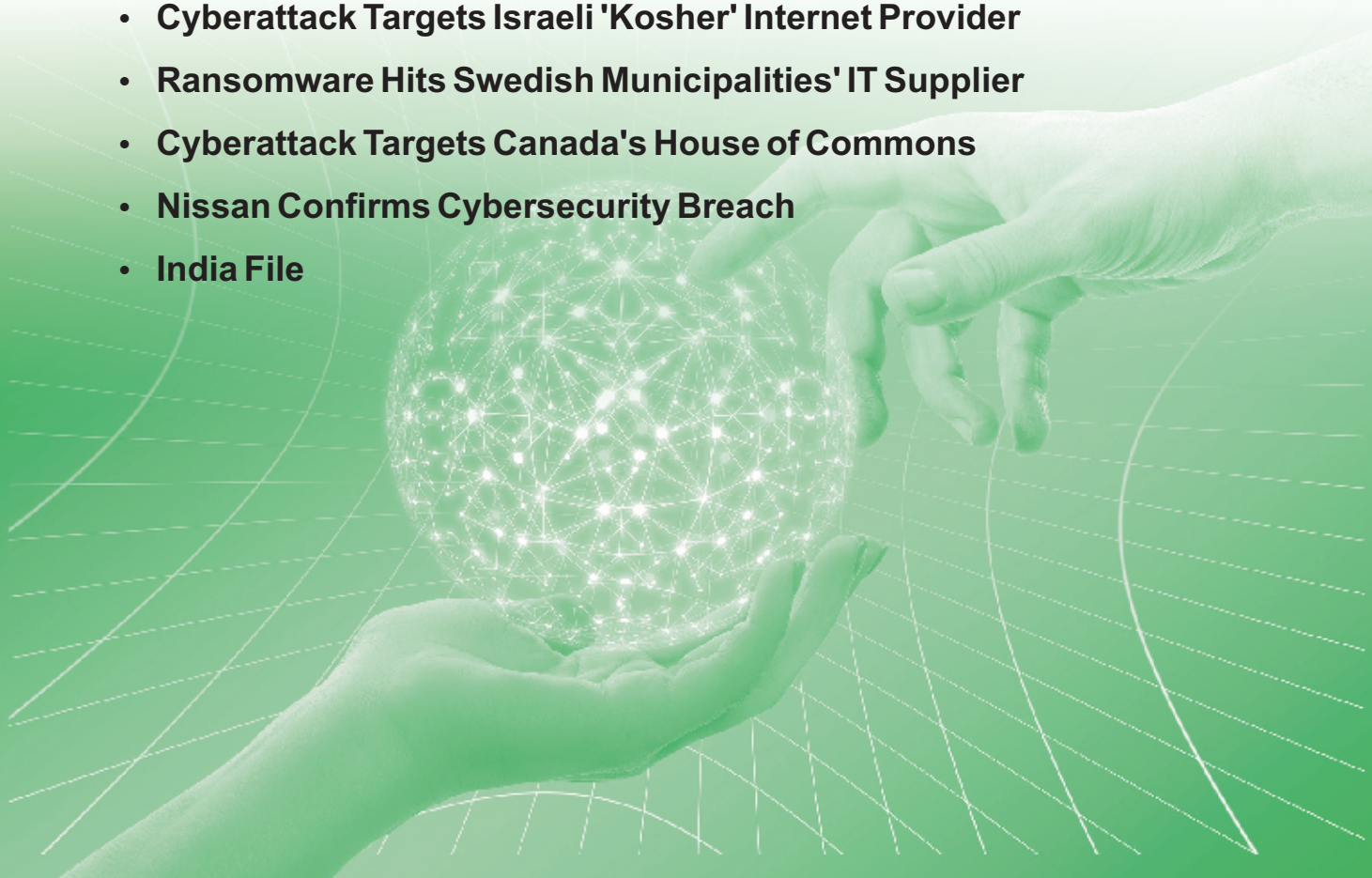
MANOHAR PARRIKAR INSTITUTE FOR DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

CYBER *Digest*

September 2025

- India Unveils Joint Cyber, Multi-Domain operations Doctrines
- Reports Flag Bangladesh's Emerging Digital Police State
- Ransomware Attack Hits Pakistan Petroleum Limited
- Cyberattack Targets Israeli 'Kosher' Internet Provider
- Ransomware Hits Swedish Municipalities' IT Supplier
- Cyberattack Targets Canada's House of Commons
- Nissan Confirms Cybersecurity Breach
- India File



India Unveils Joint Cyber, Multi-Domain operations Doctrines

Chief of Defence Staff General Anil Chauhan and the Secretary of the Department of Military Affairs unveiled the declassified Joint Doctrine for Cyberspace Operations during the Chiefs of Staff Committee meeting in New Delhi.[1] The move highlights India's resolve to strengthen transparency, accessibility, and the wider dissemination of joint warfighting concepts. The doctrine sets a unified framework for safeguarding national cyberspace interests by integrating offensive and defensive capabilities, ensuring synchronised operations across the three Services. It underscores threat-based planning, resilience, real-time intelligence fusion, and robust joint cyber capabilities development.

Subsequently, the government released the Joint Doctrine for Multi-Domain Operations.[2] The doctrine outlines the roadmap for the integrated and synergized employment of the Armed Forces across land, sea, air, space, cyber, and cognitive domains, thereby reinforcing jointness and enhancing future readiness. It has been issued to ensure greater accessibility and wider dissemination.

Report Flags Bangladesh's Emerging Digital Police State

A recently released report examines the evolution, structure, and implications of Bangladesh's surveillance apparatus, revealing a system that has expanded over the past decade with minimal transparency, oversight, or accountability.[3] A key finding is that between 2015 and 2025, at least 160 surveillance tools and spyware systems were imported or deployed in Bangladesh, often through opaque procurement processes and third-country intermediaries.

During this period, Bangladesh is estimated to have spent nearly USD 190 million on surveillance and spyware, including over USD 40 million on Israeli-origin technologies, many of which are widely used in authoritarian regimes. Notably, purchases surged ahead of, or immediately following, the national elections of 2018 and 2024, suggesting these systems were likely employed to suppress political dissent and ensure regime continuity.

Ransomware Attack Hits Pakistan Petroleum Limited

Pakistan Petroleum Limited (PPL), an oil and gas exploration firm, reported a ransomware attack affecting parts of its IT infrastructure.[4] The company stated that the incident was swiftly contained, with no compromise of critical systems or sensitive data. The attack was detected on 6 August 2025, prompting the immediate activation of PPL's internal cybersecurity protocols. It was also reported that working alongside external experts, the IT and cybersecurity teams implemented effective containment measures, including the temporary suspension of selected noncritical IT services as a precaution to limit potential impact and safeguard system integrity.

Cyberattack Targets Israeli 'Kosher' Internet Provider

It was reported that Iranian hackers, operating under the name "Promised Revenge," breached the Rimon Internet Provider, a company that offers internet filtering services for the religious and Haredi communities.[5] The incident came to light after numerous customers experienced severe service disruptions, including partial

or complete loss of connectivity. At the same time, the hackers released a video claiming to have breached Rimon's systems in real time, disabling servers and erasing internal infrastructure. While no evidence of data theft has yet been provided, the group asserts that it gained access to sensitive information from the company's internal network.

Ransomware Hits Swedish Municipalities' IT Supplier

A suspected ransomware attack on Miljödata, a Swedish software provider, is believed to have affected around 200 municipal governments across the country. According to reports, the attackers are attempting to extort the company.[6] Officials have confirmed that the full scope of the incident remains unclear, and it is still too early to assess the actual consequences. Reports indicate that Miljödata is working intensively with external experts to investigate the incident, determine the extent of the impact and those affected, and restore system functionality.

Cyberattack Targets Canada's House of Commons

The House of Commons and Canada's cybersecurity agency were investigating a major data breach in which an unknown threat actor accessed employee information.[7] Reports indicate the attacker exploited a recent Microsoft vulnerability to gain unauthorized access to a database for managing computers and mobile devices. Canada's Communications Security Establishment (CSE) confirmed it assists the House of Commons in responding to the incident but has not attributed the attack to any specific actor. The Canadian Centre for Cyber Security's latest national threat assessment identifies Canada as a "valuable target" for cybercriminals and state adversaries seeking to disrupt critical systems.

Nissan Confirms Cybersecurity Breach

The Nissan Creative Box (Nissan CBI) design studio has appeared on a cybercriminal gang's victim blog, with the hackers claiming to have exfiltrated 405,882 files, approximately 4TB of data.[8] The stolen material reportedly includes 3D design data, reports, photos, videos, and other documents related to Nissan automobiles.

Nissan Japan has confirmed the breach to the media. On 16 August 2025, suspicious access was detected on Creative Box Inc.'s data server. The subsidiary, which provides design services for Nissan, immediately implemented emergency measures, including blocking all server access, and reported the incident to police. Nissan has since launched a full investigation. Reports suggest the breach raises serious concerns over the exposure of proprietary innovation.

India File

- The Indian government has appointed IPS officer Navin Kumar Singh as the country's fourth National Cybersecurity Coordinator, a key position overseeing India's cybersecurity strategy and posture.[9] He succeeds Lt. Gen. M.U. Nair, who completed his tenure, and replaces interim coordinator Narendra Nath Gangavarapu. Singh, who earlier served as Director General of the National Critical Information Infrastructure Protection Centre (NCIIPC), is the first IPS officer to be elevated to the role of National Cybersecurity Coordinator.

- The West Bengal Police have launched a high-level probe after the state's cybercrime investigation data centre was reportedly compromised, raising nationwide concerns over data integrity, internal sabotage, and vendor accountability in critical law enforcement infrastructure.[10] The Cyber Crime Wing (CCW) discovered that its confidential state-run data centre, vital to ongoing cybercrime investigations, had been breached, resulting in a complete system disruption. The incident triggered alarm among cybersecurity officials and prompted the initiation of a criminal investigation.

- Police announced the arrest of 18 individuals accused of defrauding credit card holders across India, excluding Delhi, of nearly ₹2.6 crore.[11] The arrests followed a six-month investigation, during which authorities uncovered that the syndicate obtained confidential customer data through insiders at a Gurugram-based call centre. The accused posed as bank executives to trick victims into revealing sensitive details such as OTPs and CVVs. According to DCP (IFSO) Vinit Kumar, the group used the stolen credentials to purchase high-value electronic gift cards from online platforms, which were later sold to travel agents.

- Following a successful joint operation, the United States expressed gratitude to the CBI for its partnership and support in dismantling a cybercrime syndicate that had defrauded American citizens of more than ₹350 crore since 2023.[12] In a message posted on social media, the U.S. Embassy described it as "a big week for U.S.-India law enforcement collaboration," noting that India's CBI, working closely with the U.S. FBI, had taken down a transnational cybercrime network that cheated U.S. nationals of nearly USD 40 million through tech-support scams and apprehended key figures behind the fraud.

- The Telangana Cyber Security Bureau (TGCSB) arrested 228 people, including 27 women, for cybercrime offences between January 1 and July 31 this year.[13] The arrests were carried out through its seven cybercrime police stations across Telangana and in other states such as Andhra Pradesh, Gujarat, Maharashtra, Karnataka, Uttar Pradesh, West Bengal, and Jharkhand. According to TGCSB Director Shikha Goel, the arrested are linked to 1,313 cybercrime cases across India, including 189 in Telangana, involving fraud amounting to Rs. 92 crore.

- The Kolkata bench of the National Company Law Tribunal (NCLT) experienced a cybersecurity breach during an online hearing when an unidentified individual shared inappropriate content on screen. The unauthorized activity, which lasted three to four minutes, disrupted proceedings led by the tribunal members. The disruption was resolved after the hybrid court operator temporarily ended the session and later resumed the proceedings.

[1] Press Information Bureau (PIB), "CDS formally releases declassified versions of Joint Doctrines for Cyberspace Operations & Amphibious Operations", https://www.pib.gov.in/PressReleasePage.aspx?PRID=2153626, 7 August 2025

[2] Press Information Bureau, "Mastering existing tech & staying ready for new innovations & unforeseen challenges is key to effectively tackle complexities of modern-day warfare: Raksha Mantri at RAN SAMWAD", 27 August 2025, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2161131

[3] Techglobal Institute, "The Digital Police State: Surveillance, Secrecy and State Power in Bangladesh", August 2025, https://techglobalinstitute.com/research/the-digital-police-state.

[4] Daily Times, "Ransomware attack on PPL contained, no critical systems affected", 9 August 2025, https://dailytimes.com.pk/1350678/ransomware-attack-on-ppl-contained-no-critical-systems-affected/

[5] Israel National News, "Cyberattack on Israeli 'kosher' internet provider", 24 August 2025, https://www.israelnationalnews.com/news/413768

[6] The Record, "Hundreds of Swedish municipalities impacted by suspected ransomware attack on IT supplier", https://therecord.media/sweden-municipalities-ransomware-software , 27 August 2025

[7] CBC, "House of Commons hit by cyberattack from 'threat actor': internal email", 14 August 2025, https://www.cbc.ca/news/politics/house-of-commons-data-breach-1.7608061

[8] Cybernews, "Nissan confirms data breach", 27 August 2025, https://cybernews.com/news/nissan-ransomware-attack-creative-box-creative-box-radesign-studio-qilin-group/

[9] Bankinfosecurity, "NCIIPC Director Named India's National Cyber Coordinator", 4 August 2025, https://www.bankinfosecurity.asia/nciipc-director-named-indias-national-cyber-coordinator-a-29121

[10] The 420, "WB Cyber Crime Wing Hacked: Ransom Demanded for Data Decryption!", 3 August 2025, https://the420.in/bengal-cyber-crime-data-centre-breach-ransomware-sabotage-investigation/

[11] The New Indian Express, "18 held for duping credit card holders of Rs 2.60 crore; data theft from call centre", 17 August 2025, https://www.newindianexpress.com/cities/delhi/2025/Aug/17/18-held-for-duping-credit-card-holders-of-rs-260-crore-data-theft-from-call-centre

[12] NDTV, "US Thanks CBI For Busting Illegal Call Centre That Duped Its Citizens Of Millions", 27 August 2025, https://www.ndtv.com/india-news/cbi-thanked-by-us-on-busting-illegal-call-centre-that-duped-its-citizens-of-millions-9170463

[13] The Hindu, "228 cyber criminals arrested across India by Telangana Cyber Security Bureau", 3 August 2025, https://www.thehindu.com/news/national/telangana/228-cyber-criminals-arrested-across-india-by-telangana-cyber-security-bureau/article69889843.ece