DSCI
PROMOTING DATA PROTECTION

2025 CYBER SECURITY OUTLOOK

CYBER THREAT PREDICTIONS 2025

- **Shadow AI** - The next insider threat
- **AI to dominate cyber defence**
- **NHI** - New attack surface
- **SMEs to become frontline targets**
- **Zero trust to fail without governance**
- **Deepfake attacks become mainstream**
- **GenAI prompt injection to rise**
- **Synthetic data powered security testing**
- **Ransomware goes modular and autonomous**
- **API abuse to outpace web exploits**
- **Mandatory licensing requirement for cyber resilience**

INSIGHTS INTO CYBERSECURITY TRENDS 2025

1. Threat Evolution

AI Powered Cyber Attacks

In 2024, 79% of cyber intrusions did not involve traditional malware but relied on AI-driven social engineering, cloud exploits, and vulnerability chaining.[1] The average cost of a data breach in India in 2024 reached $2.35 million, an 8% increase from the previous year, with one in three breaches involving AI-driven techniques.[2] AI has supported evolution of traditional cyber-attacks into:

- **AI powered Polymorphic Malware** – Extensive use of AI in malware development will potentially expand to creation of polymorphic malwares that have ability to conceal themselves by changing forms and bypassing security systems.
- **Autonomous Bots** capable of conducting reconnaissance, exploitation, and propagation without human intervention, making attacks faster and harder to detect. 48% increase in bot attacks from Q1 2024 to Q4 2024.[3]
- Rapid integration of LLMs in enterprises IT Infrastructure opens pathway for threats like **GenAI prompt injection attacks, prompt bombing and jailbreaking** that will lead to increasing incidences of data leaks, harmful content generation, unauthorised actions, and security policy bypass.

Multi-Vector Attacks

By combining techniques such as phishing, malware, network exploits, cloud misconfigurations, and insider threats attackers increase their chances of success and make detection and response far more difficult.

APT36-Style ClickFix Attack: Spoofing an Indian Ministry, this attack targeted Windows and Linux systems using a ClickFix campaign that combined phishing emails with polymorphic malware to deliver malicious payload along with credential harvesting and data exfiltration.[4]

Interactive Intrusion

Political adversaries are engaging in real-time, human-driven operations on compromised systems rather than purely automated malware campaigns to explore, escalate, and exfiltrate data. **Dance of the Hillary**: Distribution of malware through social media platforms, aiming to compromise digital security across various sectors in India after India's strategic defence operation.

Deepfake Voice Phishing

Attackers using AI-generated voice clones to impersonate trusted individuals to deceive targets into divulging sensitive information or transferring funds, especially in the financial sector.

Jamtara 2.0: Deepfake technology to manipulate video KYC processes, impersonate executives, and create fake digital evidence.[5]

Ransomware-as-a-Services

RaaS has evolved into a decentralised, affiliate-driven ecosystem fueled by AI automation, leading to global surge in ransomware incidents and enabling even low-skilled actors to launch faster, more scalable, and more targeted cyber extortion campaigns.

- Ransomware Containers – evades end point detection
- Ransomware-as-a-code – dynamic delivery of payloads, harder to track
- AI-powered RaaS kits – Intelligent Automation
- RaaS marketplaces in dark web
- Command-and-Control Infrastructure

Dominant Ransomware Groups in India providing RaaS[6] – LockBit (LockBit Ransomware source code has contributed to the proliferation of ransomware attacks by new players and affiliates), RansomHub, KillSec, Akira, Fog, Makop, Mallox, BlackCat (ALPHV), Conti, etc.

Entry Points exploited: Unsecured Remote Desktop Protocols (RDP), publicly exposed MS-SQL servers (xp_cmdshell), Living off the Land Binaries and Scripts (LOLBAS), publicly exposed NAS devices and Redis Servers.

Tools:

- PowerShell allows attackers to remotely download and execute arbitrary code and binaries
- Command prompt-based commands and batch scripts
- Bring Your Own Vulnerable Driver (BYOVD)
- Remote Monitoring and Management (RMM) tools such as AnyDesk, ScreenConnect, Splashtop, etc.
- EDR killers, blockers, and silencers to disable or bypass endpoint security solutions

NPM and Smart-Contract Typosquat Attacks

A surge of over 800 malicious packages (e.g., jest-fet-mock, axioss, reacct) were uploaded to NPM in 2024.[7]

The AI Cyber Paradox 2.

- Indians lost over ₹11,000 crore to cyber frauds in the first half of 2024, with around 6,000 complaints filed daily on the National Cyber Crime Reporting Portal.[8]
- Increasing incidences of impersonation of officials from government agencies using AI to extort money.[9]
- CERT-In noted increased chatter in dark web forums about using LLMs like WormGPT and open-source clones to script exploits against Indian financial systems.
- An SSRF vulnerability exploited in early 2025 targeted Indian SMEs using white-labelled ChatGPT APIs for chatbot services.[10]

AI Powered Cyber Defence

AI is becoming **core to real-time defence**, with widespread use of AI-driven **Continuous Control Monitoring (CCM)**, **predictive threat modeling**, and **AI-assisted deception technologies.**

- **Threat Detection and Anomaly Analysis**
  - AI triage systems reduce investigation times by summarizing massive alert logs. Use of GenAI in SOC triage.
  - Scrape, cluster, and analyse threat data (IOCs, TTPs, CVEs) from dark web, forums, GitHub, etc.
- **AI powered Security Assistants and SOC Automation**
  - AI can integrate threat intel, incident analysis, and workflow automation.
  - Crafting detection rules, incident reports, and reverse engineering malware signatures using LLMs.
  - Integrating AI agents into SOCs to investigate incidents and execute response actions dynamically. Security AI Assistants will become default in SOCs.
- **AI driven SOAR**
  - Indian SOCs in telecom & energy are piloting AI-based SOAR modules integrated with legacy SIEM tools, often backed by Indian Defence Agencies analytics or in international partnerships.

Shadow AI

In 2025, most GenAI use in the enterprise (72%) is shadow IT, driven by individuals using personal accounts to access GenAI apps.[11]

- Proprietary source code sharing with generative AI apps accounts for 46% of all data policy violations.
- Regulated data, which organisations have a legal duty to protect, make up more than a third (35%) of the sensitive data being shared with GenAI applications.
- The use of GenAI apps increased from 74% to 96% of organisations from 2023 to 2024.

Implication in Cybersecurity and IT Strategy:

- Redefining security perimeter beyond known applications and infrastructure.
- Addressing new risk classes like data poisoning, hallucination-based decision making, and unvetted model training.
- Supply chain exposure - audit third-party AI interactions, integrate AI clauses in vendor contracts, and ensure data classification policies are enforced upstream.
- Equip SOC teams with LLM-aware detection tools, introduce AI observability dashboards, and conduct simulations of prompt injections and API misuse.

By embedding proactive AI governance, visibility, and cultural alignment, CISOs can turn Shadow AI from a blind spot into a lever for secure innovation.

3. Access Management

Non-Human Identity

NHIs now outnumber human users by ratio of 45 to 1, making Machine Identity Management (MIM) and third-party security a top priority. Without securing NHIs, organisations risk privilege escalation, credential theft, and unauthorized access across systems.

Current State of NHIs

- Expanding Scope beyond MIs where organisations are now formally recognising animals (IoT-tagged livestock, research animals) and organisations (customers, vendors) as NHIs within IAM systems.
- NHI lifecycle management (creation, rotation, revocation, governance) is still immature in many enterprises.
- Threat actors are actively exploiting NHIs to hijack credentials and move laterally, increasing incidences of inappropriate access via NHIs.
- Organisations increasingly include NHIs in their zero-trust architecture and move from detection (ITDR) to prevention-centric (ITPR) strategies.
- With NHIs rapidly becoming the dominant identity class, the next wave of identity security will focus on context-aware authorisation and autonomous identity orchestration tailored to machine behaviour and interconnectivity.
- Machine identities (MIs) are the fastest growing identity class, often unmanaged or loosely governed, projected to reach 100 to 1 in ratio by the end of 2025, creating a massive new attack vector.

Zero Trust Centre of Excellence

Enterprises need clearly defined Zero Trust program which also includes creation of Zero Trust Centre of Excellence – a centralised team or organisational function that drives the enterprise's ZT strategy, governance, implementation, and continuous improvement.

Approximately 63% of enterprise had initiated or partially implemented a zero-trust strategy. However, about 35% of these initiatives were reported as unsuccessful, leading to negative impacts on the organisations involved.[12]

Factors Enterprise must Consider Before Setting up ZTCE	
Executive and Stakeholder Buy-in Secure leadership alignment on ZT goals, benefits and success metrics.	**Integrated Tooling and Automation** Security solutions that provide unified visibility, centralised policy management.
Clear Business Priorities & Protected Surfaces Identifying critical assets, data, applications, and services that need protection.	**Communication and Change Management** Transparent communication with employees during ZT adoption stage.
Current IT Architecture and Readiness Identifying critical assets, data, applications, and services that need protection.	**Phased Implementation and Metrics** Gradual rolling starting with less critical systems to gain trust co-critical assets.

Biometric Access Management

By 2026, attacks using AI-generated deepfakes on face biometrics will mean that 30% of enterprises will no longer consider such identity verification and authentication solutions to be reliable in isolation.[13]

The future of authentication is moving toward **multi-modal, continuous, and context-driven identity validation**, where no single method—especially biometrics is relied upon in isolation.

- Behavioural Biometric: Based on unique user behaviour patterns like how a person types, moves a mouse, walks, or uses a touchscreen.
- Continuous and Adaptive Authentication: Instead of a one-time check, monitors user behaviour, device posture, location, and contextual signals throughout the session.
- Deepfake Detection: AI-powered anti-spoofing checks distinguish between real faces and deepfakes/images.
- Decentralised Identity and Verifiable Credentials: Enables user-controlled identity sharing via blockchain, allowing cryptographic verification without exposing raw biometric data.
- Bio-Cryptography: Uses biometrics to generate cryptographic keys on demand—never stored, making them immune to theft.

Enterprises must adopt advanced, adaptive, and continuous authentication methods that move beyond static credentials to ensure stronger and more dynamic security.

Securing Synthetic Data 4.

Not all synthetic data is secure by default; Synthetic data should be governed by **the same rigor as sensitive real data**, especially when it can influence models, decisions, or outcomes. While synthetic data may not directly reveal real identities, it can still embed sensitive patterns or biases from the original dataset, making it vulnerable to misuse or inference attacks. As synthetic data mimics the original data, it poses the risks of re-identification, model inversion, or insider inference attack.

"Technological capabilities designed to transform or generate data to protect the confidentiality of personal or sensitive source data against compromise, or to accelerate ML focused use cases." – Gartner.

- AI Model Training
- Software Testing
- Privacy-preserving Data Analytics
- Data Simulation

Emerging Practices in Synthetic Data Security

- Synthetic Data Governance Framework – defining lifecycle management for synthetic data.
- Federated Synthetic Data Training – Decentralised storage to enhance privacy.
- Explainable Synthesis Audit – Use Explainable AI (XAI) tools to validate non-bias in synthetic data.
- Tamper proof data labels using blockchain or digital watermarking.

5. Application Data Security

In coming years, organisations will increase the spend on application and data security by 15% on yearly basis highlighting the importance of securing application data.[14]

- Application data includes Personally Identifiable Information (PII), intellectual property, financial transactions, and other sensitive content.
- A breach can expose sensitive customer or corporate data, leading to reputational damage and regulatory penalties.
- Data integrity and availability are essential to keep services running and maintain stakeholder trust. Loss or manipulation of application data can disrupt operations or misinform decisions.
- Unsecure application data may result in reputational damage, regulatory action and fines, IP theft, financial fraud and data manipulation, and operational disruption.
- Enterprises must adopt secure SDLC with integrated and secured testing.
- With the advent of quantum computing, enterprises should also begin transitioning to Post-Quantum Cryptography to future-proof application data against quantum-enabled threats.
- Implementing PQC algorithms early ensures long-term confidentiality and resilience of sensitive application data.
- Although large-scale quantum computers capable of breaking classical encryption do not yet exist, the threat of "harvest now, decrypt later" is immediate.
- Threat actors are already collecting encrypted data with the intent to decrypt it in the future using quantum capabilities putting long-lifespan data (e.g., intellectual property, personal records, strategic communications) at significant risk.

Securing Greenfield Manufacturing & Industrial Projects 6.

Newly established manufacturing plants, smart factories, or infrastructure projects built from the ground up offer a unique opportunity to embed cybersecurity by design.

Key Recommendations for Security Pillar

Security Pillar

- **Continuous Monitoring & Threat Detection** – Deploy Security Information and Event Management (SIEM) systems with real-time analytics and AI-driven anomaly detection.
- **Secure by Design** – Integrate cybersecurity into architectural planning network segmentation, data zoning, and endpoint security from the start.
- **Identity & Access Control** – Use least-privilege policies, multi-factor authentication, and role-based access, especially for external vendors.
- **Secure Supply Chain** – Vet third-party software, firmware, and hardware vendors; implement Software Bill of Materials (SBOM).
- **Zero Trust Network Architecture** – Apply "never trust, always verify" to users, devices, and applications even inside the perimeter.
- **OT-IT Convergence Security** – Protect industrial control systems (ICS) by deploying firewalls, intrusion detection (IDS), and strict protocol whitelisting.
- **Data Security & Resilience** – Encrypt critical operational data and maintain secure, tested backup and disaster recovery systems.

Reducing Attack Surface

Industrial enterprises often have complex networks combining IT (Information Technology) and OT (Operational Technology) systems, which require stringent security due to critical infrastructure and safety concerns.

Network zones help reduce the attack surface in a new industrial facility by dividing the overall network into smaller, isolated segments based on function, sensitivity, or user groups, thereby limiting the scope and impact of potential cyberattacks.

Industrial Facility - Secure Network

- **Industrial Control System** – restricts all inbound/outbound traffic except from authorized maintenance systems
- **Vendor Zone** – limited, monitored access only during scheduled maintenance window
- **Guest Network** – isolated with no access to other zones
- **Corporate IT** – enforces MFA and end point security

7. Supply Chain Security

The global annual cost of software supply chain attacks to businesses was projected to reach $60 billion in 2025 where damages are predicted to grow by 15 percent year-over-year through 2031.[15]

Securing Supply Chain

- Zero Trust for supply chain ecosystem treat every supplier, device, and service as "untrusted by default".
- Continuous Supplier Risk Scoring, for example, ISO/IEC 42001:2023 (AI management systems, indirectly relevant to AI in supply chains).
- Digital Twin + Cybersecurity Simulation to simulate cyber-physical risk scenarios.
- Secure Software Bill of Materials that can be machine readable, continuously updated (instead of static PDF), and validated with hash-based integrity check.[16]
- India should mirror standards on supply chain security through bi-lateral and multi-lateral engagements.

Governance, Risk and Compliance 8.

To address an increasingly complex threat and regulatory landscape in cybersecurity, organizations are recognising the need for integrated, proactive, and adaptive GRC frameworks.

- CyberGRC for Security-First Governance – Align cybersecurity strategy with regulatory mandates, risk appetite, and business objectives to streamline policies, improve audit readiness, and ensure end-to-end visibility into cyber risks and controls.
- Optimising GRC for Cybersecurity by integrating GRC platforms with SIEM, SOAR, and threat intelligence tools to automate policy enforcement, real-time risk scoring, and control monitoring.
- In 2024 and 2025, significant changes in cybersecurity laws and regulations (CSCRF, 2024; Telecom Cyber Security Rules, 2024; DPDP Act and Draft Rules; e-Zero FIR Pilot Project; CCTV Cybersecurity Compliance; and RBI's Enhanced Cybersecurity Oversight – 2025) reflect the growing need for comprehensive regulatory frameworks based on cyber norms.
- Make operational resilience as core strategy, focusing on business continuity, disaster recovery, and incident response planning.

AI in GRC

Organisations effectively implementing AI-driven risk management tools are expected to reduce cybersecurity incidents by 25% by 2026.

- Cognitive AI and hyper-automation enables real-time risk assessment, regulatory monitoring, and AI-driven fraud detection.
- LLM and GenAI for policy automation streamlines drafting and updating of compliance documents, enhancing agility and regulatory responsiveness.
- AI-powered Continuous Control Monitoring (CCM) tools continuously evaluate compliance by analysing logs, configs, and user activity in real time.

Integrating ESG and GRC

- Update GRC Metrics to include ESG-aligned indicators such as digital ethics, secure sustainability practices, and responsible AI.
- Engage ESG teams in cyber risk assessments to jointly evaluate impact on people, planet, and policy.
- Leverage GRC platforms that allow ESG + cybersecurity risk aggregation, monitoring, and disclosure.
- Incorporate ESG in Incident Response Plans, especially for breaches involving privacy, surveillance, or environmental systems.

9. Collaborative Cyber Risk Management

Pooling expertise, intelligence, capabilities, and accountability across stakeholders—internal and external to create a shared defence posture. It bridges silos, strengthens cyber resilience, and ensures proactive, agile response to evolving threats. Centralised policy management ensures that all security rules and access controls are governed consistently and efficiently across the organisation.

With increasing adoption of Digital Public Infrastructure, centralised policy enforcement is critical across sectors like finance, health, and e-governance.

- CERT-In and MeitY are pushing for sectoral SoCs and centralised cyber governance nodes to track compliance and incident readiness across critical infrastructure.
- CERT-In, NCIIPC, and MeitY promote cyber coordination through advisories and incident reporting frameworks.
- Cross-border collaboration frameworks (especially in ASEAN and Quad nations, including India); Government-led **Collaborative Security Scorecards** for regulated industries.

Key Principles

- Cross-functional coordination within the enterprise
- External Stakeholder Engagement
- Sectoral or National Intelligence Sharing
- Technology Stack Interoperability

Cybersecure SMEs 10.

- 98% of cyber insurance claims ($1.9 billion in total) were from small to medium enterprises (SMEs) with less than $2 billion in annual revenue.[17]

SMEs have potential to be entry points into larger supply chains. The DPDP Act (2023) mandates protection of personal data even for small businesses processing customer data. Four key pillars to securing SMEs:

1. Security Operations Centres: Increasing adoption of **SOC-as-a-Service or Managed Detection & Response (MDR)** is addressing talent shortages and enhance continuous threat monitoring without needing to build costly in-house teams.
2. Virtual CISOs (vCISO): vCISOs deliver strategic cybersecurity leadership on-demand, bridging gaps in executive expertise by helping optimize security budgets by aligning tech spend with risk appetite, facilitating compliance, and negotiating vendor contracts. Driven by SMEs interests, 86% MSPs and MSSPs were offering vCISO services by end-2024.
3. Cloud- Delivered Security: Cloud platforms enable SMEs to access advanced built-in security (e.g., IAM, encryption, logging) at minimal upfront cost reducing operational overhead and streamline scaling.
4. Cost-Effectiveness & Budget Optimisation: MDR providers are offering enterprise-grade tools and expertise without capital outlay with fixed-cost, subscription-based cybersecurity.

GEOPOLITICS AND CYBERSECURITY

11. Political Turbulence

Recent Cyberattacks on India

Surge in Security Incidents[18]

- Indian Cyber agencies identified 7 APTs group responsible for launching over 15 lakh cyber-attacks targeting critical infrastructure websites
- Dance of Hillary - Pakistani Intelligence Operatives (PIOs) were found to be targeting mobile phones used by defence personnel and journalists in India
- Reported incidents of Malware Campaign, DDoS attacks, GPS Spoofing, and Misinformation Campaigns
- Transnational alliance of hacktivist groups from Asia, Africa and Latin America regions mobilized under anti-India hashtags and causes
- Website defacement and misinformation attacks

Expanded Warfare Landscape

- Hybrid warfare doctrine: Kinetic acts are paired with digital disruption to destabilise national response, influence media narratives, and pressure diplomatic channels.
- Blurring lines between cybercrime and cyberwarfare – State-drive threat actors are blending with hacktivist groups to maintain plausible deniability.
- Critical infrastructure – often run on legacy industrial control systems and SCADA networks with low cybersecurity maturity.
- Cyber espionage and data exfiltration.
- Information and psychological warfare.
- Warfare blurring with civilian space.

Strategic and Operational Impacts on Indian Cybersecurity

Domain	Cyber Defence Readiness	CERT-In Advisory Cycle	Policy Shifts	Diplomatic Cyber Deterrence
Impact	National critical infra moved to heightened alert posture with increased AI-led threat monitoring	More frequent threat advisories, TTP sharing, and joint war-gaming with PSU and private infra operators	MeitY fast-tracking frameworks on critical infra cyber zoning, red-teaming mandates, and threat intel sharing laws	India expanding bilateral dialogues with Quad, EU, and Israel for threat attribution and response coordination

Global Tensions and Impact on Cybersecurity Ecosystem[19]

Global cybersecurity ecosystem has become shadow battlefield. Nation-states are leveraging cyber capabilities to achieve strategic goals without direct military engagement.

Fault Lines

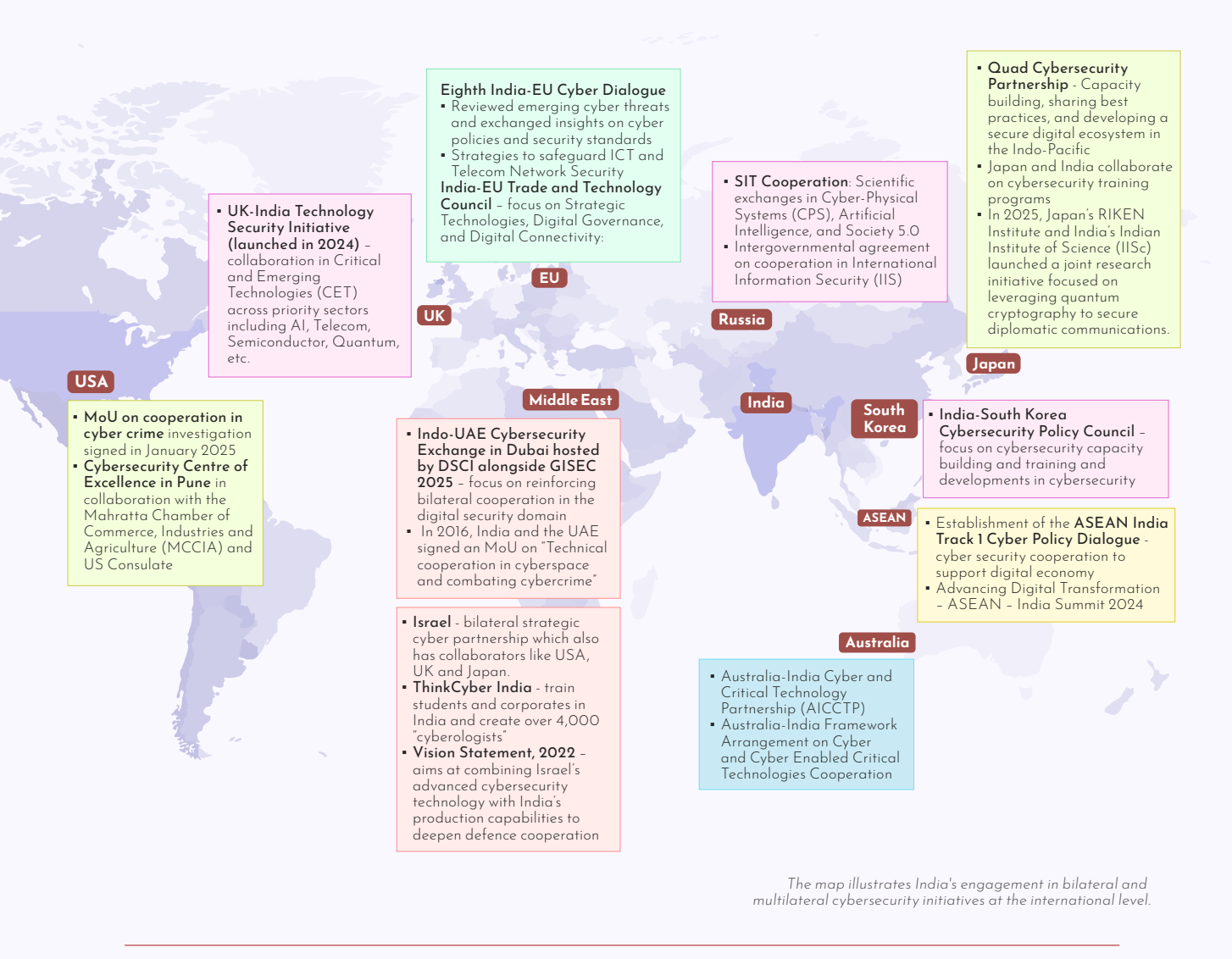
- US – China Tech War
- Russia – NATO Conflict
- Iran – Israel Tension
- Indo – Pacific Realignment
- Israel – Hamas War
- Armenia – Azerbaijan

Common Threats Associated with Geopolitical Tensions[20]

- State Sponsored Attacks
- Cyber Espionage
- DDoS Attacks
- Supply Chain Attacks
- Critical Infrastructure Sabotage
- Hacktivism and Proxy Attacks

Future Outlook

- **Cyber Alliances & Digital Defence Pacts** – Expansion of cyber clauses in military/ security alliances (e.g., NATO's Article 5 for cyber)[21]
- **Cyber Deterrence Doctrines** – States publicly attributing and retaliating for cyberattacks (e.g., U.S. DOJ indictments of APT groups)
- **Weaponisation of AI in Cyber Conflict** – Use of LLMs for autonomous intrusion, deepfake warfare, automated zero-day discovery
- **Quantum Cold War** – Nations rushing to develop **quantum-safe encryption** amid fears of post-quantum decryption by adversaries
- **Multi-lateral Convention** – Multilateral efforts to establish **norms of cyber engagement** though adoption may remain fractured


USA
• MoU on cooperation in cyber crime investigation signed in January 2025
• Cybersecurity Centre of Excellence in Pune in collaboration with the Mahratta Chamber of Commerce, Industries and Agriculture (MCCIA) and US Consulate
UK
• UK-India Technology Security Initiative (launched in 2024) – collaboration in Critical and Emerging Technologies (CET) across priority sectors including AI, Telecom, Semiconductor, Quantum, etc.
EU
Eighth India-EU Cyber Dialogue
• Reviewed emerging cyber threats and exchanged insights on cyber policies and security standards
• Strategies to safeguard ICT and Telecom Network Security
India-EU Trade and Technology Council – focus on Strategic Technologies, Digital Governance, and Digital Connectivity.
Middle East
• Indo-UAE Cybersecurity Exchange in Dubai hosted by DSCI alongside GISEC 2025 – focus on reinforcing bilateral cooperation in the digital security domain
• In 2016, India and the UAE signed an MoU on "Technical cooperation in cyberspace and combating cybercrime"
• Israel - bilateral strategic cyber partnership which also has collaborators like USA, UK and Japan.
• ThinkCyber India - train students and corporates in India and create over 4,000 "cyberologists"
• Vision Statement, 2022 – aims at combining Israel's advanced cybersecurity technology with India's production capabilities to deepen defence cooperation
Russia
• SIT Cooperation: Scientific exchanges in Cyber-Physical Systems (CPS), Artificial Intelligence, and Society 5.0
• Intergovernmental agreement on cooperation in International Information Security (IIS)
India
Japan
• Quad Cybersecurity Partnership - Capacity building, sharing best practices, and developing a secure digital ecosystem in the Indo-Pacific
• Japan and India collaborate on cybersecurity training programs
• In 2025, Japan's RIKEN Institute and India's Indian Institute of Science (IISc) launched a joint research initiative focused on leveraging quantum cryptography to secure diplomatic communications.
South Korea
• India-South Korea Cybersecurity Policy Council – focus on cybersecurity capacity building and training and developments in cybersecurity
ASEAN
• Establishment of the ASEAN India Track 1 Cyber Policy Dialogue - cyber security cooperation to support digital economy
• Advancing Digital Transformation – ASEAN – India Summit 2024
Australia
• Australia-India Cyber and Critical Technology Partnership (AICCTP)
• Australia-India Framework Arrangement on Cyber and Cyber Enabled Critical Technologies Cooperation

The map illustrates India's engagement in bilateral and multilateral cybersecurity initiatives at the international level.

References

1. Global Threat Report, 2025, Crowdstrike
2. Cost of Data Breach Report 2024, IBM
3. State of Application Security Report 2024, Indusface
4. Advisory - Targeted APT36 Campaign Exploiting Pahalgam Terror Incident for Cyber Espionage, Maharashtra Cyber
5. Jamtara 2.0 and Deepfake Fraud: India to Lose ₹70,000cr in 2025, Data Quest, India
6. India Ransomware Report 2024, Cert-In
7. 800+ NPM Registry Packages at Risk of 'Manifest Confusion' Attacks, Secure Blink
8. India Lost Over ₹11,000 Crore to Cyber Scams in First 9 Months of 2024, Hindustan Times
9. How Scammers Are Using AI, Transforming India's Cybercrime Landscape: '60-70% of Our Work Depends on It', The Print
10. ChatGPT Commit f9f4bbc SSRF Vulnerability Exploited, Broadcom
11. Cloud and Threat Report: Generative AI 2025, Netskope
12. State of Zero Trust Adoption Survey, 2024, Gartner
13. Anticipate and Manage Disruptive Trends to Boost Resilience in 2025, Gartner
14. Over 100 Data, Analytics and AI Predictions Through 2030, Gartner
15. Software Supply Chain Attacks To Cost The World $60 Billion By 2025, Newswire
16. Technical Guidelines on Software Bill of Materials (SBOM), 2024, CERTIn
17. Cyber Claims Study, 2024, NetDiligence
18. Pakistan-Allied Hackers Launched 15 Lakh Cyber Attacks on Indian Websites; Only 150 Successful, The Economic Times
19. Global Cybersecurity Outlook 2025, World Economic Forum
20. Top Geopolitical Risks of 2025, S&P Global
21. Article 5 – Collective Defence, NATO (*If a NATO Ally is the victim of an armed attack, each and every other member of the Alliance will consider this act of violence as an armed attack against all members and will take the actions it deems necessary to assist the Ally attacked, North Atlantic Treaty outlines.*)

Disclaimer:

The information presented pertains to the period between January 2024 and May 2025. Please note that there may have been updates or changes subsequent to this timeframe.

Data Security Council of India
4th Floor, Nasscom Campus, Plot No. 7-10, Sector 126, Noida, UP-201303
+91-120-4990253 | info@dsci.in | www.dsci.in
data-security-council-of-india/ DSCI_Connect dsci.connect
dsci.connect dscivideo security chips

All Rights Reserved © DSCI 2025