MANOHAR PARRIKAR INSTITUTE FOR
DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

CYBER *Digest*

December 2025

Sandworm Hackers Hit Ukraine's Grain Industry with Wiper Attacks

Reports indicate that between June and September, the Kremlin-linked group Sandworm launched several data-wiping malware attacks against Ukrainian entities in the grain, energy, logistics, and government sectors.[1] Although wiper attacks have been common since the invasion, Ukraine's agricultural sector, a vital export lifeline and has seldom been directly targeted. Sandworm, according to assessments by Western intelligence, is linked to Russia's GRU, which is responsible for some of the most destructive cyberattacks Ukraine has faced. Ukrainian cyber officials have repeatedly cautioned that Russian groups, including Sandworm, often synchronize such cyber operations with missile and drone strikes to maximize disruption.

Cyberattack Targeted Russian Port Operator

Russian port operator Port Alliance has confirmed service disruptions following a cyberattack that targeted critical parts of its digital infrastructure.[2] The company said attackers carried out a large-scale distributed denial-of-service (DDoS) attack and attempted to infiltrate its networks. Despite the intensity of the assault, Port Alliance reported that its terminals and related facilities remained fully operational. According to the firm, the hackers employed a botnet of more than 15,000 unique IP addresses from across the globe, including some inside Russia, and repeatedly shifted tactics to evade security defenses. Maritime logistics hubs are now central targets in modern conflict, with cyberattacks used to disrupt economies and signal geopolitical intent.

Breach Exposes Knownsec's China-Backed Hacking Tools

Reports indicate that Chinese cybersecurity firm Knownsec has suffered a major data leak exposing more than 12,000 confidential files and offering a rare look into China's state-linked hacking tools and operations.[3] Knownsec, a key player in China's cyber ecosystem, had been involved in developing cyber weapons and maintaining lists of foreign targets. The leaked documents reveal broad espionage efforts across more than 20 countries, including intrusions into critical infrastructure such as telecommunications networks.

Exposed data includes 95 GB of Indian immigration records, 3 TB of South Korean call logs, and 459 GB of transport data from Taiwan. The leak also uncovered various hacking tools, including remote access trojans (RATs) and specialized utilities for covertly extracting data from Android devices. Although Beijing has denied any knowledge of the incident, the breach raises fresh concerns about the role of private firms in China's state-sponsored cyber operations.

Australian Spy Chief Says Chinese Hackers Probed Key Facilities

Australia's spy chief has accused Chinese state and military-backed hackers of probing the nation's telecommunications networks and critical infrastructure, warning that such activity poses a serious risk of economic disruption and potential sabotage.[4] He said espionage cost Australia an estimated US$8.1 billion last year, including billions in stolen trade secrets and intellectual property.

He further noted that the Chinese hacking group Volt Typhoon had not only infiltrated U.S. telecom systems as part of a strategic espionage campaign, but had also been probing Australia's telecommunication networks. He said Volt Typhoon's operations showed intent to disrupt, having already compromised U.S. critical infrastructure to prepare for potential sabotage. He warned that large-scale disruption to telecom networks could severely affect banking, transportation, and even essential services such as water and power.

Pakistan NCCIA Arrests Suspect in Massive Personal Data Leak

Pakistan's National Cyber Crime Investigation Agency (NCCIA) has arrested a man accused of selling the personal data of Pakistani citizens online. Authorities also seized a hard disk reportedly holding information on millions of individuals.[5] The arrest followed an Interior Ministry–ordered probe into reports of widespread data leaks. Acting on the directive, the NCCIA chief set up a special investigation committee, which, after several days of inquiry, traced and detained the suspect. Officials said a one-terabyte hard disk found in the suspects' possession contained sensitive data that he had allegedly bought on the black market. Investigators added that he was running more than ten websites used to sell people's personal information.

In a separate development, four senators disclosed that they had been targeted by scammers.[6] One of the affected lawmakers said the attackers primarily used financial fraud schemes, while another reported losing money during an online transaction. The senators also noted that the scammers appeared to have information about their family members.

Pak-Linked Hackers Hit Indian Govt, Military with Spyware

According to assessments made by intelligence agencies, they have alerted the Ministry of Home Affairs to a major cyber-espionage operation by Pakistan-linked group Transparent Tribe, which is targeting Indian government and military networks with an advanced spyware tool known as DeskRAT.[7] The report notes that the group has upgraded its methods this year, shifting from public cloud services such as Google Drive to private servers, making their activity harder to detect and block.

According to agencies, the attackers are deploying sophisticated phishing emails disguised as government circulars, ZIP files, and intelligence briefings that are often timed to coincide with security alerts or border incidents. This is to lure officials into opening infected attachments. The report further warns that the hackers are leveraging artificial intelligence and large language models (LLMs) to quickly generate new malware variants, enabling them to stay ahead of traditional cybersecurity defenses.

India File

- The Centre is preparing to introduce a new set of cybersecurity regulations for the power sector, outlining extensive upgrades to strengthen India's electricity network against cyber threats.[8] The move comes in the wake of heightened security concerns following–Pakistan conflict in May 2025, during which

India reportedly blocked at least two lakh cyberattacks targeting its power infrastructure. The rules, drafted by the Central Electricity Authority (CEA), are expected to take effect from April 2026 after public consultation and final revisions are completed.

- The Indian government has confirmed that seven major airports were impacted by cyberattacks, including Delhi, where incoming flights reported GPS spoofing.[9] Airports in Mumbai, Kolkata, Hyderabad, and Bengaluru were also affected. Officials said no flights were disrupted despite the spoofing attempts. In response, all Indian airlines have completed the necessary software upgrades, allowing their aircraft to safely resume commercial operations.

- The Ministry of Electronics and Information Technology (MeitY) has unveiled India's AI Governance Guidelines under the IndiaAI Mission to promote safe, inclusive, and responsible adoption of artificial intelligence across sectors.[10] The release marks a major milestone ahead of the India-AI Impact Summit 2026, reinforcing India's leadership in responsible AI governance. The guidelines outline a strong governance framework aimed at fostering innovation while ensuring that AI is developed and deployed safely and ethically.

- The Government of India has notified the Digital Personal Data Protection (DPDP) Rules, 2025, completing the implementation of the DPDP Act, 2023.[11] Together, the Act and the new Rules provide a simple, citizen-centric, and innovation-friendly framework for the responsible handling of digital personal data. Passed by Parliament on 11 August 2023, the DPDP Act sets out a comprehensive system for safeguarding digital personal data, defining the responsibilities of Data Fiduciaries and the rights and duties of Data Principals.

- India's Department of Telecommunications (DoT) has issued a new regulation requiring WhatsApp and other OTT communication apps like Telegram and Signal to remain continuously linked to users' SIM cards, with platforms given 90 days to comply. The directive also mandates automatic six-hour logouts on web and desktop versions, requiring re-authentication via QR code pairing. The move aims to curb fraud and anonymous misuse by ensuring accountability, as current systems allow apps to function even if a SIM is removed or deactivated. Telecom operators, represented by COAI, support the measure, arguing it will reduce spam and financial fraud while strengthening digital security.[12] The government is invoking its powers under the amendment rules, notified in October, to bring messaging platforms under a more tightly regulated cybersecurity framework.

[1] The Record, Russia's Sandworm hackers deploying wipers against Ukraine's grain industry, 6 November 2025, https://therecord.media/russia-sandworm-grain-wipers

[2] The Record, Cyberattack on Russian port operator aimed to disrupt coal, fertilizer shipments, 14 November 2025, https://therecord.media/cyberattack-on-russian-port-operator

[3] SC Media, Cybersecurity breach exposes Chinese firm Knownsec's government-backed hacking tools, 17 November 2025, https://www.scworld.com/brief/cybersecurity-breach-exposes-chinese-firm-knownsecs-government-backed-hacking-tools

[4] Reuters, Australian spy chief says Chinese hackers probing telecoms, key facilities, 12 November 2025, https://www.reuters.com/world/china/australia-spy-chief-says-chinese-hackers-probing-telecommunications-critical-2025-11-12/

[5] The Express Tribune, Man arrested for selling data of millions of Pakistanis online, 7 November 2025, https://tribune.com.pk/story/2576342/man-arrested-for-selling-data-of-millions-of-pakistanis-online

[6] The Express Tribune, Four senators reveal they were targeted by scammers, 6 November 2025, https://tribune.com.pk/story/2576116/four-senators-reveal-they-were-targeted-by-scammers

[7] The New Indian Express, Pak-linked hacker group targets Indian government, military networks with advanced spyware: Report, 7 November 2025, https://www.newindianexpress.com/nation/2025/Nov/07/pak-linked-hacker-group-targets-indian-government-military-networks-with-advanced-spyware-report

[8] Money Control, Power sector set for major security upgrade as Centre plans new framework against cyber threats, 6 November 2025, https://www.moneycontrol.com/news/business/power-sector-set-for-major-security-upgrade-as-centre-plans-new-framework-against-cyber-threats-13657489.html

[9] NDTV, Govt Confirms Seven Airports Affected By Cyberattack: Report, 1 December 2025, https://www.ndtvprofit.com/nation/govt-confirms-cyber-attacks-on-seven-airports-report

[10] PIB, MeitY Unveils India AI Governance Guidelines under IndiaAI Mission to Ensure Safe, Inclusive, and Responsible Adoption of Artificial Intelligence across Sectors, 5 November 2025, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2186639&reg=3&lang=2

[11] PIB, Government notifies DPDP Rules to empower citizens and protect privacy, 14 November 2025, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2190014&reg=3&lang=2

[12] Voicendata, DoT orders WhatsApp and other apps to enforce continuous SIM link, 1 December 2025, https://www.voicendata.com/ott/dot-orders-whatsapp-and-other-apps-to-enforce-continuous-sim-link-10828702