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

CYBER *Digest*

September 2026

- US Mobilises Private Sector to Combat Transnational Cybercrime
- Ransomware Attack Hits Colombia's Justice Ministry
- Iran-Linked Hackers Disrupt UK Power Plant
- UAE Thwarts Cyberattacks Targeting Energy, Aviation Sectors
- Cyberattack Disrupts Operations at Three North Carolina Ports
- Italy Creates Military Cyber Role
- UK Airport Customer Data Breached
- INTERPOL Report Links AI to Over Half of Africa's Cybercrime
- Ransomware Disrupts Canada Health Sciences Centre Systems
- India File

US Mobilises Private Sector to Combat Transnational Cybercrime

The United States has issued a memorandum aimed at strengthening efforts to combat cybercrime perpetrated by transnational criminal organizations (TCOs) by leveraging the capabilities of the private sector.[1] The memorandum highlights the U.S. private sector's technological expertise, scale and speed as critical assets in countering cyber threats. It notes that American businesses have historically been underutilized in identifying and disrupting criminal networks operating online. Under the new approach, the U.S. Government will partner with vetted American companies under Federal oversight to enhance efforts against TCOs. The initiative seeks to use private-sector innovation alongside other national capabilities to disrupt cyber-enabled crime, fraud and predatory schemes targeting American citizens, businesses and national security.

Ransomware Attack Hits Colombia's Justice Ministry

Colombia's Ministry of Justice confirmed that a ransomware attack disrupted part of its technology infrastructure, affecting several public-facing services.[2] The incident occurred just five days before the country's presidential handover. The attack disrupted services related to illicit-drug monitoring and legal processes, highlighting growing cyber threats facing Colombian government institutions. The incident came a day after Colombia's national CERT, ColCERT, warned that ransomware groups were increasingly targeting the country.

Iran-Linked Hackers Disrupt UK Power Plant

Iran-linked hackers reportedly disrupted a British power plant, according to a report.[3] The incident was not publicly disclosed until weeks later, suggesting that the affected facility may have been relatively small and that authorities sought to limit publicity surrounding the attack.. However, UK authorities, including the National Cyber Security Centre (NCSC), have provided limited public information about the incident. The reported attack comes amid concerns over potential cyber operations by Iran and Iran-linked groups following its conflict with the US earlier this year. Since the start of the Iran war, Iranian hackers have targeted the critical infrastructure of the US and its allies. Other than Israel, the UK is generally considered to be a major ally of the US.

UAE Thwarts Cyberattacks Targeting Energy, Aviation Sectors

The UAE's Cyber Security Council has thwarted cyberattacks targeting the country's aviation, energy and education sectors, a state news agency reported.[4] The council said the intrusion attempts were detected and contained before attackers could achieve their objectives or disrupt critical systems and services. The attacks involved multiple techniques, including attempts to breach digital infrastructure, compromise accounts and operational data, launch targeted phishing campaigns and exploit users to gain access to targeted environments. National cybersecurity teams detected and repelled the malicious activity, tracked the attackers' pathways and indicators of compromise, and

implemented technical measures to neutralise the threats. The council said the measures also prevented the attacks from spreading and helped protect critical infrastructure and essential services across the country.

Italy Creates Military Cyber Role

Italy's Council of Ministers has approved a reform strengthening the armed forces' role in protecting national security in cyberspace.[5] The reform, sponsored by Defence Minister, establishes a dedicated military cyber domain and defines a national cyberspace area of interest for defence and military security. The Defence Ministry will identify and periodically update its boundaries. Under the new framework, the Chief of Defence Staff will serve as the Defence Ministry's cyber authority and assume overall responsibility for defence-related data, while existing national cyber governance arrangements remain in place. The reform also creates a new category of military cyber specialists aimed at developing and retaining highly skilled personnel as cyber capabilities become increasingly important to modern warfare and national defence.

UK Airport Customer Data Breached

Three major UK airports- Manchester, East Midlands and London Stansted have been hit by a cyber incident in which hackers accessed the personal data of approximately 8.7 million customers and demanded a ransom.[6] Manchester Airports Group (MAG), which operates the airports, said the attackers obtained customer email addresses, vehicle registration details and postcodes over the weekend. The majority of the compromised information related to email addresses provided for Wi-Fi registration at airport terminals. MAG said it refused to pay the undisclosed ransom and confirmed that passenger safety and aviation security were not affected. The company said it had contained the incident and was taking measures to protect customer information.

INTERPOL Report Links AI to Over Half of Africa's Cybercrime

Artificial intelligence is enabling 55% of reported cybercrime across Africa, making attacks faster, more scalable and increasingly difficult to detect, according to INTERPOL's African Cyberthreat Assessment Report 2026.[7] The report highlights the rapid expansion of Africa's digital landscape, with more than 1.1 billion mobile subscribers recorded in 2025. However, fragmented cybercrime legislation and limited AI readiness among law enforcement agencies are creating significant challenges in combating emerging threats. Based on survey data from 36 African member countries, the report identifies a major shift in the nature of cybercrime, describing it as an increasingly industrialized and borderless ecosystem rather than a collection of isolated incidents. INTERPOL warned that stronger regional cooperation and improved technological capabilities are needed to address the evolving threat.

Ransomware Disrupts Canada Health Sciences Centre Systems

A ransomware attack on Winnipeg's Health Sciences Centre, Manitoba's largest hospital, has disrupted certain facility maintenance systems, affecting door

access, heating, ventilation and air conditioning.[8] Shared Health said the incident has not affected patient care or clinical operations, which continue uninterrupted. The health authority said there is currently no indication that patients have been impacted and urged those requiring medical services to attend the hospital as planned. An investigation is underway to determine the nature and scope of the attack and assess the affected systems. The authority has notified the provincial government and sought assistance from cybersecurity experts to contain the incident and restore affected facility systems.

India File

- India recorded 18,187 mobile threat detections in the first quarter of 2026, the highest among Asia-Pacific markets analysed by Kaspersky. Indonesia followed with 15,163 detections, while China reported 6,797.[9] Kaspersky's analysis highlights a growing concentration of mobile cyber threats across the region, with attackers increasingly targeting fewer users but repeatedly compromising the same victims. Across the eight APAC markets studied, the average number of detections per affected user rose 49% year-on-year, from 4.9 to 7.3 in Q1 2026. The increase was observed across all eight markets despite an overall decline in the number of users encountering mobile threats, indicating that those targeted are facing more frequent attacks.
- The National Institute of Electronics and Information Technology (NIELIT), under the Ministry of Electronics and Information Technology (MeitY), launched CYBER KUSHTI 2026 on August 15.[10] The national cybersecurity and Artificial Intelligence (AI) hackathon aims to test and recognise human judgment and decision-making in cybersecurity assessments. The competition was organised in collaboration with the Information Sharing and Analysis Center (ISAC) Foundation under the National Security Database (NSD), with the Indian Computer Emergency Response Team (CERT-In) serving as the Knowledge Partner. The initiative seeks to provide participants with a platform to demonstrate their cybersecurity and AI capabilities while promoting innovation and strengthening India's cybersecurity talent ecosystem.
- The Government has taken note of the 2026 Standing Committee's recommendation to scale up the CyberShakti programme, aimed at strengthening cybersecurity awareness and skills among women government officials.[11] The programme was initially approved for two years beginning in October 2024. Its second phase was recommended by the Working Group on Cyber Security in May 2026, with the objective of expanding the initiative and further enhancing the cybersecurity capabilities of women officials across government institutions.
- The Indian Computer Emergency Response Team (CERT-In) detected and successfully mitigated more than 9.2 lakh incidents involving malicious

scanning, probing and exploitation of vulnerable services targeting India's banking and healthcare sectors over the past one-and-a-half years.[12] In the healthcare sector alone, CERT-In identified 34,480 such incidents, including 18,855 cases during the first six months of 2026. The figures highlight the growing volume of cyber threats targeting critical sectors and the continued need for stronger cybersecurity measures to protect sensitive systems and essential services.

- The Indian Cyber Crime Coordination Centre (I4C) under the Ministry of Home Affairs has warned users about a growing cyber fraud campaign involving malware-laced applications promoted through Facebook and Instagram advertisements disguised as pornographic content.[13] According to the advisory, users are tricked into downloading APK files from sources outside official app stores, potentially giving cybercriminals control over their mobile devices. Once installed, the malicious applications can enable attackers to monitor online activity and conduct unauthorised banking transactions. Authorities cautioned that the apps, advertised as gateways to adult content, may instead contain malware capable of compromising devices.
- On August 11, the Press Information Bureau (PIB) reported that the Minister of State for Home Affairs Bandi Sanjay Kumar informed the Lok Sabha in a written reply that the Government has taken several measures to combat cyber fraud.[14] As of June 30, 2026, the I4C had blocked 3,718 mobile applications, including fraudulent loan apps, under Sections 69(A) and 79(3)(b) of the Information Technology Act, 2000. More than 30.48 lakh suspect identifiers received from banks and 32.08 lakh Layer-1 mule accounts were shared with entities participating in the Suspect Registry, helping prevent transactions worth Rs. 25,698 crore. The Government has also blocked more than 15.75 lakh SIM cards and 5.77 lakh IMEIs reported by police authorities as part of efforts to curb cyber-enabled financial fraud.
- Representatives from CERT-In participated in the annual Asia Pacific Computer Emergency Response Team (APCERT) Drill, which tests the incident response capabilities of leading Computer Security Incident Response Teams (CSIRTs) across the Asia-Pacific region.[15] The 2026 exercise focused on the theme "Incident Response: RMM-related Compromise", addressing real-world cybersecurity threats arising from the malicious use of Remote Monitoring and Management (RMM) solutions widely deployed in enterprise environments. The drill aimed to strengthen regional coordination, enhance incident response capabilities and improve preparedness against cyberattacks involving the misuse or compromise of RMM technologies.

[1] The White House, Expanding Capabilities To Combat Transnational Cyber-Enabled Crime, 12 August 2026, https://www.whitehouse.gov/presidential-actions/2026/08/expanding-capabilities-to-combat-transnational-cyber-enabled-crime/

[2] Dark Reading, Ransomware Hits Colombian Justice Ministry Days Before Presidential Transition, 12 August 2026, https://www.darkreading.com/cyberattacks-data-breaches/ransomware-hits-colombian-justice-ministry-presidential-transition

[3] Security Week, Iran-Linked Hackers Shut Down UK Power Plant for Four Days, 24 August 2026, https://www.securityweek.com/iran-linked-hackers-shut-down-uk-power-plant-for-four-days/

[4] Arab News, UAE thwarts cyber attacks targeting energy and aviation sectors, 10 August 2026, https://www.arabnews.com/middle-east/uae-thwarts-cyber-attacks-targeting-energy-and-aviation-sectors-2654095

[5] Euractiv, Italy creates military cyber specialist role under new defence reform, 5 August 2026, https://www.euractiv.com/news/italy-creates-military-cyber-specialist-role-under-new-defence-reform/

[6] BBC, Hackers steal data from millions of airport customers, 27 August 2026, https://www.bbc.com/news/articles/c7v4353rry7o

[7] INTERPOL, INTERPOL report finds AI linked to more than half of cybercrime in Africa, 3 August 2026, https://www.interpol.int/en/News-and-Events/News/2026/INTERPOL-report-finds-AI-linked-to-more-than-half-of-cybercrime-in-Africa

[8] CBC, Ransomware attack on Health Sciences Centre affects doors, ventilation and air conditioning, 10 August 2026, https://www.cbc.ca/news/canada/manitoba/health-sciences-centre-ransomware-hack-9.7302058

[9] Business Standard, India tops APAC in mobile threat detections as attacks turn more targeted, 26 August 2026, https://www.business-standard.com/technology/tech-news/india-mobile-threats-cybercriminals-kaspersky-apac-2026-126082600626_1.html

[10] PIB, NIELIT Launches CYBER KUSHTI 2026: National Cybersecurity & AI Hackathon scores judgment rather than detection speed, 16 August 2026, https://www.pib.gov.in/PressReleaseDetail.aspx?PRID=2300120&reg=48&lang=1

[11] PIB, Government Strengthens Cyber Security Capacity of Women Officials through CyberShakti Programme, 12 August 2026, https://www.pib.gov.in/PressReleaseDetail.aspx?PRID=2298110&reg=48&lang=1

[12] The Times of India, 9 lakh cyber attacks detected in India's banking and healthcare sectors", 8 August 2026, https://timesofindia.indiatimes.com/city/bengaluru/9-lakh-cyber-attacks-detected-in-indias-banking-and-healthcare-sectors/articleshow/133051968.cms

[13] India Today, Porn app trap can hack phones, empty bank accounts: Govt issues cyber fraud alert, 31 August 2026, https://www.indiatoday.in/india/story/porn-app-scam-alert-mha-warns-apk-malware-can-hack-phones-and-empty-bank-accounts-2984031-2026-08-31

[14] PIB, "Misleading Mobile Applications", 11 August 2026, https://www.pib.gov.in/PressReleaseDetail.aspx?PRID=2297626&reg=6&lang=1

[15] Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT), APCERT Cyber Drill 2026 "Incident Response: RMM-related Compromise, 27 August 2026, https://www.hkcert.org/press-centre/apcert-cyber-drill-2026-incident-response-rmm-related-compromise