using obscure language features or encoding tricks.

The core technical development involves the use of Unicode characters especially homoglyphs, right-to-left override (RTLO) characters, and invisible characters like non-breaking spaces or zero-width joiners to disguise malicious behaviour in code. These characters, when inserted strategically, can make code appear benign or functionally different to human reviewers and static analysers. For example, variable names using Cyrillic or Greek characters that resemble Latin characters may appear identical visually but function differently at runtime, creating opportunities for variable shadowing or logic subversion.

Attackers have also used RTLO characters to reverse the visible order of file extensions or command-line arguments, leading to misleading file names or execution flows. These tactics hinder code review and allow harmful logic to be smuggled into seemingly safe functions or packages, especially within open-source ecosystems like npm and PyPI. Static analysis tools may fail to flag such code if they do not normalize or visually flag suspect characters during scans.

The broader implication of Unicode-based obfuscation is its capacity to erode trust in source code transparency and undermine automated security pipelines. As software supply chain threats rise, understanding and mitigating Unicode abuse is critical for maintaining the integrity of codebases and reinforcing static analysis methodologies. It reflects a broader trend where adversaries increasingly exploit the gap between machine parsing and human interpretation to breach software supply chains.

Read more: https://safedep.io/digging-into-dynamic-malware-analysis-signals/#abnormal-binary-execution

https://www.veracode.com/blog/down-the-rabbit-hole-of-unicode-obfuscation/

Clone, Compile, Compromise: Water Curse's Open-Source Malware Trap on GitHub

A newly documented cyber-espionage campaign, dubbed Water Curse, has been attributed to a likely China-linked advanced persistent threat (APT) group targeting governmental and critical infrastructure entities across Southeast Asia. The key actors involved include the unidentified threat group whose tactics and infrastructure bear hallmarks of China-nexus APT activity and victims spanning government agencies, military institutions, and national telecommunications providers. This campaign unfolds within a broader geopolitical context marked by intensifying competition in the South China Sea, growing concerns over regional cyber sovereignty, and persistent tensions between China and neighboring states.

The Water Curse operation leverages a multi-stage infection chain and custom malware toolkit to conduct long-term intelligence gathering. Initial access is typically achieved through spear-phishing emails containing

malicious archive files, often exploiting password-protected RAR attachments to bypass email security filters. Once executed, the payload drops a loader that communicates with a command-and-control (C2) server to retrieve further modules, including surveillance and credential-theft components. These modules allow for the collection of system metadata, screenshots, keylogging, and lateral movement across compromised networks.

Notably, Water Curse incorporates anti-analysis features such as virtual machine detection, encrypted communications, and code obfuscation, demonstrating operational maturity and an intent to evade both automated and manual detection efforts. The C2 infrastructure is resilient, using dynamically generated domain names and cloud-based hosting to obscure attribution and ensure persistence.

The campaign aligns with longstanding regional espionage patterns involving cyber operations against political institutions and critical industries, aiming to extract strategic intelligence rather than cause disruption. Strategically, Water Curse illustrates the continued expansion of state-aligned cyber capabilities focused on influence projection and situational awareness in contested geopolitical environments. It reinforces the need for enhanced regional cybersecurity cooperation, threat intelligence sharing, and advanced detection capabilities to counter increasingly sophisticated and targeted cyber intrusions by nation-state actors.

Read more: https://www.trendmicro.com/en_us/research/25/f/water-curse.html

Russian Hackers Bypass Gmail 2FA in Complex Phishing and Social Engineering Attack

A sophisticated cyber operation linked to Russian threat actors has successfully bypassed Gmail's two-factor authentication (2FA) through a carefully orchestrated phishing and social engineering campaign, targeting individuals in government, defense, and security sectors. The actors involved are believed to be part of the state-sponsored group APT29, also known as Cozy Bear, which has longstanding ties to Russia's Foreign Intelligence Service (SVR). The operation highlights an evolution in adversarial tactics aimed at compromising high-value accounts protected by modern security protocols.

The attackers employed adversary-in-the-middle (AitM) techniques by deploying a phishing infrastructure capable of intercepting credentials and authentication tokens in real time. Victims were lured to credential-harvesting portals through emails impersonating trusted sources, often under the guise of urgent security notices. Once victims entered their credentials and 2FA codes, the attackers used those session tokens to gain immediate access to their Gmail accounts without needing the actual password again. This method enabled sustained access and bypassed alerts associated with suspicious login attempts, increasing the stealth and longevity of the intrusion.

Notably, the attackers tailored the phishing domains to closely resemble legitimate services, and in some cases, followed up with social engineering tactics via phone calls or text messages to pressure the targets into taking immediate action. The operation appears to have been conducted with a high degree of coordination and technical sophistication, reflecting both strategic intent and operational discipline.

This incident underscores the growing effectiveness of phishing operations against even hardened targets and highlights the limitations of 2FA when not coupled with robust phishing-resistant protocols like hardware security keys or passkeys. Strategically, the attack reveals persistent Russian interest in espionage-focused cyber operations against Western institutions. It also emphasizes the urgent need for both public and private sector entities to adopt advanced identity protection measures, as phishing continues to be a preferred vector for state-aligned cyber espionage activities.

Read more: https://www.bitdefender.com/en-au/blog/hotforsecurity/russian-hackers-bypass-gmail-2fa-in-complex-phishing-and-social-engineering-attack

Mocha Manakin delivers custom NodeJS backdoor via paste and run

A newly identified cyber threat campaign involving a Node.js-based backdoor, codenamed "Mocha Manakin," has been uncovered, showcasing a stealthy approach to persistent access and espionage operations. The campaign targets Windows systems and is notable for its abuse of the Node.js runtime environment a less common tactic that allows the malware to blend into environments where JavaScript-based applications are legitimate. The key actors behind this threat remain unattributed, though the operational tactics and focus on stealth suggest a well-resourced adversary with advanced capabilities, possibly aligned with state interests.

Mocha Manakin is delivered via phishing campaigns or trojanized software, deploying in multiple stages. Once executed, the malware establishes persistence by manipulating registry keys and creating scheduled tasks. It then launches a Node.js-based implant that connects to a command-and-control (C2) server, allowing the operators to execute commands remotely, exfiltrate files, and monitor system activity. The backdoor includes capabilities such as file enumeration, command execution, and reconnaissance, with the added benefit of operating in a less-detectable scripting environment compared to traditional compiled malware.

The use of Node.js as a backdoor platform represents a broader trend in threat actor innovation, where commonly used development frameworks are repurposed for malicious operations, evading traditional endpoint detection mechanisms. In this case, the threat actors utilize standard Node.js libraries to perform malicious functions while avoiding behaviors that would immediately trigger alerts. The modular nature of the malware also allows easy updates and customization, making it a flexible tool for extended campaigns.

Strategically, Mocha Manakin underscores the growing complexity of malware ecosystems and the expanding use of non-traditional programming languages in advanced persistent threat (APT) operations. It reflects a shift toward more evasive and adaptive tooling, reinforcing the need for defenders to monitor not just binary executables but also script-based and runtime-level anomalies. The campaign highlights the persistent risk posed by espionage-focused actors leveraging overlooked attack surfaces to infiltrate critical infrastructure and sensitive networks.

Read more: https://redcanary.com/blog/threat-intelligence/mocha-manakin-nodejs-backdoor/

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.