DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

CYBER THREAT ADVISORY

ESCALATING CYBER RISKS DUE TO THE ONGOING MIDDLE EAST CONFLICT

IMPLICATIONS FOR THE INDIAN INDUSTRY

MARCH 2026

Critical Update: February 2026 Escalation

Cyber Dimension of the February 2026 Conflict

Parallel to the kinetic campaign, Israel launched what has been described as the largest cyberattack in history against Iran, contributing to a near-total internet blackout. Iran's connectivity dropped to approximately 4% of normal levels, severely disrupting government services, state media (IRNA, Tasnim), and security communications. Critical infrastructure and local applications across Tehran, Isfahan, and Shiraz experienced widespread outages.

Multiple Iranian state-aligned cyber entities have initiated retaliatory operations. The 'Electronic Operations Room,' established on 28 February 2026, coordinates attacks by groups including Handala Hack (linked to MOIS), APT Iran and DieNet. These actors have claimed attacks on Israeli energy companies, Jordan's fuel systems, airports in Bahrain and Sharjah, Saudi bank websites and UAE airport infrastructure along with AWS infrastructure.

Key Threat Actors

Threat Actor	Attribution	Tactics & Targets
APT36 (Transparent Tribe)	Pakistan linked	Evolved from Poseidon to Ares RAT; spear-phishing with weaponized .xlam, .ppam, .lnk files; targeted Government Sector
SideCopy	Pakistan-aligned	MSI installers, sideloaded DLLs, open-source RATs targeting defence and critical sectors
RipperSec	Pro-Pakistan hacktivist	30%+ of all DDoS claims against India; deployed MegaMedusa DDoS tool enabling low-skilled participants
AnonSec	Hacktivist collective	20+ critical websites in May 2025: defence, finance, aviation, urban development, state portals
35+ hacktivist groups	Pakistan, Turkey, Bangladesh, Indonesia, Morocco	Coordinated #OpIndia campaign; Mostly DDoS attacks were done.

Evolving Middle East Threat Landscape (2023-2026)

The Middle East cyber conflict has escalated through three distinct phases: the Israel-Hamas war (Oct 2023-ongoing), the 12-day Iran-Israel conflict (June 2025), and now the US-Israel strikes on Iran (February 2026). Each phase has expanded the geographic scope, actor sophistication, and spillover risk to India.

State-Sponsored Operations

Iranian state-sponsored cyber capabilities have been deployed as a core asymmetric pillar since the Stuxnet era. Groups like APT33 (Elfin), APT34 (OilRig), MuddyWater, and CyberAv3ngers wage sustained campaigns against Gulf energy, aerospace, defense, and government targets.

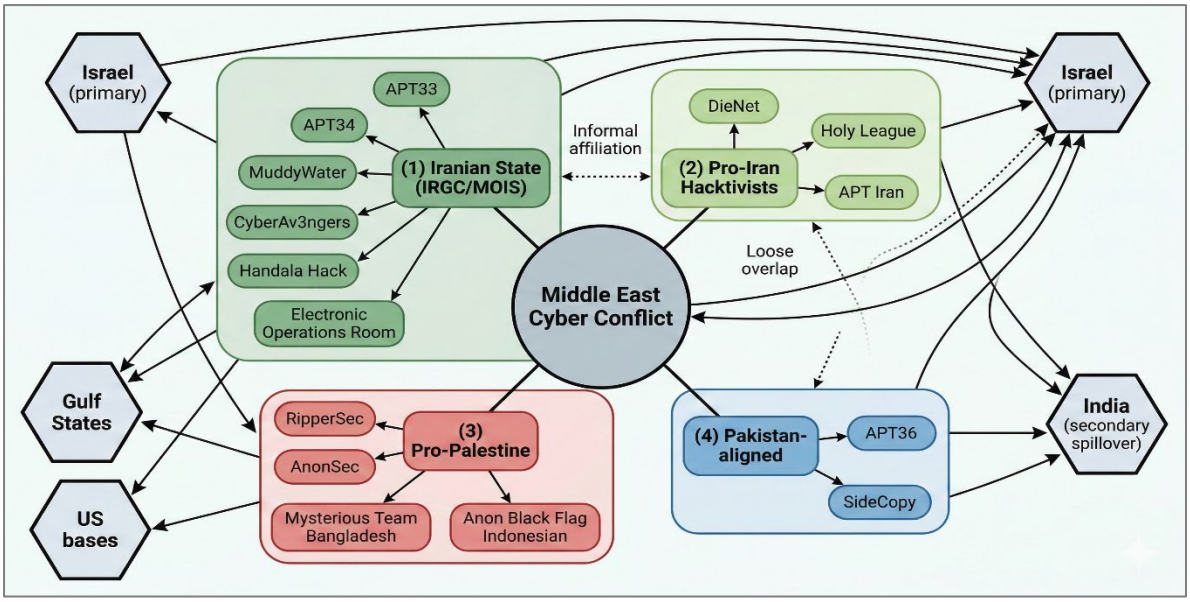
Iran's cyber operations expanded approximately 700% following the mid-2025 Iran-Israel conflict, and the February 2026 escalation is expected to dramatically amplify this trajectory.

The February 2026 conflict has introduced unprecedented elements: Israel's cyber campaign caused Iran's internet to drop to approximately 4% capacity, while Iran's Electronic Operations Room coordinates retaliatory operations against Israel, Gulf states, and their economic partners. CloudSEK's situation report identifies India as a second order affected country facing elevated risk from espionage, supply-chain compromise, DDoS, ransomware, and disinformation.

Hacktivist Alliances: From Ideology to Operational Coordination

Hacktivist collectives have evolved from loosely organized ideological groups to operationally coordinated networks with sophisticated tooling. Key alliances active in the current escalation include:

- **Handala Hack:** Linked to Iran's MOIS, blending data exfiltration with operations against Israeli political/defence establishments. Now targeting Jordan fuel systems and Gulf infrastructure.
- **DieNet:** Pro-Iran group conducting DDoS attacks on airports (Bahrain, Sharjah), banking (Riyadh Bank, Bank of Jordan), and Gulf airports.
- **Holy League / RipperSec / AnonSec:** Cross-border hacktivist coalitions that were active in both the Israel-Hamas conflict and the recent attack in May 2025, demonstrating willingness to target India specifically.
- **Mysterious Team Bangladesh / Anon Black Flag Indonesian:** Over 150 pro-Palestinian hacktivist groups that targeted Indian critical infrastructure during 2023-2024, with 4,000+ attacks recorded.



Why is the Indian Industry at Elevated Risk

Energy Supply Chain: The Hormuz Chokepoint

India's energy exposure has reached crisis levels. India imports approximately 90% of its crude oil, over 66% of LPG, and more than 50% of LNG. Nearly 50% of crude and 54% of LNG imports transit the Strait of Hormuz. After US pressure restricted Russian oil purchases in late 2025, India pivoted more heavily toward Gulf suppliers, **increasing Hormuz-linked exposure from 40% (Nov-Dec 2025) to 50% (Jan-Feb 2026).** India's combined strategic and commercial reserves cover only 25-30 days, well below the IAEA benchmark of 90 days.

A cyberattack on Gulf energy infrastructure, port operations, or tanker navigation systems could compound physical supply disruptions. The CyberAv3ngers group (IRGC-linked) has already demonstrated the capability to target water and energy systems globally and Infrastructure Destruction Squad in India. SCADA/ICS vulnerabilities in maritime automation and energy distribution are prime targets.

IT/ITeS Global Delivery Exposure

India's IT services industry delivers to clients across the Gulf, Israel, and globally. Any breach in one Indian IT provider can cascade internationally. The 2025 Marks & Spencer breach demonstrated how a single compromised vendor relationship can cause massive losses. India's IT hubs face elevated risk during geopolitical crises as threat actors probe supply chains connecting Indian service providers to Middle Eastern and Western clients.

BFSI Sector: Trust as Target

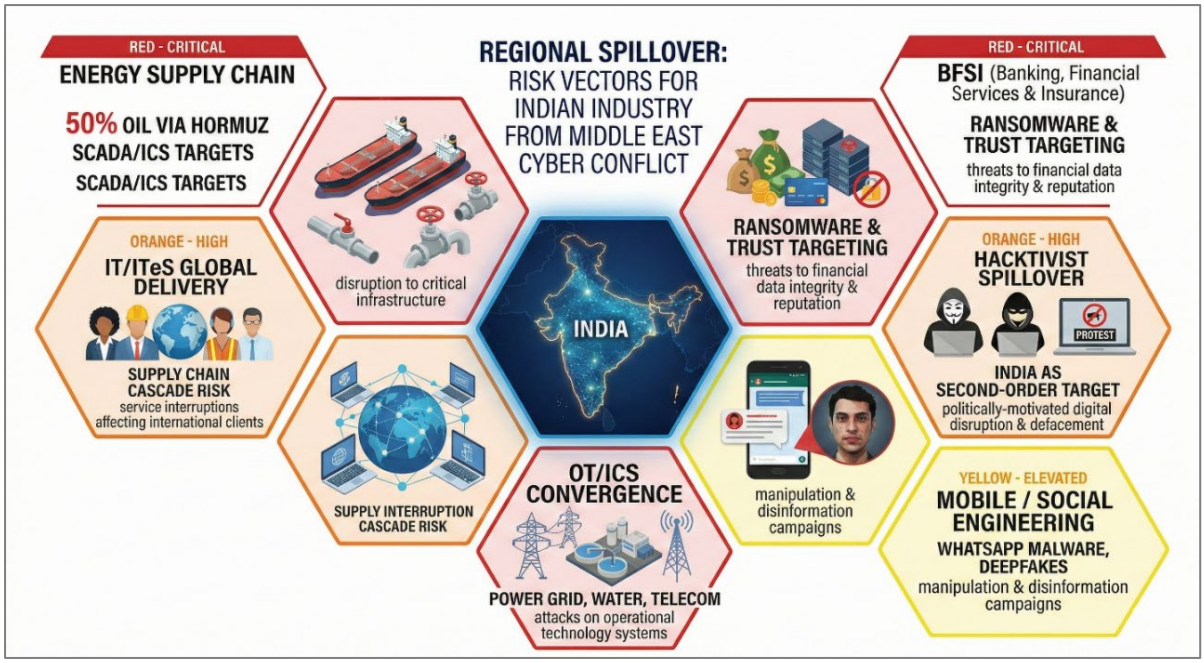
CERT-In's Advisory CIAD-2025-0019 specifically warned financial institutions of elevated cyber risks in the month of May 2025. The same dynamic applies now with even greater urgency. Ransomware groups like RansomHub, LockBit 3.0, and RansomEXX are actively targeting Indian financial infrastructure. A recent misconfigured Jenkins server at a tech vendor led to a massive RansomEXX attack that severely disrupted India's banking ecosystem, demonstrating that institutions are only as secure as their weakest third-party vendor.

Hacktivist Targeting of India

India's diplomatic positioning makes it a recurring target. Over 150 pro-Palestinian hacktivist groups have previously targeted Indian infrastructure. In May 2025, Pakistan-aligned groups coordinated with actors from Turkey, Bangladesh, Indonesia, and Morocco. **In the current Iran crisis, India is explicitly identified as a 'second-order affected country'** by CloudSEK's situation report, facing elevated risk from espionage, supply-chain compromise, DDoS, ransomware, and disinformation.

WhatsApp & Mobile Attack Vectors

Cybercriminals are weaponizing trust through WhatsApp, deploying 'RewardSteal' APK malware disguised as urgent government notifications. Fake traffic violation alerts, electricity board notices, and gas company warnings are used to harvest credentials and deploy malware. With heightened public anxiety during the current crisis, social engineering attacks themed around energy prices, government alerts, and national security are extremely likely.



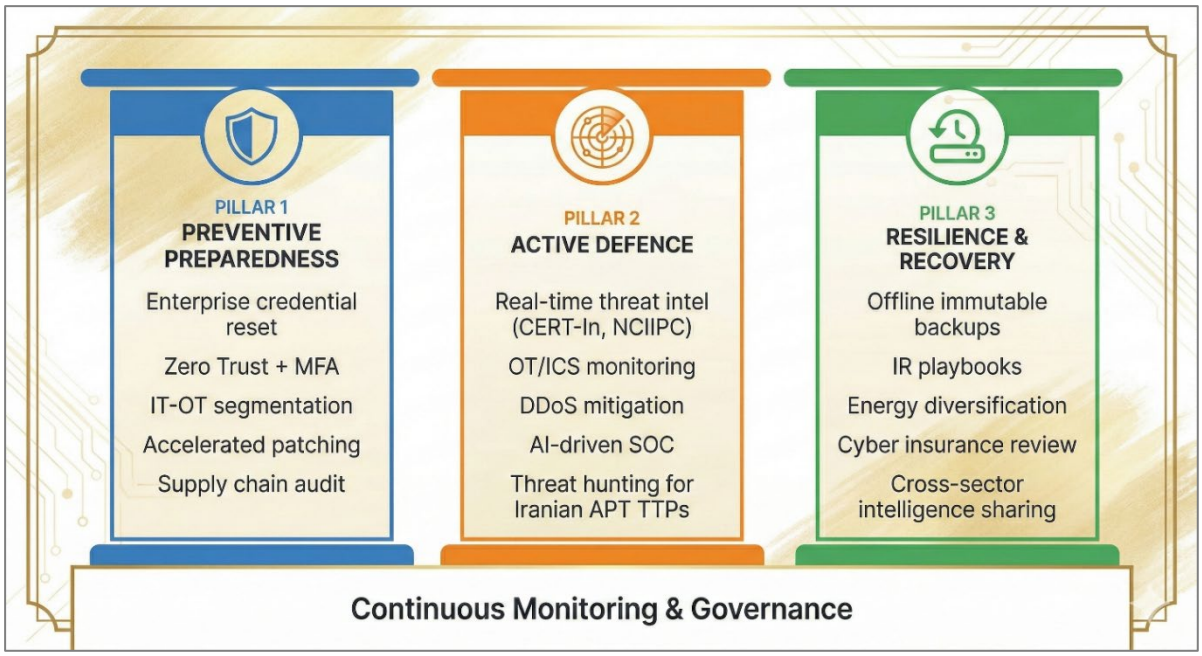
Vulnerability Exploitation: Priority Patching Matrix

Iranian APT groups and affiliated hacktivists exploit known vulnerabilities rapidly. Cyble documented attackers using newly disclosed CVEs within days of public release. The following table lists high-priority vulnerabilities actively exploited in the current threat landscape:

CVE / Vulnerability	Affected Product	Exploitation Context
CVE-2018-13379	Fortinet FortiGate VPN	APT33 and APT34 continue to exploit for initial access to energy sector networks
CVE-2021-26855 (ProxyLogon)	Microsoft Exchange Server	MuddyWater campaigns for email exfiltration and lateral movement
CVE-2024-4577	PHP-CGI (Windows)	Exploited within days of disclosure; enables remote code execution on web servers
CVE-2024-5910	Palo Alto Expedition	Credential theft and firewall policy exfiltration targeting network security infrastructure
CVE-2023-48795 (Terrapin)	SSH Protocol	Prefix truncation enabling MITM against encrypted SSH sessions; widespread exposure
AiTM / Token Theft	Cloud Identity Platforms (M365, Entra ID)	Adversary-in-the-Middle attacks highlighted as major threat in Gulf region; bypasses MFA
VPN / Edge Device Backdoors	Multiple vendors (Fortinet, Pulse, Citrix, F5)	CloudSEK Feb 2026 advisory: audit VPN appliances for backdoors, unknown accounts, and unauthorized config changes

Strategic Recommendations: Three-Pillar Framework

The following framework integrates lessons from recent cyber-attacks into actionable guidance for the Indian industry.



Pillar 1: Preventive Preparedness

IMMEDIATE ACTION: Enterprise-Wide Credential Reset

CloudSEK's 2 March 2026 advisory recommends organization-wide credential rotation as the first defensive action. This prepares organizations against hacktivist and low-to-moderate-level threat actors that rely on credential-based compromise. Check dark web marketplaces for leaked credentials associated with your organization.

- **Geopolitical risk as cyber risk:** Formally integrate Middle East conflict monitoring into SOC/SIEM alert prioritization. Establish threat escalation criteria linked to geopolitical developments.
- **Zero Trust + conditional MFA:** Enforce multi-factor authentication on all external access paths (VPN, RDP, SSH, cloud admin). Implement conditional access and session controls to mitigate Adversary-in-the-Middle and token-theft attacks.
- **IT-OT segmentation:** Air-gap or strictly segment OT/ICS networks from corporate IT. Indian power grid, water utilities, and manufacturing must harden SCADA interfaces. Deploy industrial DMZs and unidirectional security gateways.
- **Accelerated patching regime:** Prioritize the vulnerability matrix in Section 7. Iranian APTs exploit known CVEs within days of disclosure. Implement 24-48 hours patching for internet-facing appliances (VPN, firewalls, exchange servers).

- **Supply chain security audit:** Assess all third-party vendors with Middle Eastern exposure. The Jenkins/RansomEXX banking incident and M&S breach demonstrate that one compromised vendor can cascade into sector-wide disruption.
- **Employee awareness - crisis-themed:** Conduct immediate training on social engineering attacks themed around the Iran conflict, oil prices, government alerts, and national security. WhatsApp malware and deepfake attacks will increase.

Pillar 2: Active Defence

- **Align with government advisories:** Track CERT-In, NCIIPC alerts in real-time. Integrate IOCs and TTP updates from Palo Alto Unit 42, CrowdStrike, and CloudSEK into detection engineering. CERT-In handled 29.44 lakh incidents, issued 1,530 alerts, 390 vulnerability notes, and 65 advisories in 2025.
- **Hunt for Iranian APT TTPs:** Deploy threat hunts focused on VPN logs, identity infrastructure, and edge devices. Look for Cobalt Strike beacons, web shells, PowerShell abuse, credential dumping, and anomalous DNS/HTTP patterns consistent with Iranian tradecraft.
- **DDoS mitigation at scale:** Engage ISPs and cloud providers for surge-capable DDoS scrubbing. In May 2025, India saw 7 DDoS attacks per hour at peak; the current conflict involves actors with proven capability against major Gulf infrastructure.
- **AI-driven security operations:** Deploy AI-augmented SOC capabilities. The WEF warns that defending against AI-driven threats requires AI-driven defence. Behaviour-based detection is critical as signature-based approaches fail against polymorphic malware and LOLBins.
- **Geographic traffic filtering:** Apply enhanced scrutiny to traffic from Middle Eastern IP ranges and connections involving regional partners. Monitor hacktivist Telegram channels for #OpIndia or India-targeting campaigns.

Pillar 3: Resilience & Recovery

- **Offline, immutable backups:** Maintain air-gapped backups for all critical systems, especially ICS/OT, core banking, and healthcare. Test restoration under simulated wiper and ransomware scenarios, as Iranian actors have deployed wiper malware in the current conflict.
- **Crisis-specific IR playbooks:** Define escalation and response playbooks for: (a) DDoS on critical services, (b) ransomware with data exfiltration, (c) supply chain compromise, (d) OT/ICS targeted attack, (e) disinformation campaign. Conduct purple-team exercises simulating Iranian APT and hacktivist tactics.
- **Cyber insurance review:** Review policy exclusions for state-sponsored attacks and 'acts of war.' The Merck v. Zurich precedent and current kinetic-cyber hybrid conflict make war exclusion clauses a critical concern.
- **Cross-sector intelligence sharing:** Participate in CERT-In and private threat intelligence platforms. The convergence of hacktivist, criminal, and nation-state actors requires collective defence.

Key Learnings for Indian Industry Leadership

i. Cyber conflict is now inseparable from kinetic conflict

The February 2026 Iran strikes demonstrate that cyber operations are the first move, not an afterthought. Israel's cyber campaign preceded and paralleled kinetic strikes. Every future geopolitical crisis will have a cyber dimension affecting India through supply chains, energy markets, and shared infrastructure.

ii. India is never just a bystander

India faces cyber spillover regardless of its diplomatic stance. In today's global interconnected and complex supply chain, global ripples can quickly reach Indian shores.

iii. Energy security = cyber security

With 90% crude import dependency and 50% transiting through Hormuz, a cyberattack on Gulf port operations, tanker navigation, or pipeline SCADA systems compounds physical supply disruptions. Indian energy companies must treat cyber resilience as essential to energy security.

iv. AI is the double-edged sword

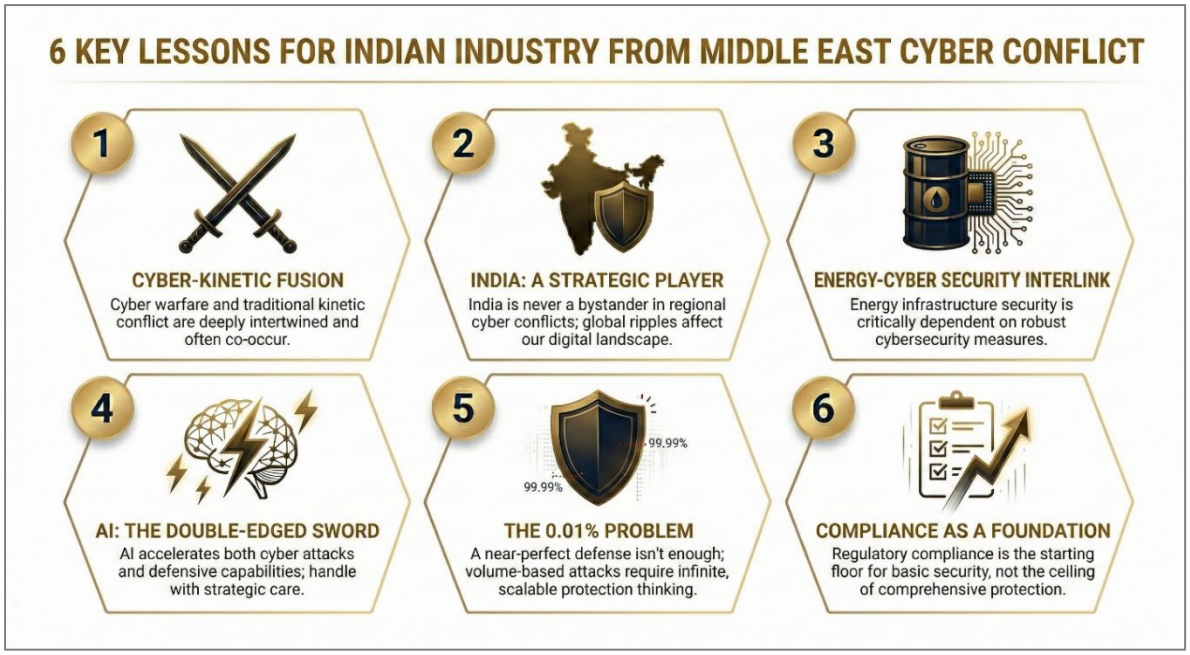
The UAE reported AI-enabled cyberattacks in the week before the February 2026 strikes. Meanwhile, AI-powered phishing, deepfakes, and automated vulnerability scanning operate at machine speed. India's response must match this pace with AI-augmented detection, behaviour-based analytics, and automated response capabilities.

v. The 0.01% problem demands volume-based defence thinking

When adversaries can launch 1.5 million attacks or coordinate 150+ hacktivist incidents in 72 hours (Feb 2026 Iran), even near-perfect defences yield breaches. Resilience, rapid detection, and recovery capability are as important as prevention.

vi. Compliance is the floor, not the ceiling

Compliance provides baseline requirements, but compliance alone is insufficient against state-sponsored APTs and coordinated hacktivist campaigns. Industry must invest in proactive, intelligence-driven security strategies that go beyond regulatory minimums.



References

[1] CloudSEK, "Situation Report: Middle East Escalation (February 27 – 1 March 2026)," CloudSEK Blog, 2 March 2026. Available at: https://www.cloudsek.com/blog/middle-east-escalation-israel-iran-us-cyber-war-2026

[2] The Jerusalem Post, "Israel plunges Iran into darkness with largest cyberattack in history during attack against Iran," 28 February 2026. Available at: https://www.jpost.com/israel-news/defense-news/article-888271

[3] NetBlocks, Internet connectivity monitoring data confirming Iran traffic dropped to 4% of normal levels, 28 February 2026. Cited in Jerusalem Post, Infosecurity Magazine, ZENDATA, and CloudSEK reports.

[4] Infosecurity Magazine, "Hybrid Middle East Conflict Triggers Surge in Global Cyber Activity," 3 March 2026. Available at: https://www.infosecurity-magazine.com/news/middle-east-conflict-surge-global/

[5] SecurityWeek, "US-Israel and Iran Trade Cyberattacks: Pro-West Hacks Cause Disruption as Tehran Retaliates," 2 March 2026.

[6] Sify, "Digital Siachen: How India's Cyber Warriors Thwarted Pakistan's 1.5 Million Cyber Onslaught," 20 May 2025. Available at: https://www.sify.com/ai-analytics/digital-siachen-how-indias-cyber-warriors-thwarted-pakistans-1-5-million-cyber-onslaught/

[7] Silobreaker, "Hacktivism in the India-Pakistan Conflict: Analysis of Recent Campaigns," June 2025. Available at: https://www.silobreaker.com/blog/geopolitical/hacktivism-in-the-india-pakistan-conflict-analysis-of-recent-campaigns/

[8] Lieber Institute, "Firewalls and Fault Lines: Cyber War in the Middle East," August 2025.

[9] CYFIRMA, "India Threat Landscape Report 2024," 2024.

[10] ZENDATA Cybersecurity, "Cyber Warfare in the US-Israel vs Iran Conflict (Roaring Lion & Epic Fury)," 2 March 2026. Available at: https://zendata.security/2026/03/02/cyber-warfare-in-the-us-israel-vs-iran-conflict-roaring-lion-epic-fury/

[11] SOCRadar, "Cyber Reflections of the U.S. & Israel-Iran War," 1 March 2026. Available at: https://socradar.io/blog/cyber-reflections-us-israel-iran-war/

[12] CNBC, "India hit by high oil prices, flight cancelations amid Iran conflict," 2 March 2026. Available at: https://www.cnbc.com/2026/03/02/india-impact-iran-middle-east-conflict-oil-prices-airlines.html

[13] Kpler, "US-Iran conflict: Strait of Hormuz crisis reshapes global oil markets," 1 March 2026.

[14] Business Today, "US Israel strike on Iran: Attack puts 50% of India's oil imports at risk via Hormuz," 28 February 2026.

[15] Down To Earth, "From crude to basmati: Iran war threatens India's energy and trade stability," 2 March 2026.

[16] Deccan Herald / Climate Trends, "Iran & Israel-US conflict: Strait of Hormuz crisis sparks energy security concerns for India," 1 March 2026.

[17] CyberPeace, "Cybersecurity Threats to India's Digital Ecosystem in 2026," January 2026.

[18] Palo Alto Networks Unit 42, "Threat Brief: March 2026 Escalation of Cyber Risk Related to Iran," 3 March 2026.

[19] CERT-In / PIB, "Year-End Review 2025: Ministry of Electronics & IT," December 2025. Source for 29.44 lakh incidents handled, 1,530 alerts, 390 vulnerability notes, and 65 advisories.

[20] World Economic Forum, "Global Risks Report 2026: Cybersecurity ranked #1 risk for India," January 2026.

[21] Seqrite (DSCI), "India Cyber Threat Report 2026," January 2026.

[22] Algoritha Security, "India Cyber Threat Report 2026: 500M Malware Detections," March 2026.

[23] Check Point Software, "2026 Cyber Security Report: India faces 3,195 weekly attacks per organisation," February 2026.

[24] Enterprise IT World, "India's Critical Infrastructure Faces the Reality of AI-Powered Cyber Warfare," January 2026.

[25] Nextgov/FCW, "Intelligence firms watch for uptick in Iran cyber activity after US, Israel strikes," 3 March 2026.

Disclaimer

This advisory is produced for informational purposes only and is intended to assist the Indian industry in understanding and preparing for cyber threats arising from the Middle East conflict. The information contained herein is based on publicly available threat intelligence as of 3 March 2026 and is subject to change as the situation evolves.

However, DSCI disclaims all warranties as to the accuracy, completeness, or adequacy of such information. The information contain herein should not be relied upon as a substitute for specific professional advice.

DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

ABOUT DSCI

Data Security Council of India (DSCI) is a not-for-profit, industry body on data protection in India, set up by Nasscom, committed to making cyberspace safe, secure, and trusted by establishing best practices, standards and initiatives in cybersecurity and privacy. DSCI works together with the Government and their agencies, law enforcement agencies, industry sectors including IT-BPM, BFSI, Telecom, data protection authorities and think tanks for public advocacy, thought leadership, capacity building and outreach initiatives.

Data Security Council of India
4th Floor, Nasscom Campus, Plot No. 7-10, Sector 126, Noida, UP-201303

data-security-council-of-india/ DSCI_Connect dsci.connect
dsci.connect dscivideo security chips