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

CYBER *Digest*

November 2025

- Ukraine Parliament Backs Cyber Forces Plan
- U.S. Air Force Probes Possible Data Breach
- China Alleges U.S. Hacked National Time Center
- Seventy-two Nations Sign First UN Cybercrime Treaty
- Renault UK Confirms Customer Data Stolen
- China-Linked Hack Hits Major US Law Firm
- Hackers Took Over Airport PA Systems in US, Canada
- Raids on Myanmar scam compounds lead to mass exodus
- India File

Ukraine Parliament Backs Cyber Forces Plan

The Ukrainian parliament has approved in its first reading a bill to create Cyber Forces within the country's military, highlighting the growing significance of cyberspace in the ongoing war with Russia.[1] Backed by 255 lawmakers, the bill seeks to establish the Cyber Forces as a dedicated military command responsible for strengthening Ukraine's defense and security capabilities in cyberspace. The Main Directorate of Radio Electronic and Cyber Warfare under Ukraine's General Staff will oversee its formation. The new command will conduct regular training and manage the recruitment and coordination of cyber force reserves. Service in these reserves will not require formal military enlistment and can be performed temporarily or periodically to carry out specific missions.

U.S. Air Force Probes Possible Data Breach

The U.S. Air Force is investigating a possible exposure of service members' personal data through Microsoft SharePoint, a collaborative platform used for file sharing, management, and intranet services.[2] The Department of the Air Force confirmed awareness of the privacy issue and stated that a preliminary investigation is underway to determine its extent and identify necessary corrective measures. Following the incident, reports indicated that the Air Force continues to use the system while implementing mitigation measures.

China Alleges U.S. Hacked National Time Center

China has accused the United States of conducting cyber espionage and infiltrating its National Time Service Center, warning that such breaches could have disrupted communication networks, financial systems, power supplies, and even the international standard time.[3] According to Chinese authorities, the U.S. National Security Agency carried out a prolonged cyberattack campaign targeting the center. The authorities further alleged that the U.S. intelligence agency exploited a vulnerability in the messaging service of a foreign smartphone brand in 2022 to gain access to staff members' devices, though the brand was not identified. The National Time Service Center, a research institute under the Chinese Academy of Sciences, is responsible for generating, maintaining, and disseminating China's standard time.

Seventy-two Nations Sign First UN Cybercrime Treaty

Seventy-two countries have signed a landmark United Nations treaty in Hanoi to combat cybercrime.[4] Adopted by the UN General Assembly in December 2024 after five years of negotiations, the Convention against Cybercrime creates the first global framework for investigating and prosecuting online offences including ransomware, financial fraud, and the non-consensual sharing of intimate images.The treaty criminalises a wide range of cyber-dependent and cyber-enabled crimes, enables cross-border sharing of electronic evidence, and establishes a 24/7 international cooperation network among

member states. Notably, it is the first international agreement to classify the non-consensual distribution of intimate images as a criminal offence, a major milestone for victims of online abuse.[5]

Renault UK Confirms Customer Data Stolen

Renault UK has confirmed that a cyberattack on a third-party data processing provider led to the theft of some customer information.[6] The company stated that no financial details such as passwords or bank account information were compromised, though other personal data was accessed. Renault has advised customers to remain cautious. While the French automaker did not disclose how many individuals may have been affected, citing ongoing security concerns, it noted that the incident has not impacted its own systems and is not expected to have broader consequences for the company.

Renault UK said that the breach may also impact people who entered competitions or shared their information with the company without actually purchasing a vehicle. According to the carmaker, the compromised data may include some or all of the following: customer names, addresses, dates of birth, gender, phone numbers, vehicle identification numbers, and vehicle registration details.

China-Linked Hack Hits Major US Law Firm

Suspected Chinese state-sponsored hackers have breached the computer systems of U.S. law firm Williams & Connolly, which represents several of the nation's most influential political figures, according to a client notification letter and media reports.[7] The attack is part of a broader espionage campaign targeting multiple U.S. law firms, with hackers gaining access to the email accounts of selected attorneys. The campaign reflects Beijing's ongoing efforts to gather intelligence supporting its strategic competition with Washington across national security, trade, and other domains. In this instance, the attackers exploited a previously unknown software vulnerability highly prized in espionage circles for its ability to operate undetected to infiltrate Williams & Connolly's network.

Hackers Take Over Airport PA Systems in US, Canada

Hackers hijacked public address systems at four airports- three in Canada and one in the United States to broadcast messages praising Hamas and criticizing U.S. President Donald Trump, according to officials and media reports.[8] At Victoria International Airport in British Columbia, hackers played messages in a foreign language along with music over the PA system, an airport spokesperson said. The intrusion occurred through a breach of third-party, cloud-based software used to manage the system. Airport officials said they quickly switched to an internal system to regain control, and normal operations were restored shortly afterward.

Raids on Myanmar scam compounds lead to mass exodus

Cyber scam operations have surged in Cambodia and Myanmar since the COVID-19 pandemic, as many Chinese-owned

casinos and hotels shifted to illegal online activities. From large-scale scam centres, tens of thousands of workers run online scams known as pig-butchering, generating tens of billions of dollars in illicit profits annually.

A global effort targeting the vast scam-compound economies operating in Southeast Asia, particularly along the Thai-Myanmar border and in Cambodia is currently underway. The U.S. and U.K. launched an operation against Cambodian tycoon Chen Zhi, chairman of the Prince Group, for orchestrating these forced-labor enterprises.[9] This action included the U.S. Department of Justice filing the largest forfeiture action in history, seizing approximately 127,271 Bitcoin, valued at about $15 billion. In response to misuse, SpaceX proactively disabled over 2,500 Starlink satellite devices used by the scam centers in Myanmar, following operations at sites like KK Park.[10] These multilateral actions aim to dismantle criminal networks relying on illicit finance and human trafficking.

Nearly 500 Indian nationals who fled KK Park were detained after they crossed into Thailand. The Indian government has been coordinating with Thai authorities to repatriate these citizens.[11] Indian authorities had carried out a similar mission in March, bringing home 549 nationals following a previous cybercrime crackdown along the same border region.[12]

Dozens of South Korean nationals detained in Cambodia for their alleged involvement in cyber scam operations have been repatriated and placed under arrest, according to South Korean authorities.[13] A police official told media that officers apprehended the individuals aboard a chartered flight sent to bring them back from Cambodia.

India File

- According to reports, the National Stock Exchange (NSE) faces nearly 170 million cyberattacks each day, with a dedicated team of cybersecurity experts working around the clock to maintain seamless operations.[14] During "Operation Sindoor," a simulated DDoS exercise, the NSE recorded its highest-ever volume of 400 million cyberattacks in a single day. Despite the scale of the assault, attackers were unable to cause any disruption because of coordinated efforts of personnel, technology, and automated defense systems.
- The Central Bureau of Investigation (CBI) is investigating a large-scale fake call centre network dismantled in Igatpuri in August 2025, which allegedly operated under the protection of a Maharashtra Police officer holding the rank of Inspector General (IGP).[15] The officer, reportedly one of the key masterminds, is believed to have used his political influence to shield and support the syndicate, which had operations spread across multiple districts and possible political backing. The syndicate operated using advanced digital tools, cloud servers, e-commerce gateways, and VPNs to target victims overseas.

- In a recent cybercrime incident, the Chief Information Security Officer of Generali Central Life Insurance Company filed a complaint after the firm was allegedly targeted by the Medusa ransomware group.[16] Generali has appointed a forensic audit firm to conduct a detailed technical investigation. While the company has not received a direct ransom demand, a post on the Medusa Blog reportedly demanded: USD 500,000 for deleting the stolen data; USD 500,000 for allowing the company to download its data, and USD 10,000 for extending the payment deadline. The post further warned that if payment was not made by October 25, the stolen data would be sold on the dark web.

- Following a cyberattack earlier this year that resulted in the loss of critical data from the Indian Council of Agricultural Research (ICAR) including information related to recruitment and research projects, the organisation has removed the director of the institute overseeing its data centre, just three days before his tenure was set to end.[17] Reports indicate that ICAR, the country's apex agricultural research body, has also transferred two Principal Scientists linked to the institute as part of disciplinary action recommended by an inquiry committee that investigated the breach. In October, an official order appointed a new director for the Indian Agricultural Statistics Research Institute (IASRI), which operates under ICAR and manages its central data centre.

[1] The Kyiv Independent, "Ukraine's parliament backs creation of cyber forces in first reading", 9 October 2025, https://kyivindependent.com/ukraines-parliament-backs-creation-of-cyber-forces-in-first-reading/

[2] Air & Space Forces, "Air Force Investigating Privacy Compromise on SharePoint Sites", 6 October 2023, https://www.airandspaceforces.com/air-force-investigating-privacy-issue-microsoft-sharepoint/

[3] Reuters, "China accuses US of cyber breaches at national time centre", 21 October 2025, https://www.reuters.com/world/china/china-accuses-us-cyber-breaches-national-time-centre-2025-10-19/

[4] United Nations, United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-16&chapter=18&clang=_en

[5] UN News, "Sixty-five nations sign first UN treaty to fight cybercrime, in milestone for digital cooperation",

[6] BBC, "Renault customers told to be vigilant after data hack", 3 October 2025, https://www.bbc.com/news/articles/c1edy30qzdno

[7] CNN, "US law firm with major political clients hacked in spying spree linked to China", 8 October 2025, https://edition.cnn.com/2025/10/08/politics/williams-and-connolly-law-firm-hack-chinese-hackers-suspected

[8] Reuters, "Hackers use some Canada and US airport PA systems to praise Hamas, criticize Trump ", 17 October 2025, https://www.reuters.com/business/media-telecom/hackers-use-some-canada-us-airport-pa-systems-praise-hamas-criticize-trump-2025-10-16/

[9] US Department of Justice, Chairman of Prince Group Indicted for Operating Cambodian Forced Labor Scam Compounds Engaged in Cryptocurrency Fraud Schemes, 14 October 2025, https://www.justice.gov/opa/pr/chairman-prince-group-indicted-operating-cambodian-forced-labor-scam-compounds-engaged

[10] BBC, "SpaceX says it has cut Starlink services to Myanmar scam camps", 22 October 2025, https://www.bbc.com/news/articles/cpd2e5541d1o

[11] India Today, "500 Indians from Myanmar scam-hub stranded in Thailand; Delhi trying to help them", 30 October 2025, https://www.indiatoday.in/india/story/indian-nationals-detained-thailand-fleeing-myanmar-repatriated-scam-centre-2810350-2025-10-29

[12] India Today, "549 Indians Rescued from Myanmar Cyber Crime Centres", 12 March 2025 https://www.deccanchronicle.com/nation/india-brings-back-549-citizens-freed-from-myanmar-thai-border-cyber-crime-centres-1866391

[13] Aljazeera, "South Koreans freed from Cambodian scam centres return home under arrest", 18 October 2025, https://www.aljazeera.com/news/2025/10/18/south-koreans-freed-from-cambodian-scam-centres-return-home-under-arrest

[14] Business Standard, "NSE faces around 170 mn daily cyberattacks; cyber warriors safeguard ops", 12 October 2025, https://www.business-standard.com/markets/news/nse-faces-around-170-mn-daily-cyberattacks-cyber-warriors-safeguard-ops-125101200146_1.html

[15] The Free Press Journal, "Igatpuri Fake Call Centre Probe: How A Fake Call Centre Network Grew Under An IG's Supervision, CBI Probe Reveals Shocking Links (FPJ Exclusive)", 14 October 2025, https://www.freepressjournal.in/mumbai/maharashtra-police-top-brass-under-scanner-as-cbi-uncovers-deep-rooted-fake-call-centre-racket

[16] The Free Press Journal, "Mumbai Cyber Crime News: Generali Central Life Insurance Targeted By Medusa Ransomware; FIR Filed",13 October 2025, https://www.freepressjournal.in/mumbai/mumbai-cyber-crime-news-generali-central-life-insurance-targeted-by-medusa-ransomware-fir-filed

[17] The Indian Express, "ICAR data breach: Head of institute replaced 3 days before end of term", 20 October 2025, https://indianexpress.com/article/india/icar-data-breach-head-of-institute-replaced-3-days-before-end-of-term-10316914/