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

CYBER *Digest*

July 2025

- **Cyber Warfare Escalates Amid Israel-Iran Conflict**
- **US House Bans WhatsApp on Official Devices**
- **Sweden Probes Coordinated Telecom Cyberattacks**
- **Scattered Spider targets aviation sector**
- **Swiss Government Impacted by Radix Cyber Breach**
- **Hackers Exploit Malaysian Minister's WhatsApp for Scam**
- **INTERPOL Cracks Down on Global Infostealer Network**
- **India File**

Cyber Warfare Escalates Amid Israel-Iran Conflict

Shortly after news of the military operation broke, Iran-aligned threat actors ramped up activity on their public and private Telegram channels.[1] The Cyber Bulletin channel received a message from an actor under the alias #OpIsrael, claiming attacks on Israel's Tzofar public alert system, which warns civilians of missile threats. Meanwhile, groups like Mysterious Team Bangladesh warned Jordan and Saudi Arabia of potential cyberattacks on their national infrastructure if they support Israel. On the other side, pro-Israel hacking group Predatory Sparrow, reportedly linked to Israel, claimed a cyberattack on an Iranian bank in retaliation for its alleged role in funding Iran's military and nuclear programs.[2]

Iran's state-owned TV broadcaster was also hacked overnight, disrupting regular programming to air videos urging street protests against the Iranian government, according to multiple reports.[3] The identity of the attackers remains unknown, though Iranian authorities have accused Israel of being behind the incident. Reports also indicate that Iran has been tapping into private security cameras in Israel to gather real-time intelligence, highlighting a recurring vulnerability in such devices that has surfaced in other global conflicts as well.[4]

US House Bans WhatsApp on Official Devices

WhatsApp has been banned from all U.S. House of Representatives devices, according to a memo issued to House staff.[5] The Office of Cybersecurity flagged the app as a high-risk platform, citing concerns over its lack of transparency in data protection, absence of stored data encryption, and potential security vulnerabilities. The memo, issued by the Chief Administrative Officer, advised staff to switch to more secure messaging alternatives. The House Chief Administrative Officer (CAO) said that Microsoft Teams, Wickr, Signal, iMessage and FaceTime are all acceptable alternatives to WhatsApp.[6] Congress is also taking steps to limit the use of AI programs, including Microsoft Copilot and Deepseek. Use of ChatGPT has been limited to the paid version.

Sweden Probes Coordinated Telecom Cyberattacks

Swedish Prime Minister Ulf Kristersson confirmed a wave of cyberattacks targeting public broadcaster SVT and other critical institutions.[7] Addressing parliament, he said Sweden is facing intense cyberattacks, affecting SVT, banks, and the Bank-ID system. The incidents, identified as Distributed Denial-of-Service (DDoS) attacks, have sparked concerns over the robustness of the country's digital infrastructure. Cybersecurity experts have cautioned that such breaches could escalate further, threatening not only digital services but also eroding public trust.

Scattered Spider targets aviation sector

Hawaiian Airlines has reported a cybersecurity incident amid fresh warnings from the FBI and cybersecurity firms about the Scattered Spider group targeting the aviation sector.[8] The FBI noted that the group has expanded its focus to airlines and urged industry players to report any signs of intrusion. Hawaiian Airlines confirmed the breach affected certain IT systems and stated that precautionary measures were taken to protect operations. The airline is still assessing whether the incident will have a significant impact.

Swiss Government Impacted by Radix Cyber Breach

Switzerland has confirmed that a cyberattack on the non-profit health foundation Radix, which involved data theft and encryption, also impacted the federal administration.[9] Authorities stated that several federal offices are among Radix's clients and that some of the stolen data has been leaked on the dark web, though specific details were not disclosed. Authorities are working to identify the specific units and data impacted by the attack, the statement noted, while clarifying that the attackers did not gain direct access to state-run data systems.

Hackers Exploit Malaysian Minister's WhatsApp for Scam

Malaysia's Home Minister, Datuk Seri Saifuddin Nasution Ismail, had his WhatsApp account hacked and used to send malicious links to his contacts, police confirmed.[10] The attacker reportedly used a VPN to carry out the breach, though officials did not disclose the exact method of the hack. So far, no financial losses have been reported. The Ministry of Home Affairs confirmed the incident and warned the public not to respond to messages or calls claiming to be from the minister, especially those requesting personal or financial information. An investigation is underway to trace the hacker's location.

INTERPOL Cracks Down on Global Infostealer Network

More than 20,000 malicious IP addresses and domains linked to information-stealing malware were dismantled in Operation Secure, a global cybercrime crackdown coordinated by INTERPOL. Law enforcement agencies from 26 countries—primarily in Asia—collaborated to trace servers, map networks, and execute targeted takedowns. INTERPOL partnered with private-sector cybersecurity firms, including Singapore-based Group-IB, to generate cyber activity reports and share key intelligence with regional cyber units. [11]

The operation, conducted from January to April, led to the arrest of 32 individuals, including 18 suspects in Vietnam. Vietnamese authorities seized computers, SIM cards, cash, and corporate documents tied to schemes involving the creation and sale of fraudulent business accounts for criminal use. Authorities also dismantled 41 servers and confiscated over 100 GB of stolen data across multiple info-stealer variants, such as Lumma, Risepro, and Meta.

Hong Kong police identified 117 command-and-control servers hosted across 89 internet service providers. These servers were allegedly used for phishing campaigns, credential theft, and social media scams. More than 216,000 potential victims were notified and advised to change passwords or freeze compromised accounts. While the takedown disrupted infrastructure such as Lumma, much of its Russia-hosted backend remains operational.

India File

- Amid rising cyber threats from China and Pakistan, the Indian Armed Forces launched a 12-day, multi-phase cybersecurity exercise from June 16-27 to strengthen national cyber resilience.[12] Organized by the tri-Service Defence Cyber Agency (DCA), the 'Cyber Suraksha' exercise involved over 100 participants from key national agencies and the defence sector. The program included focused training sessions, performance evaluations, and a dedicated leadership module for Chief Information Security Officers (CISOs).

- India's Central Bureau of Investigation (CBI) has arrested a Delhi resident and seized cryptocurrency worth over $327,000 (Rs. 2.8 crore) after dismantling a transnational cybercrime network targeting victims in the U.S. and Canada.[13] The arrest followed coordinated raids at three locations across India, where investigators uncovered advanced tools used to impersonate government officials and tech support agents in order to defraud individuals abroad.

- Indian car-sharing platform Zoomcar has disclosed a data breach affecting at least 8.4 million customers, compromising personal details such as names, phone numbers, and car registration numbers.[14] In a filing with the U.S. Securities and Exchange Commission, the Bengaluru-based company confirmed unauthorized access to its systems. Zoomcar said it became aware of the breach after employees received messages from a threat actor claiming to have accessed company data.

- Indian grocery delivery startup KiranaPro has suffered a major cyberattack, resulting in the complete wipeout of its data, the company's founder confirmed to media.[15] The breach destroyed critical assets, including app code and servers holding sensitive customer information such as names, addresses, and payment details. While the app remains online, it is currently unable to process orders.

- The Supreme Court has upheld the Tamil Nadu governments' use of preventive detention laws against cybercriminals, emphasising the urgent need for stronger and swifter legal mechanisms to tackle the rising wave of online financial fraud.[16] With cybercrime surging across India, the Court noted that conventional processes, like the FIR investigation trial route, are often too slow, allowing offenders to escape or reoffend. It called for modern, proactive tools to effectively counter these evolving digital threats.

[1] Radware, Heightened Cyberthreat Amidst Israel-Iran Conflict, 13 June 2025 https://www.radware.com/security/threat-advisories-and-attack-reports/heightened-cyberthreat-amidst-israel-iran-conflict/.

[2] The Record, Pro-Israel hackers claim breach of Iranian bank amid military escalation, 17 June 2025.https://therecord.media/pro-israel-hackers-claim-attack-on-iranian-bank

[3] The Hacker News, Iran's State TV Hijacked Mid-Broadcast Amid Geopolitical Tensions; $90M Stolen in Crypto Heist, 20 June 2025, https://thehackernews.com/2025/06/irans-state-tv-hijacked-mid-broadcast.html

[4] Hindustan Times, Iranian hackers hijacking home security cameras to spy within Israel, 20 June 2025, https://www.hindustantimes.com/world-news/iranian-hackers-hijacking-home-security-cameras-to-spy-within-israel-101750396147899.html

[5] Reuters, WhatsApp banned on US House of Representatives devices, memo shows, 24 June 2025, https://www.reuters.com/world/us/whatsapp-banned-us-house-representatives-devices-memo-2025-06-23/

[6] Axios, Scoop: WhatsApp banned on House staffers' devicesScoop: WhatsApp banned on House staffers' devices 23 June 2025, https://www.axios.com/2025/06/23/whatsapp-house-congress-staffers-messaging-app

[7] Euractiv, Sweden under cyberattack: Prime minister sounds the alarm, 11 June 2025 https://www.euractiv.com/section/tech/news/sweden-under-cyberattack-prime-minister-sounds-the-alarm/,

[8] Security Week, Hawaiian Airlines Hacked as Aviation Sector Warned of Scattered Spider Attacks, 30 June 2025, https://www.securityweek.com/hawaiian-airlines-hacked-as-aviation-sector-warned-of-scattered-spider-attacks/

[9] Reuters, Swiss government says it was affected by cyberattack on health foundation, 30 June 2025 https://www.reuters.com/business/media-telecom/swiss-government-says-it-was-affected-by-cyberattack-health-foundation-2025-06-30/

[10] The Record, Malaysian home minister’s WhatsApp hacked, used to scam contacts, 2 June 2025, https://therecord.media/malaysia-hack-scam-whatsapp-minister

[11] INTERPOL, 20,000 malicious IPs and domains taken down in INTERPOL infostealer crackdown, 11 June 2025, https://www.interpol.int/en/News-and-Events/News/2025/20-000-malicious-IPs-and-domains-taken-down-in-INTERPOL-infostealer-crackdown.

[12] The Times of India, 'Cyber Suraksha': Armed forces launch cybersecurity drill, 17 June 2025, https://timesofindia.indiatimes.com/india/armed-forces-launch-cybersecurity-drill/articleshow/121895517.cms.

[13] Decrypt, India CBI Busts Transnational Cybercrime Ring, Seizes $327K in Crypto, 11 June 2025, https://decrypt.co/324588/india-cbi-transnational-cybercrime-seizes-327k-crypto

[14] TechCrunch, Car-sharing giant Zoomcar says hacker accessed personal data of 8.4 million users,16 June 2025, https://techcrunch.com/2025/06/16/car-sharing-giant-zoomcar-says-hacker-accessed-personal-data-of-8-4-million-users/

[15] TechCrunch, Indian grocery startup KiranaPro was hacked and its servers deleted, CEO confirms, 3 June 2025, https://techcrunch.com/2025/06/03/indian-grocery-startup-kiranapro-was-hacked-and-its-servers-deleted-ceo-confirms/

[16] The 420, Detaining Hackers Before the Crime? Supreme Court Approves Preventive Custody for Cyber Offenders, 26 June 2025, https://the420.in/supreme-court-approves-preventive-detention-cybercriminals-tamil-nadu-crackdown-digital-fraud-under-goonda-act