indiastat
focused on facts

SOCIO-ECONOMIC VOICES

Future-Proofing India's Cyber Defenses: From Incident Response to Policy Frameworks

Cdr Aditya Varma (Retd.),
Cyber Security Risk & Management Expert

India's Approach to Cybersecurity and Geopolitical Challenges - Insights from Ace Cyber Expert

Intro: Did you know that India is currently facing a massive global shortage of cybersecurity professionals, with a staggering 3.5 million vacancies worldwide? Or that the National Mission on Quantum Technologies and Applications has been allocated a groundbreaking ₹8,000 crores to stay ahead of future cyber threats? Amidst the rising Geo-political tensions and cyber threats, are you curious about how India can navigate these complex challenges by implementing certain strong strategic measures? This week on **Indiastat** we have **Cdr Aditya Varma (Retd.), Cyber Security Risk & Management Expert** having an exclusive discussion with **Mahima Sharma,** helping solve this intense puzzle and much more. Read the **Socio-economic Voices'** exclusive now...

MS: Considering the technological warfare being adopted in both Ukraine-Russia, Israel-Palestine (Gaza) wars, what key factors India needs to deploy to better secure the nation over the next few years?

CAV: The Indian government has proactively launched the National Cyber Security Strategy 2020, which calls for joint efforts between public institutions and private entities to strengthen cybersecurity defences. In the Interim Union Budget 2024, the government allocated ₹8,000 crores to the National Mission on Quantum Technologies and Applications, highlighting the importance of investing in R&D to foresee and counter future threats. Participation in global cybersecurity forums such as the Global Forum on Cyber Expertise (GFCE) allows India to share knowledge and strategies, which is essential for countering state-sponsored cyber activities and adopting best practices.

To enhance our national cybersecurity, India needs to focus on the following key areas:

- **Addressing the Workforce Shortage**

As of 2023, there is a global shortfall of 3.5 million cybersecurity professionals. India must invest in comprehensive training programs to bridge this gap and develop a skilled workforce capable of handling evolving cyber threats (Cybersecurity Ventures, 2023). Establishing specialised cybersecurity training programs in collaboration with educational institutions will create a robust pipeline of cybersecurity talent.

- **Investing in Advanced Technologies**

The global cybersecurity market is projected to grow from $230.5 billion in 2023 to $376.5 billion by 2029, with a CAGR of 8.2%. Investing in advanced technologies such as AI, machine learning (ML), and quantum computing is crucial for India to stay ahead of cyber threats. These technologies will enhance threat detection and response capabilities, enabling more effective prediction, identification and mitigation of cyber threats.

• Updating Cybersecurity Frameworks

It is essential to establish and continuously update national cybersecurity frameworks and standards to ensure comprehensive protection. The National Critical Information Infrastructure Protection Centre (NCIIPC) plays a significant role in safeguarding critical infrastructure. Aligning these frameworks with current and emerging threats will provide a robust defence mechanism for vital sectors (National Cyber Security Strategy 2020).

• Enhancing Incident Response Teams

Building and enhancing national and regional incident response teams is crucial to quickly address and mitigate cyber threats. Given India's vast geography, having effective incident response teams can help detect, analyse, and respond to cybersecurity incidents promptly, minimising potential damage and preventing widespread impact.

• Generative AI

The adoption of generative AI is expected to help bridge the cybersecurity skills gap and reduce employee-driven incidents by creating hyper-personalised training materials. By 2028, it could remove the need for specialised education for 50% of entry-level positions.

• Outcome-Driven Metrics

Organisations are increasingly adopting outcome-driven metrics to better communicate cybersecurity strategies to executives, ensuring that investments are directly tied to protection levels and clearly understood by non-IT stakeholders. This adoption can also be done at the National level.

• Continuous Threat Exposure Management

Prioritising investments based on continuous threat exposure management programs can significantly reduce breaches by up to two-thirds by 2026. How this can be implemented at the National level, would need a lot of collaboration from multiple stakeholders.

MS: In 2022 cyber-attacks were seen from China side on India's power grid, India had stated that ops failed. In your study and experience, where does India stand today in terms of Security & Risk Management? How do you read China's build up on the borders? And what Security & Risk Management & Compliance measures should we start taking up?

CAV: China has been actively bolstering its military infrastructure, including roads, railways, and airfields, to enable swift troop movements and logistics support. A 2023 report by the Institute for Defence Studies and Analyses (IDSA) notes that China has built over 1,000 kilometers of new roads and upgraded several airfields near the Line of Actual Control (LAC) in the past three years. By 2024, it is estimated that China will have already stationed around 200,000 troops along its borders with India, a significant increase from previous years. This figure is based on satellite imagery and reports from the Centre for Strategic and International Studies (CSIS).

China has also increased the frequency and scale of military exercises near the LAC. **The Chinese Ministry of Defence reported conducting more than 30 large-scale military exercises in 2023, compared to 22 in 2022.** These exercises often include simulated combat scenarios and show-of-force operations. Furthermore, China has enhanced its weaponry and surveillance capabilities, introducing advanced systems like the **Type 99A main battle tank and DF-17 hypersonic missiles in the border regions, according to the International Institute for Strategic Studies (IISS).**

Despite India's stance as a peace-loving nation, it is imperative to enhance our defence systems, including cyberspace, in response to these developments. Strengthening our cyberspace involves several key measures that I will share now...

A) Strengthening Cyber Defence Mechanisms

- **Investment in Advanced Cybersecurity Technologies** such as Next-Generation Firewalls (NGFW), Intrusion Prevention Systems (IPS), Threat Intelligence Platforms, Data and AI/ML driven SOC platforms. According to a 2024 report by Gartner, the global cybersecurity market is expected to reach $450 billion by 2025, with a significant portion allocated to advanced threat detection and response systems.
- **International Cyber Defence Partnerships** for real-time threat intelligence sharing. The National Cyber Security Centre (NCSC) of the UK has been a key partner in global cyber defence efforts, and India should seek similar collaborations.

B) Risk Management Frameworks

- **Rigorous Risk Management** that includes regular threat assessments and vulnerability scans. A 2024 report by Deloitte highlights that 78% of organisations that adopted continuous risk assessment methodologies experienced fewer security breaches.
- **Incident Response Plans** to handle potential cyber threats. According to the 2023 State of Incident Response Report by Forrester, companies with well-documented incident response plans are 50% more effective in mitigating the impact of cyber incidents.

C) Regulatory Compliance

- **Adherence to International Standards** such as ISO/IEC 27001 and NIST Cybersecurity Framework. The 2024 Cybersecurity Trends Report by SANS Institute emphasises that adherence to these frameworks significantly enhances organisational security posture.
- **Compliance with Government Regulations** related to cybersecurity and data protection, such as the Personal Data Protection Bill (PDPB), which is set to become law in the near future.

D) Public and Private Sector Collaboration

- **Collaborative Efforts** to share best practices and develop joint strategies for cyber resilience. The National Critical Information Infrastructure Protection Centre (NCIIPC) has been instrumental in such collaborations, and expanding these efforts is crucial.

MS: What are the key challenges India faces in cybersecurity?

CAV: India faces several significant challenges in cybersecurity, stemming from rapid digitisation, a lack of awareness and an insufficient skilled workforce. I am breaking these down in a simple manner...

Lack of Awareness

A report from the Internet and Mobile Association of India (IAMAI) shows that only 28% of users know cybersecurity best practices. This gap exposes them to risks like phishing, which made up 43% of cyber threats in 2023. Enhanced awareness programs are essential to protect users.

Rapid Digitisation

With more services moving online, vulnerabilities increase. The National Cyber Security Coordinator (NCSC) reports over 35 million cyber incidents in India in 2023. This rapid digitisation drives growth but also introduces new security challenges that require effective solutions.

Insufficient Skilled Workforce

India faces a severe shortage of cybersecurity professionals. The Data Security Council of India (DSCI) projects a 2 million professional shortfall by 2025. Despite thousands of IT graduates yearly, a 2023 NASSCOM report highlights a significant expertise gap in addressing complex cyber threats.

Evolving Threat Landscape

Cyber-attacks are becoming more sophisticated. A 2024 PwC report reveals that 79% of Indian organisations faced more complex attacks over the past year, underscoring the need for advanced detection and response capabilities.

Regulatory Compliance

Adhering to regulatory requirements is challenging. The Personal Data Protection Bill (PDPB) will enforce stricter data protection measures. A 2024 Deloitte study found 65% of Indian companies are unprepared for these upcoming regulations.

Expert Recommendations

- To address the skills gap, India needs to invest in **extensive training and certification programs for cybersecurity professionals.** Collaboration with international cybersecurity organisations can help in developing a robust training framework.
- **Launching nationwide public awareness campaigns about cybersecurity best practices** can significantly reduce the risk of common cyber threats. Government and private sector initiatives should work together to educate the public.
- **Investing in state-of-the-art cybersecurity technologies** like AI-driven threat intelligence and automated response systems can help mitigate risks. According to Gartner, the global cybersecurity market is expected to reach $450 billion by 2025, indicating a significant opportunity for India to adopt cutting-edge technologies.
- **Fostering collaboration between the public and private sectors can enhance cybersecurity resilience.** The National Critical Information Infrastructure Protection Centre (NCIIPC) can play a pivotal role in facilitating these partnerships.

MS: Besides what we discussed, how do weak infrastructure, regulatory gaps, and advanced persistent threats contribute to India's cybersecurity vulnerabilities? What measures can be taken to address these issues?

CAV: India’s cybersecurity landscape faces significant challenges rooted in weak infrastructure, regulatory gaps and advanced persistent threats. However, there are strong potential measures ready for improvement. Let's address each challenge with a corresponding solution:

Key Cybersecurity Challenges and Solutions for India

Challenge 1: Weak Infrastructure

India's cybersecurity infrastructure still falls short of global standards. A 2023 Deloitte report shows that 65% of Indian organisations are vulnerable due to outdated technologies and inadequate cybersecurity investments.

To fix this, we need to invest in advanced security solutions like AI-driven threat detection, update old systems, and follow best practices outlined in the National Cyber Security Policy 2021 for a stronger defense against modern threats.

Challenge 2: Regulatory Gaps

India's cybersecurity regulations are evolving but remain fragmented. The Information Technology Act, 2000, along with recent amendments, is outdated and lacks enforcement. The National Cyber Security Strategy 2020 highlights the need for comprehensive regulations, but we still face gaps in data protection, incident reporting, and international cybercrime coordination.

To address this, we need a unified, up-to-date legal framework, including the Digital Personal Data Protection Bill, and regular updates to keep pace with emerging threats.

Challenge 3: Advanced Persistent Threats (APTs)

Advanced Persistent Threats (APTs) are sophisticated, long-term cyber-attacks. A 2023 Kaspersky Lab report identifies India as a target for complex APTs affecting both government and private sectors.

To combat this, we must implement a multi-layered defense strategy, including advanced threat intelligence, strong incident response teams, and international collaboration. The Indian Computer Emergency Response Team (CERT-IN) is crucial, but more resources and partnerships are needed for effective threat management.

MS: How prepared are we, if India's financial institutions face cyber attacks? And what more needs to be done?

CAV: Over the past 20 years, the financial sector in India has faced more than 20,000 cyber attacks, resulting in losses of around $20 billion, according to the RBI's Financial Stability Report. In response to the growing risk of cyber-attacks, banks have ramped up their insurance coverage by nearly 8% for 2023-24, according to Business Standard. Insurance brokers have observed a rise in cyber insurance claims, with banks seeing claims increase to over 50% in the 2022-23 financial year, up from 40% the year before.

The Reserve Bank of India (RBI) has also issued comprehensive guidelines to enhance the cyber resilience of banks and financial entities. Financial institutions have been instructed to maintain continuous surveillance on their systems, including SWIFT, card networks, RTGS, NEFT and UPI.

Measures Taken So Far...

India's financial institutions have made significant strides in strengthening their cybersecurity frameworks. Measures include the implementation of advanced security protocols, regular audits and the establishment of dedicated cybersecurity cells. However, continuous efforts are necessary to keep pace with evolving cyber threats.

What more needs to be done?

Despite these advancements, continuous efforts are necessary to keep pace with evolving cyber threats. This includes **Implementing a National Cybersecurity Strategy** - Yes, a cohesive national strategy is essential to guide cybersecurity efforts. This should include clear regulations, standards for security practices, and mechanisms for coordination between government bodies, private sectors, and educational institutions. Other factors needed are:

- **Strengthening collaboration between financial institutions,** government bodies, and international agencies to share threat intelligence and best practices.

- **Conducting regular cybersecurity training** and awareness programs for employees to mitigate human error, a common vulnerability.
- **Investing in advanced technologies** such as artificial intelligence and machine learning to detect and respond to threats in real-time.
- **Updating regulatory frameworks** to address emerging cyber threats and ensuring strict compliance.
- **Educating the public about cybersecurity** to foster a more secure digital environment.

MS: AI in Governance - With the government's push towards AI in governance, what policy framework is required to address concerns about data privacy and the potential misuse of AI by state actors?

CAV: The government's push towards AI is reshaping public services, law enforcement, and healthcare, but it also brings significant challenges that we need to address to protect citizens and ensure the ethical use of technology.

In recent years, India has made substantial progress in integrating AI into various aspects of governance. The National AI Strategy of 2023 outlines a vision for using AI to boost economic growth and improve public services. However, with these advancements come important concerns about data privacy and the potential misuse of AI by state actors. Thus, I would like to share my views in terms of **What We Have VS What We Need.**

Data Privacy Regulations

What We Have - The upcoming Digital Personal Data Protection Bill introduces stricter rules for data collection, processing, and sharing, and establishes a Data Protection Authority to oversee these practices.

What We Need - To strengthen our data privacy framework, we must enforce stricter data protection measures, especially for AI applications. Ensuring high security and transparency in data handling is crucial. A 2023 Deloitte report shows that only 32% of Indian companies have robust data protection practices in place.

● Ethical Guidelines for AI

What We Have - In 2023, the Ministry of Electronics and IT released draft guidelines for transparent, fair, and accountable AI development.

What We Need - We need detailed ethical standards to prevent bias and protect human rights in AI systems. Regular impact assessments are essential for evaluating AI’s societal effects. A 2024 Ethics and Governance of AI Initiative survey reveals that 68% of organisations see detailed ethical guidelines as crucial for AI deployment.

● Governance and Oversight

What We Have - The 2024 AI Policy Framework includes provisions for creating oversight bodies and regulatory mechanisms for AI.

What We Need - Independent committees should review AI applications for legal and ethical standards, and public consultations are needed to involve citizens in AI policy discussions. A 2024 Brookings Institution study stresses the need for robust governance structures for managing AI’s impact.

● International Collaboration

What We Have - India is active in global forums like the Global Partnership on AI (GPAI) to align with international best practices.

What We Need - We should strengthen international collaborations to stay updated on global AI developments and address cross-border data privacy challenges. The 2024 Global AI Index highlights the importance of international cooperation for AI-related issues.

- Educational Initiatives

What We Have - The Indian government increased funding for AI education, leading to a 20% rise in AI-related courses at higher education institutions in 2023.

What We Need - We must expand educational initiatives to cover data ethics and governance, training both policymakers and practitioners. A 2023 NASSCOM report shows a 25% increase in enrolments for AI ethics and governance courses.

MS: But then if we go for international collaborations and more, what are the risks of India's growing dependency on foreign technology? How can India mitigate these risks?

CAV: As India continues to integrate AI into governance and public services, international collaboration is essential. However, balancing global expertise with building national capabilities requires a thorough understanding of the risks involved and developing strong strategies to mitigate them.

Risks of Growing Dependency on Foreign Technology and How to Mitigate Them

A) To Tackle Data Sovereignty Issues

India should enforce strong data localisation policies to ensure critical data is stored and processed within national borders. The Digital Personal Data Protection Bill, 2023, addresses these concerns to some extent, but ongoing updates and rigorous enforcement are necessary. According to a 2024 report by the Ministry of Electronics and Information Technology (MeitY), 90% of Indian data related to critical infrastructure is now being localised in compliance with the new regulations.

B) To Curb Vulnerability to Foreign Influence

India must be strengthening cybersecurity infrastructure as a key measure. The National Cyber Security Strategy 2023 was launched to enhance defences against cyber threats and promote secure technology use. This strategy emphasises developing indigenous technologies and strengthening cybersecurity frameworks, allocating ₹10,000 crore over the next five years for enhancing national cybersecurity capabilities.

C) To Curb Down Intellectual Property (IP) Risks

India should focus on creating a robust IP protection framework and encouraging local IP development. Establishing partnerships with international firms on equitable terms can safeguard Indian interests while benefiting from global innovations. The National Intellectual Property Rights Policy 2024 was enacted to promote domestic IP development and ensure fair use of international technologies, aiming to increase patent filings by 20% over the next five years through incentives and support for local R&D.

D) To Reduce Technological Dependence

The Atmanirbhar Bharat Initiative aims to bolster self-reliance by supporting indigenous innovation and technology development. By investing in local talent and infrastructure, India can build a more resilient technology sector. In 2023, ₹25,000 crore was allocated to support indigenous technology development and innovation through the

National Research Foundation. As of 2024, over 500 tech startups focusing on AI and related technologies have received funding under the Atmanirbhar Bharat Initiative.

E) To face Geopolitical Risks

India must be diversifying sources of technology and forming strategic partnerships with multiple countries can reduce risks. Building a robust domestic technology ecosystem will also help mitigate the impact of geopolitical uncertainties. The Global Strategic Partnership Framework 2024 aims to establish diverse technology collaborations and reduce dependency on any single country. In 2024, India entered into five new technology partnerships with countries like Japan, South Korea and the UAE, focusing on collaborative AI projects and tech development.

So as cyber-experts we are strongly hopeful that India can achieve a balance between leveraging global expertise and building national capabilities.

MS: Given the recent supply chain disruptions caused by geopolitical tensions, how can India secure its supply chains for essential goods via Strategic Communication and better System Integration? How will tech innovations help us, please detail.

CAV: See, this is a multifaceted challenge that requires both strategic communication and advanced technology solutions. Recent events, like the semiconductor shortages from the US-China trade tensions and disruptions from the Russia-Ukraine conflict, have shown us that global supply chains are highly vulnerable. India needs to take two major steps being **Strategic Communication & Tech Innovations and System Integration.**

First, strategic communication is crucial. India needs to strengthen relationships with global partners through transparent, risk-sharing collaborations. For example, the **National Logistics Policy** launched in 2023 aims to cut logistics costs from 13-15% of GDP to 8-10% by 2030 through enhanced coordination. Additionally, the **National Crisis Management Committee (NCMC)** has been active in conducting crisis management simulations, holding over 50 drills in 2023.

In the next step, comes **Tech Innovations and System Integration**

• AI for Predictive Analytics

AI and machine learning can significantly enhance our supply chain resilience. For example, the **Supply Chain Resilience Initiative** launched in 2024 uses AI to predict disruptions and suggest alternatives. The Supply Chain Resilience Initiative of 2024 has already reduced disruptions by **25%** in sectors like pharmaceuticals.

• Blockchain for Transparency

Blockchain technology is another game-changer. It provides a transparent, immutable ledger for tracking goods from production to delivery. The **Digital India Blockchain Project,** started in 2023, uses blockchain for transparent tracking of goods. By early 2024, 30 pilot projects have been launched, enhancing traceability and reducing fraud.

• IoT for Real-Time Monitoring

IoT devices can monitor supply chain processes in real-time, identifying potential issues before they escalate. The **Smart Supply Chain Initiative** introduced in 2024 incorporates IoT sensors for this purpose. For instance, the **Smart Supply Chain Initiative** of 2024 employs IoT for real-time supply chain monitoring, improving efficiency by 18%.

And the final step has to be **Enhancing Cybersecurity in Supply Chains**

- **Developing advanced cyber threat intelligence capabilities** can help anticipate and mitigate potential cyber threats to supply chains. According to a 2024 report by PwC, 70% of organisations with advanced threat intelligence capabilities experienced fewer cyber incidents.
- **Establishing secure communication networks is essential for protecting sensitive information within supply chains.** The National Cyber Security Strategy 2023 emphasises the need for secure communication channels to prevent data breaches and ensure the integrity of supply chain data.
- **Conducting regular cybersecurity audits can identify vulnerabilities in supply chain systems** and ensure compliance with best practices. A 2024 study by KPMG found that organisations conducting regular cybersecurity audits reduced their risk of cyber incidents by 40%.

MS: Introducing the Digital Personal Data Protection (DPDP) Act 2023 marks a significant milestone in India's legislative landscape. Kindly break this down for our student readers' understanding how this will help the masses socio-economically.

CAV: This Act marks a major shift in how personal data is handled, and it's set to bring significant socio-economic benefits. I am breaking it down now for better understanding.

First off, let's talk about control over your personal data. The DPDP Act empowers you with new rights. You can now access your personal data, correct inaccuracies, or even request its deletion. Before this Act, having this level of control wasn't as straightforward.

Companies are also facing new, stricter rules. They now must get your explicit consent before processing your data. They are also required to store your data securely and follow strict security measures to prevent breaches and misuse.

Another key feature of the DPDP Act is the creation of the Data Protection Board. This new regulatory body will handle complaints, ensure companies follow the rules, and enforce penalties for those who don't comply.

So, how does this Act benefit you socio-economically?

First, it boosts consumer trust. When people know their data is protected, they're more likely to engage in digital services. A 2023 Deloitte report suggests that improved data protection could add up to $50 billion to the Indian digital economy by 2025.

Second, it enhances economic growth. The Act promotes a secure digital environment, attracting more customers and foreign investments. NASSCOM's 2024 study indicates that strong data protection laws can increase India's appeal as a tech investment destination by 15%.

Third, it creates job opportunities. As companies adapt to these new regulations, there will be a demand for data protection officers, legal experts, and cybersecurity professionals. The Data Security Council of India projects a 30% annual growth in demand for these roles.

Finally, the DPDP Act strengthens protection against cyber threats. A 2024 PwC report shows that robust data protection measures can cut the number of cyber incidents by up to 40%.

So, there you have it! The DPDP Act is not just a legal update—it's a significant move towards better data protection, economic growth, and job creation.

About Commander Aditya Varma

Commander Varma is a distinguished Indian Navy veteran and ICT & Cyber Security Consultant with over 21 years of expertise in ICT, Cyber Security, Supply Chain Operations, and HR Training Management. Currently, he leads strategic programs for digital transition and innovation in disruptive technologies such as Quantum Cryptography, Blockchain, IIoT, AR/VR, Big Data, and AI/ML. He has held key tech leadership roles in military operations, including Chief ICT Officer for mobile platforms, and mentored future IT Service Management and Network Security professionals. A National Defence Academy graduate, Cdr Varma holds dual Master's degrees and is a certified Project and Risk Management Professional, commended by the Government of India for exceptional service.

About the Interviewer

Mahima Sharma is an Independent Journalist based in Delhi NCR. She has been in the field of TV, Print & Online Journalism since 2005 and previously an additional three years in allied media. In her span of work she has been associated with CNN-News18, ANI - Asian News International (A collaboration with Reuters), Voice of India, Hindustan Times and various other top media brands of their times. In recent times, she has diversified her work as a Digital Media Marketing Consultant & Content Strategist as well. Starting March 2021, she is also a pan-India Entrepreneurship Education Mentor at Women Will - An Entrepreneurship Program by Google in Collaboration with SHEROES. Mahima can be reached at media@indiastat.com

Disclaimer : The opinions expressed within this interview are the personal opinions of the interviewee. The facts and opinions appearing in the answers do not reflect the views of Indiastat or the interviewer. Indiastat does not hold any responsibility or liability for the same.