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

CYBER *Digest*

April 2026

- Cyber Warfare Escalates in US–Israel Conflict with Iran
- Trump White House Unveils New Cybersecurity Strategy
- Puerto Rico Transport Services Hit by Cyberattack
- Ransomware Attack Disrupts Operations at Spanish Port
- Dutch Finance Ministry Portal Knocked Offline by Cyberattack
- Taiwan targeted by LNG shortage disinformation campaign
- Albanian Parliament hit by major cyberattack, emails disrupted
- India File

Cyber Warfare Escalates in US–Israel Conflict with Iran

The cyber domain has become a crucial component in the ongoing conflict in West Asia. Reports suggest that Israel infiltrated Tehran's extensive traffic camera network to monitor the movements of bodyguards assigned to Ayatollah Ali Khamenei and other senior Iranian officials, allegedly in preparation for an assassination attempt on the Supreme Leader.[1] The cameras in Iran are thought to form part of the state's broader surveillance system, used by authorities to identify and track protesters and political dissidents. However, according to the report, Israel's intelligence agency, Mossad, managed to repurpose this network for its own operations against the Iranian regime.

In a separate incident, a major cyberattack severely disrupted the global networks of Stryker, one of the world's leading medical device companies, with an Iran-linked hacking group, identified as the Handala Hack Team, claiming responsibility for the breach.[2] The same group also claimed responsibility for hacking into the personal email account of FBI Director, Kash Patel.[3] The group published what it claimed to be Patel's résumé along with photographs of him on its website. The FBI confirmed that it is aware of malicious actors targeting Patel's email account, clarifying that the exposed material is historical in nature and does not include any government-related information.

Pro-Russian politically motivated hackers reportedly collaborated with Iranian hacktivist groups to target Israeli defence and municipal entities, including defence contractor Elbit Systems.[4] The same Russian-linked hacktivists also claimed to have breached an Israeli water management system and other industrial control systems. However, these assertions could not be independently verified by researchers.

Trump White House Unveils New Cybersecurity Strategy

The Trump administration has unveiled a new cybersecurity strategy that commits the United States to disrupting malicious cyber actors, safeguarding critical infrastructure, leveraging AI, and easing regulatory burdens on businesses.[5] The seven-page Cyber Strategy for America provides little detail on how the government plans to implement the six pillars of Donald Trump's broader cybersecurity agenda. At a time when nation-state actors and cybercriminals are increasingly disrupting business operations and threatening critical infrastructure, the document emphasises the need for the U.S. to impose meaningful costs on adversaries to deter attacks on American networks.

President Trump also signed an Executive Order aimed at countering cybercrime, fraud, and predatory schemes targeting American families, businesses, and critical infrastructure.[6] The Order directs relevant officials within the administration to undertake a comprehensive review of existing operational, technical, diplomatic, and regulatory tools, identifying areas for improvement in tackling transnational criminal organizations involved in cyber-enabled crime and fraudulent activities.

Puerto Rico Transport Services Hit by Cyberattack

Puerto Rico's Department of Transportation was compelled to cancel all appointments at the agency responsible for issuing driver's licences, permits, and vehicle registrations following a cyberattack.[7] Officials stated that the Puerto

Rico Innovation and Technology Service (PRITS) is working alongside the Department of Transportation to restore affected systems. The Executive Director of PRITS, also confirmed that all Transportation Department systems had to be disconnected after the cyberattack was detected.

Ransomware Attack Disrupts Operations at Spanish Port

A ransomware attack disrupted digital systems at the Port of Vigo, forcing authorities to disconnect parts of its network and temporarily switch to manual cargo operations, according to port officials.[8] The attack impacted computer servers used to manage cargo traffic and other digital services at the port, located in the Galicia region of northwest Spain. Local media reports indicated that some equipment was locked and that the incident involved a ransom demand. In response, the port authority's technology team isolated the affected systems from external networks to contain the disruption and prevent further spread.

Dutch Finance Ministry Portal Knocked Offline by Cyberattack

The Dutch Ministry of Finance announced that it had taken parts of its infrastructure offline, including its treasury banking portal, after detecting a cyberattack.[9] The incident affected a section of employees and led to the temporary shutdown of critical systems. The breach, identified following an alert from a third party, resulted in unauthorized access to internal systems within the policy department. In response, the treasury banking portal was taken offline, preventing around 1,600 public entities including ministries, agencies, educational institutions, social funds, and local governments, from accessing account balances and key services.

Taiwan targeted by LNG shortage disinformation campaign

Taiwan has been targeted by a wave of online disinformation falsely claiming that its gas supplies are on the verge of depletion due to disruptions linked to the conflict in West Asia, a narrative officials warn could trigger panic and erode public confidence in the government.[10] The misleading posts, which have garnered thousands of views on Chinese-language social media platforms, allege that Taiwan could run out of liquefied natural gas (LNG) within 11 days and face widespread power outages due to Iran restricting tanker movement through the Strait of Hormuz. Fact-checkers identified roughly two dozen posts originating from China-based accounts promoting this narrative, many of which reused the same scripted video content.

Albanian Parliament hit by major cyberattack, emails disrupted

Parliament of Albania confirmed that it had been targeted by a "sophisticated" cyberattack aimed at deleting data and compromising multiple internal systems.[11] In a statement to local media, the parliament said its core systems and official website remained operational, but confirmed that internal email services used by the parliamentary administration were temporarily suspended, disrupting both incoming and outgoing communications. Local reports indicated that parliamentary staff and lawmakers were unable to access computers and email systems for several hours following the incident. While authorities have not formally attributed the attack, a hacker group known as Homeland

Justice claimed responsibility, alleging it had obtained internal communications involving Albanian lawmakers. The group also shared screenshots of what it said were leaked documents on its Telegram channel.

India File

- A nationwide audit of CCTV networks across major cities, including Delhi and Mumbai, has uncovered serious vulnerabilities in the country's surveillance infrastructure following the busting of a spy ring by the Ghaziabad Police.[12] In response, central agencies have directed all relevant law enforcement bodies and police departments to urgently review every camera installation under their jurisdiction, marking one of the most significant security directives issued in recent years.
- According to a recent report by cybersecurity firm Kaspersky, its security systems blocked nearly 47 million online threats in India in 2025, averaging around 130,000 web-based attacks per day.[13] These threats primarily included phishing attempts, malware, malicious or suspicious websites, and various forms of online fraud. The report highlights that the rapid growth of digital payments, online banking, and internet-based services has further incentivised cybercriminal activity. Between January and December 2025, Kaspersky products detected and blocked over 47.5 million internet-based threats targeting computer and network systems across the country. During this period, approximately 24.7 percent of internet users in India were exposed to some form of online threat.
- In a major crackdown on rising cybercrime, the Delhi Police carried out a nationwide operation targeting an organised fraud network.[14] The West District Cyber Cell conducted coordinated raids across 11 states, resulting in the arrest of 27 suspects. Investigators revealed that the group was involved in multiple forms of cyber fraud, including investment scams, cheating through platforms like WhatsApp and Instagram, credit card fraud, and cyber scams involving malicious APK files.
- The Technology Development Board (TDB), under the Department of Science and Technology (DST), has extended financial support to Matisoft Cyber Security Labs Pvt. Ltd., New Delhi, for a project titled "Development of an Advanced Open-Source Framework Sanitization Tool Facilitating Secure Transfer of Data Between Multiple Air-Gapped Networks."[15] The initiative aims to develop an indigenous cybersecurity solution that enables secure and controlled data exchange across highly sensitive, air-gapped environments, particularly in the defence and critical infrastructure sectors. The proposed system focuses on creating a USB sanitization and data transfer control software tailored to meet the stringent security requirements of organisations such as the Indian Navy. It ensures that only verified and sanitized data is transferred between isolated networks, thereby reducing risks associated with malware, unauthorised access, and zero-day cyber threats.
- A total of 350 cadets from the inaugural batch of a Diploma programme in Information Technology and Cyber

Security jointly developed by SRM Institute of Science and Technology (SRMIST) and the Officers Training Academy Chennai (OTA) graduated from the academy[16]. The programme was designed to combine technological expertise with military training, with experienced faculty and technical specialists from SRMIST delivering the curriculum in close coordination with OTA authorities, according to an official statement. This one-year course covered core areas such as IT fundamentals, network security, secure systems design, cyber hygiene, and incident response, along with emerging domains including cyber warfare, artificial intelligence applications, and information assurance.

[1] The Times of Israel, "Report: Israel hacked Tehran traffic cameras to track Khamenei ahead of assassination", 3 March 2026, https://www.timesofisrael.com/report-israel-hacked-tehran-traffic-cameras-to-track-khamenei-ahead-of-assassination/

[2] Aljazeera, "Iran-linked hackers hit medical giant Stryker in retaliatory cyberattack", 11 March 2026, https://www.aljazeera.com/news/2026/3/11/iran-linked-hackers-hit-medical-giant-stryker-in-retaliatory-cyberattack

[3] BBC, "Iran-backed hackers breach FBI director Kash Patel's personal emails", 28 March 2026, https://www.bbc.com/news/articles/cvgl4yk7vgpo

[4] Axios, "Hackers join U.S. and Israel's fight with Iran", 11 March 2026, https://www.axios.com/2026/03/11/iran-war-trump-israel-ai-cyberattack

[5] Cybersecurity Drive, "Trump's new cybersecurity strategy makes promises but lacks details", 6 March 2026, https://www.cybersecuritydive.com/news/white-house-trump-cybersecurity-strategy/814120/

[6] The White House, "Fact Sheet: President Donald J. Trump Combats Cybercrime, Fraud, and Predatory Schemes Against American Citizens", 6 March 2026, https://www.whitehouse.gov/fact-sheets/2026/03/fact-sheet-president-donald-j-trump-combats-cybercrime-fraud-and-predatory-schemes-against-american-citizens/

[7] The Record, "Puerto Rico government agency cancels driver's license appointments after cyberattack", 25 March 2026, https://therecord.media/puerto-rico-gov-agency-cancels-driver-license-appointments-cyber-incident

[8] The Record, "Ransomware attack disrupts operation at major Spanish fishing port", 25 March 2026, https://therecord.media/port-of-vigo-ransomware

[9] SC Media, "Dutch Ministry of Finance portal offline after cyberattack", 31 March 2026, https://www.scworld.com/brief/dutch-ministry-of-finance-portal-offline-after-cyberattack

[10] Taipei Times, "Disinformation targets Taiwan LNG supply", 29 March 2026, https://www.taipeitimes.com/News/taiwan/archives/2026/03/29/2003854659

[11] The Record, "Iran-linked hackers claim cyberattack on Albania's parliament email systems", 11 March 2026, https://therecord.media/iran-linked-hackers-claim-cyberattack-albania-parliament

[12] News 18, "Pan-India CCTV Audit In Major Cities After Cops Bust Pakistan Spy Ring | Exclusive", 23 March 2026, https://www.news18.com/india/pan-india-cctv-audit-in-major-cities-after-cops-bust-pakistan-spy-ring-exclusive-ws-kl-9991806.html

[13] The 420, "Digital Battle Intensifies: 47 Million Cyber Attacks Targeted India, Around 130,000 Web Threats Recorded Daily", 8 March 2026, https://the420.in/india-47-million-cyber-attacks-kaspersky/

[14] The 420, "Delhi Police Launches Major Crackdown On Cyber Fraud Gang, Raids in 11 States, 27 Arrested", 1 March 2026, https://the420.in/delhi-police-27-arrested-11-states-cyber-fraud-crackdown/

[15] PIB, ""TDB-DST supports Indigenous Cybersecurity Solution for Secure Data Transfer Across Air-Gapped Networks", 23 March 2026, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2243913&reg=3&lang=1

[16] The Hindu, "350 cadets pass out with Diploma in IT and Cyber Security jointly curated by SRMIST and OTA", 3 March 2026, https://www.thehindu.com/news/national/tamil-nadu/350-cadets-pass-out-with-diploma-in-it-and-cyber-security-jointly-curated-by-srmist-and-ota/article70699909.ece