6 | Trust: The security and justice imperative

Building a secure and just future for India, where trust forms the foundation of cyber defences, transparent policies, advanced tech and equitable access to justice, is essential for protecting its growing digital economy, ensuring national security and promoting social equity.

In a world that is becoming more digitally connected, trust is now the cornerstone of justice and security. Maintaining trust in our digital spaces and legal systems is essential as technology transforms almost every part of our lives. Public confidence in the institutions in charge of national security, governance and equitable access to justice is based on trust, which supports individual safety and privacy. This important idea is examined in the four chapters under *Trust: The security and justice imperative,* which provide guidance on establishing and preserving trust in both the legal and digital spheres.

Strong cyber defences are essential to national security as cyberthreats become more sophisticated. The chapter, *Securing the nation's cyber defence and strengthening connectivity,* includes the key takeaways from a panel discussion on *Fortifying Digital Infrastructure – Elevating Cyber Defence for a Secure, Resilient and Vibrant Nation.* Various leaders also speak on *Building a Secure and Viksit Bharat.*

The chapter, *Designing trust-first policies,* includes a *Manthan* on Building trust with Sovereign Cloud – *Policy, Technology and Strategy.* This chapter delves into the importance of creating transparent, accountable policies that protect user data and privacy, emphasizing that sovereign cloud ecosystems enable compliance with local regulations and enhance overall data sovereignty. The *chapter on Decoding and optimising modern SoCs* comprises a *Manthan* on demystifying modern SoCs in hybrid and hyperconnected environments. This chapter examines how optimising SoCs for security, reliability and efficiency can strengthen device performance while protecting sensitive data.

The chapter on *Ensuring fair and timely justice for all* covers two sessions. In the first session, the Honourable Minister of State (IC) for Law & Justice, Arjun Ram Meghwal, speaks on the story of transforming law and justice in Digital India. The second is a *Manthan* on envisioning a user-centric justice system. Both sessions discuss strategies for ensuring accessible, transparent and timely justice.

All four chapters offer a comprehensive guide to building a trust-based foundation in security and justice.

6a. Securing the nation's cyber defence and driving sustainable growth

Lieutenant General
N. S. Raja Subramani
PVSM, AVSM, SM, VSM,
Vice Chief of Army

Rajendra Kumar
Secretary (Border Management),
Ministry of Home Affairs,
Government of India

Cybersecurity and self-reliance in defence are pillars of a strong Bharat, ensuring safety, sovereignty and sustainable growth.

India's journey to becoming a secure, resilient and digitally empowered nation hinges on a strong commitment to cybersecurity and self-reliance in defence. As digital infrastructure expands, this rich landscape also faces evolving cyberthreats. This, in turn, necessitates the urgency of high-quality defence mechanisms to protect India's digital economy and safeguard sensitive citizen data. At the heart of that nation's fortified digital framework are initiatives such as zero-trust cybersecurity models and AI-driven threat detection, which provide proactive, rapid responses to dynamic threats.

This also highlights the roles of citizens and cross-sectoral collaborations in building an enduring digital environment, with multi-stakeholder efforts such as the National Cybercrime Reporting Portal (NCRP) and the Indian Cybercrime Coordination Centre (I4C) being instrumental building blocks for a resilient digital ecosystem.

Furthermore, India's drive towards self-reliance in defence, rooted in indigenous manufacturing and technological advancement, is also crucial. India's advancements in geospatial intelligence and real-time data analytics for enhanced border security and disaster response are all made possible through PPPs. By reducing foreign dependencies through homegrown defence production, India strengthens both its sovereignty and national security. Taken together, these projects collectively create the image of a technologically advanced and resilient Bharat ready to lead the world.

Leaders Speak: Building a Secure Bharat, A Viksit Bharat
Speakers:
Lieutenant General N. S. Raja Subramani, PVSM, AVSM, SM, VSM, Vice Chief of Army; Dr Rajendra Kumar, Secretary (Border Management), Ministry of Home Affairs, Government of India

Moderator:
Anthony Crasto, President, Assurance, Deloitte South Asia

Digital security is the backbone of a resilient, self-reliant India, driving the nation forward to *Viksit Bharat 2047.*

As India rapidly expands its technological capabilities, the integration of advanced technologies is key to protecting borders, enhancing internal security and supporting disaster management.

Directing the nation's defence sector towards self-reliance and augmenting strong cyber defence measures are necessary to protect the sovereignty of the country as well as safeguard the interests of its citizens. These strategic initiatives and technological advancements were discussed by Lieutenant General N.S. Raja Subramani and Dr Rajendra Kumar in this special panel. Over the course of this discussion, both speakers highlighted the importance of indigenisation, cybersecurity, data management and PPPs in building a secure Bharat.

Integrating AI and advanced technologies in defence and security

AI empowers our armed forces to make rapid, informed decisions, ensuring that India remains secure in an increasingly complex world.

Lieutenant General N. S. Raja Subramani
PVSM, AVSM, SM, VSM, Vice Chief of Army

As India's defence sector continues to build an effective digital arsenal, AI-driven solutions for optimising decision-making and real-time surveillance have also seen integrated usage. Just as the government has integrated AI into logistics and health monitoring systems in other sectors, AI-based solutions' capacity to process vast amounts of data allows them to power novel military systems, including those used for autonomous weaponry and strategic operations. Emphasizing the role of data centres, esteemed Lt. General Subramani noted the importance of secure data processing to facilitate faster, informed decisions in critical scenarios.

The use of geospatial intelligence further enhances India's security framework. Real-time satellite imagery, drones and remote sensing technologies provide precise situational awareness in disaster-prone areas and border regions, where threats such as smuggling and infiltration are common. These advanced technologies, combined with real-time monitoring systems, enable the Indian defence forces to proactively address both internal and external security challenges.

Strengthening cybersecurity

From zero-trust cybersecurity to sovereign data clouds, India's secure digital infrastructure is a model of resilience and strategic foresight.

With digital expansion comes an increase in cyberthreats, and cybersecurity is now considered essential for a secure Bharat. Embracing a zero-trust policy for cybersecurity, India's strategy includes securing government systems on sovereign clouds and establishing multiple Centres of Excellence (CoE) in collaboration with leading academic institutions, such as IIT Delhi and IIT Madras. The I4C plays a central role, providing a framework for coordinating cyber defence across federal and state agencies and supporting real-time response to cyber incidents.

The creation of platforms such as the NCRP enables citizens to report incidents while multi-stakeholder teams respond rapidly to mitigate risks. This infrastructure, combining public and private expertise, ensures that India's digital ecosystem remains secure and resilient in the face of evolving cyberthreats.

Data as a strategic asset

Data is the new strategic asset, and sovereign cloud infrastructure is crucial for safeguarding sensitive information and supporting real-time intelligence.

Dr Rajendra Kumar
Secretary, Border Management, Ministry of Home Affairs, Government of India

Recognising that data is the new oil, the Indian government has implemented sovereign cloud infrastructure to securely store and process government data. Data analytics plays a critical role in intelligence gathering, especially in military operations where quick, accurate insights are essential. For instance, real-time data analysis enables better responses to border threats and improves efficiency in handling large-scale operations. The integration of Augmented Reality/Virtual Reality (AR/VR) networks and dedicated data centres across the armed forces enhances data accessibility, reduces redundancy and enables coordinated action among military branches.

A secure Bharat is the foundation of a Viksit Bharat. By combining technological innovation, cyber resilience and self-reliance in defence, we are shaping a future where national security and digital empowerment go hand in hand.

Anthony Crasto

Moreover, real-time data processing across departments and quick integration with other security agencies ensure India's defence system remains agile and responsive, effectively addressing threats at every level.

Advancing indigenisation in the defence sector

A self-reliant defence sector is vital for national security. "Design, Develop and Make in India" is more than just a slogan; it's our roadmap to resilience.

India's self-reliance in defence is fundamental to maintaining national security and reducing dependence on foreign sources for military equipment. The government is working with MSMEs and academic institutions to bolster indigenous manufacturing capabilities. Through PPPs, defence projects such as Tejas aircraft development and indigenous drone manufacturing are gaining momentum. This focus on "Design, Develop and Make in India" aligns with the broader vision of a self-sufficient defence sector, which includes establishing incubation centres and CoEs dedicated to R&D in defence technologies.

As stressed previously, indigenisation supports national security, creates a robust defence ecosystem, expanding manufacturing bases and ensuring that India can maintain and enhance its defence capabilities independently.

Panel: Fortifying Digital Infrastructure – Elevating Cyber Defence for a Secure, Resilient and Vibrant Nation

Participants:

Laxmi Singh, Commissioner of Police, Gautam Buddha Nagar, Government of UP; Dr Amit Sharma, Advisor (Cyber) and Additional DG, Office of Secretary, Department of Defence (R&D), Ministry of Defence; G Narendra Nath, Joint Secretary, NSCS

Moderator:

Gaurav Shukla, Partner, Deloitte India

A resilient digital infrastructure is the backbone of a secure, inclusive and future-ready India.

In today's digital age, a secure and resilient cyber infrastructure is foundational to India's ambition of becoming a US$1 trillion digital economy. India has witnessed exceptional growth in its Digital Public Infrastructure, with notable achievements such as Aadhaar, the world's largest biometric system, and UPI, a widely used instant payment system. These advancements have propelled the country into the digital age, driving greater connectivity, promoting inclusivity and improving service delivery across the nation.

With this context in mind, however, it is still important to remember that cybersecurity is no longer just a technical issue. It represents a cornerstone of national resilience that impacts every facet of society, ranging from citizen safety to economic health. That is why it is crucial to fortify digital infrastructure by using a full understanding of what good defence systems need across critical sectors. Initiatives such as *Cyber Surakshit Bharat* play a vital role in enhancing the security and resilience of the nation's digital framework. When these are paired with enhanced digital literacy and collaborative PPPs to protect and empower citizens in an increasingly digital landscape, only then can the nation advance to realise its vision of *Viksit Bharat 2047.*

Expanding cyber defence across critical sectors

Each sector has unique vulnerabilities, and cybersecurity protocols must be tailored to address them effectively.

G Narendra Nath
Joint Secretary, NSCS

From telecom to financial services and beyond, robust cybersecurity protocols must be upheld for every sector that operates in India's burgeoning digital ecosystem. This translates to implementing secure-by-design principles in system architecture, adopting a zero-trust model across devices and networks and fortifying systems against Advanced Persistent Threats (APTs).

A notable solution that can assist in this regard is the National Malware Repository. This initiative uses AI-based threat detection capabilities and provides organisations with insights into malware trends and preventative measures across various operating systems and platforms. This collaborative tool is essential for national security, allowing public and private agencies to strengthen their defences against the rapidly evolving cyberthreat landscape.

Collaborative PPPs for enhanced cyber resilience

An effective response to cyberthreats requires strong collaboration between government, industry and academia. Achieving this requires critical PPPs for intelligence sharing, capacity building and the development of advanced cybersecurity solutions.

A cyber-aware society begins with every individual being equipped with the knowledge to recognise and report risks.

Laxmi Singh
Commissioner of Police, Gautam Buddha Nagar, Government of UP

Through joint initiatives such as CENCOPS (a fusion centre integrating data across 112 emergency systems, forensics and law enforcement), India can enhance real-time response capabilities and strengthen data integrity across critical systems. By using resources and expertise from both sectors, these collaborations aim to provide a robust defence structure that can scale alongside India's digital growth.

Building a digitally literate and cyber-aware society

Building a secure digital society depends on citizens being digitally literate and aware of cyberthreats. To this effect, "cyber hygiene" is an important educational front that must be taught, encouraging users to remain vigilant and report suspicious activity when identified.

Initiatives such as the *Chakshu Portal* empower citizens to report cyber fraud in real time, increasing awareness and helping law enforcement agencies identify emerging threats quickly. Additionally, simplifying processes for citizens to recognise trusted sources, such as standardised bank URLs and SMS codes, minimises risks and enhances public trust in digital interactions.

Adopting AI-driven solutions and advanced technologies

Traditional security approaches have become obsolete in the present cyber landscape. Our response systems and next-generation technologies need agility to combat sophisticated threats. With digital boundaries extending beyond office premises to remote workplaces and devices, security paradigms must adapt accordingly. As cybercriminals increasingly use sophisticated tools, the role of AI in cybersecurity becomes paramount. AI-driven solutions allow for rapid detection of anomalies and predictive analysis, helping organisations anticipate and mitigate threats before they escalate.

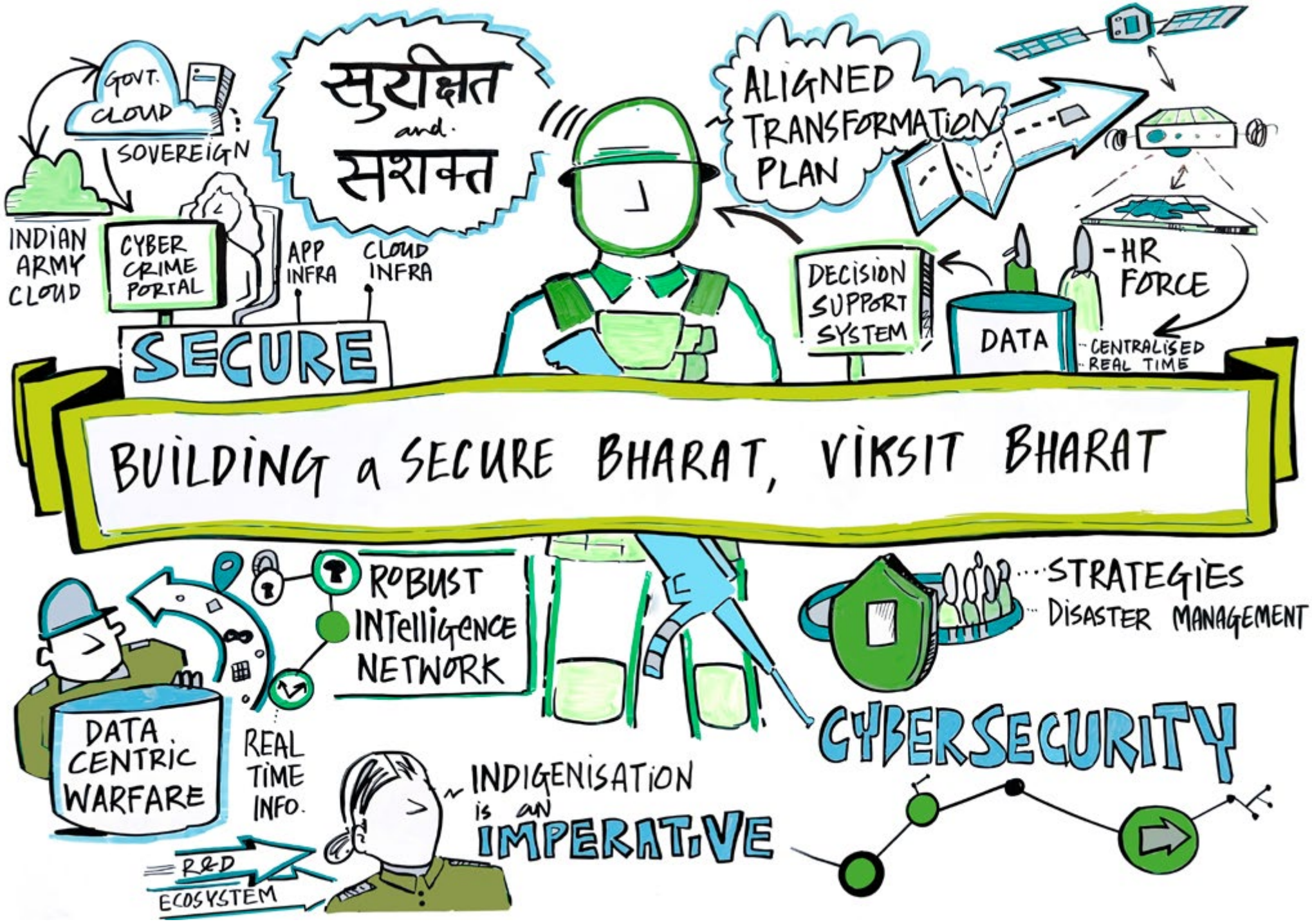
By opting for AI-based endpoint protections and zero-trust architecture for digital assets, only verified users and devices can access vital data, even within internal systems. The integration of AI with other advanced threat monitoring tools can provide a proactive, as opposed to reactive, defence posture against complex cyberattacks on critical infrastructure.

Technology is never good or bad. It's the application. Somebody uses it incorrectly, but the same technology can still be used for positive purposes.

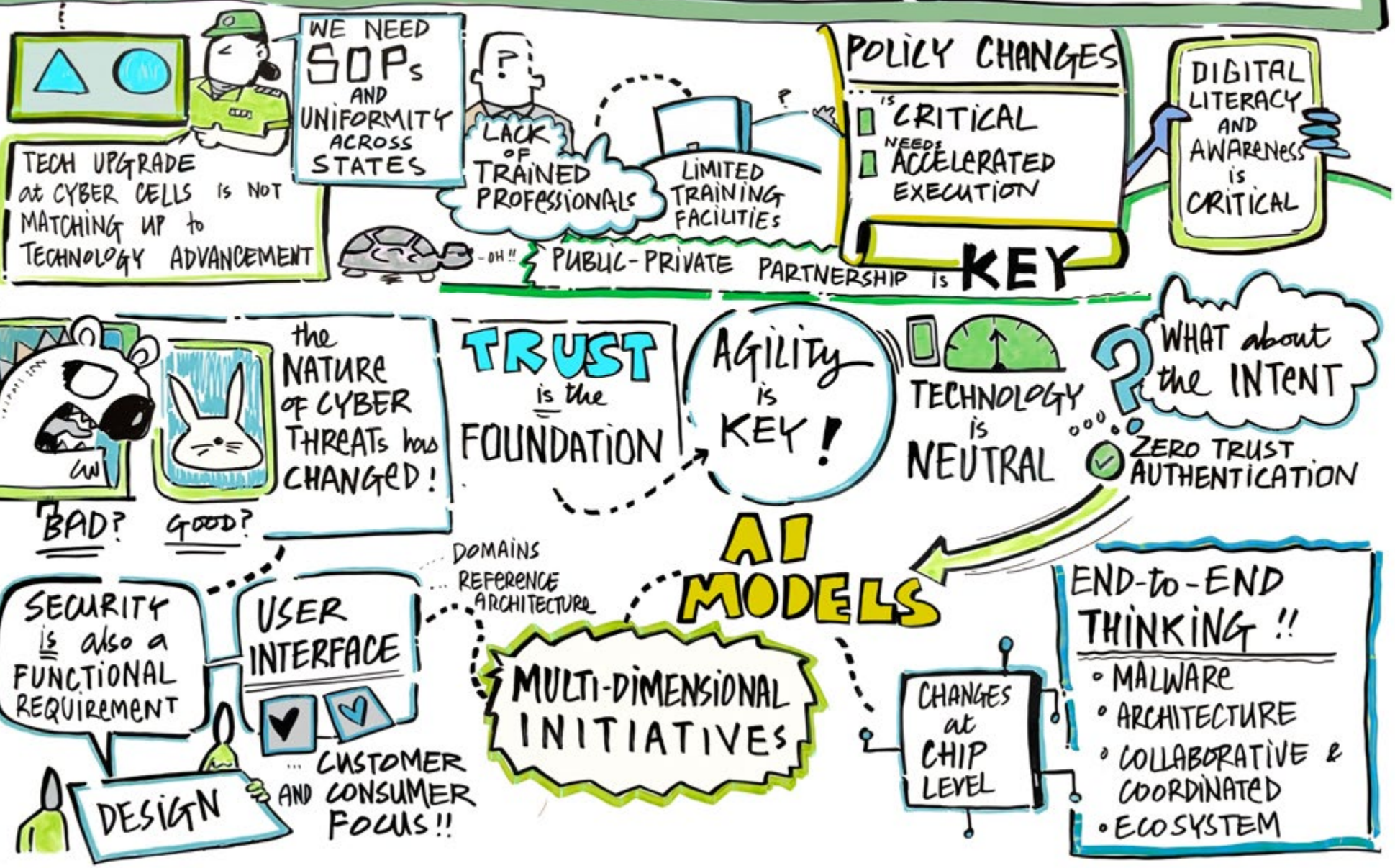
Dr Amit Sharma
Advisor (Cyber) and Additional DG, Office of Secretary, Department of Defence (R&D), Ministry of Defence

Key takeaways

- **Sector-specific cybersecurity measures:** Each sector needs to implement unique protocols, from zero-trust models to malware detection repositories, to address specific vulnerabilities and bolster national cybersecurity resilience.
- **PPPs and intelligence sharing:** Collaborative initiatives such as CENCOPS enhance real-time response and data integrity, fostering a robust defence framework through shared resources and expertise.
- **Digital literacy and public cyber awareness:** Educating citizens on cyber hygiene and simplifying the recognition of legitimate digital interactions, such as secure bank SMS codes, is essential for reducing vulnerabilities and empowering users.
- **AI-driven threat detection and zero-trust architecture:** Integrating AI into cybersecurity, including endpoint protection and anomaly detection, offers proactive protection, allowing India to stay ahead of advanced cyberthreats.
- **Security-by-design in system design:** Embedding security as a functional requirement in digital systems ensures a security-by-design architecture, establishing a foundation of trust and resilience from the ground up.
- **AI-driven defence and surveillance:** AI is integral to modern defence, enhancing decision-making, real-time monitoring and logistics, allowing India's armed forces to maintain a strategic advantage.
- **Data sovereignty and real-time analytics:** Secure data storage and real-time analytics on sovereign cloud platforms enable faster, data-driven decisions crucial for national security.
- **Indigenisation and PPPs:** Promoting indigenous defence manufacturing through PPPs reduces foreign dependency and fosters a resilient domestic defence ecosystem.
- **Geospatial intelligence for security and disaster management:** Using geospatial technology enhances situational awareness across border security and disaster management, ensuring a proactive approach to both natural and human-made threats.


GOVT. CLOUD
SOVEREIGN
INDIAN ARMY CLOUD
CYBER CRIME PORTAL
APP INFRA
CLOUD INFRA
SECURE
सुरक्षित and सशक्त
ALIGNED TRANSFORMATION PLAN
DECISION SUPPORT SYSTEM
DATA
HR FORCE
CENTRALISED REAL TIME
BUILDING a SECURE BHARAT, VIKSIT BHARAT
ROBUST INTELLIGENCE NETWORK
DATA CENTRIC WARFARE
REAL TIME INFO.
R&D ECOSYSTEM
INDIGENISATION is an IMPERATIVE
STRATEGIES
DISASTER MANAGEMENT
CYBERSECURITY

FORTIFYING DIGITAL INFRA: ELEVATING CYBER DEFENCE FOR A SECURE, RESILIENT AND VIBRANT NATION



6b. Designing trust-first policies

Distributed Cloud AirGap is a pioneering solution that combines cloud power with complete ownership and control for enterprises.

Trust is a fundamental element of governance in the digital age. As governments rely on digital technologies to enhance public services and improve citizen satisfaction, ensuring the protection and sovereignty of national digital systems is paramount. At the heart of this digital transformation lies the concept of a sovereign cloud, a technology framework that allows nations to retain control over their data, software and operations.

Manthan: Building Trust with Sovereign Cloud – Policy, Technology and Strategy

Participants:

Kshitij Kushgra, Scientist, MeitY; Brigadier S Balakrishnan, Army (MoD); Colonel Nishant Rathee, Army (MoD); Amrish Kohli, Google Cloud; Kapil Kapoor, Google Cloud; Vinamra Jain, Google Cloud; Mohit Gulati, Google Cloud.

Gurus:

Amit K Singh, Partner, Deloitte India; Ritesh Pal, Partner, Deloitte India

During the *Manthan,* "Building Trust with Sovereign Cloud," experts from industry, government and technology came together to explore the role of sovereign cloud in shaping India's digital future. They emphasized the importance of trust-first policies underpinned by cloud sovereignty to safeguard sensitive data and ensure the success of India's digital transformation.

Data sovereignty: A necessity in today's cloud solutions

Data sovereignty was a recurrent theme in the session. With ever-escalating data privacy and cybersecurity threats, keeping sensitive information within national borders has become non-negotiable. Data-sensitive entities, such as defence and government, are especially focused on maintaining control over data for security reasons. The sovereign cloud solution presented by Google Distributed Cloud (GDC) addresses this need by offering an environment where data

Data sovereignty goes beyond security; it ensures that critical national assets remain within the control of the nation.

remains within the country's borders, with no external access or transfers. By combining the strengths of a public cloud with the operational independence of a sovereign cloud, GDC provides the flexibility and control that sensitive industries require.

Software sovereignty and the open-source approach

Unlike data sovereignty, which ensures ownership of critical information, software sovereignty seeks to minimise reliance on certain systems. The session speakers explained how hyperscalers (large cloud service providers) often lock their customers into using their software.

Software sovereignty is about having the freedom to choose and control the technology stack that best serves your mission without being locked into a single provider.

Ritesh Pal

This becomes a problem when the goal is to enable independent process automation for some specific functions, especially in governments and defence sectors.

To address these concerns, Google has introduced the use of open-source software within its GDC solution. This approach allows organisations to run their operations without being tied to a specific provider's proprietary technology. GDC ensures that organisations can manage their workloads independently without relying on third-party vendors for critical updates or maintenance.

The influence of geopolitical risks on cloud adoption

As the global geopolitical landscape becomes more volatile, the dependence on foreign cloud service providers for sensitive and critical applications is apprehensive. The session emphasizes the necessity of operational sovereignty, which goes beyond merely owning data and software.

In today's geopolitical climate, survivability and control over mission-critical workloads are paramount. We cannot afford to be reliant on external forces when national security is at stake.

Amit K Singh

Google's GDC solution, particularly its AirGap component, is designed to mitigate these risks. The AirGap system operates entirely offline, isolated from the public internet, ensuring that even the most sensitive operations are carried out securely within national borders. This feature is critical for defence and government agencies, as it guarantees that their operations remain shielded from external geopolitical pressures.

The power of GDC and Vertex AI

The session also introduced participants to the advanced capabilities of the GDC solution, particularly its integration with Vertex AI. This AI-driven functionality allows organisations to process large amounts of data on-premises, ensuring that critical data is analysed securely and efficiently.

This synergy of advanced AI with secure cloud networks enables organisations to have the solutions they need in the new context of a data-oriented environment. Whether analysing videos, translating text or using AI, the GDC solution enables sensitive industries to harness these opportunities while having full control over their operations.

Modularity and flexibility: Addressing the integration challenge

One major theme of the session was tackling the challenge of integrating sovereign cloud solutions with current systems. For many organisations, the fear of vendor lock-ins and the complexity of integrating new solutions into legacy systems can be significant barriers to cloud adoption.

Google's solution to this problem lies in its modular and flexible architecture. The GDC platform is designed to easily integrate with existing systems, allowing organisations to scale their operations without being locked into a specific provider's ecosystem. By offering a modular approach, GDC empowers organisations to adopt new technologies and expand their operations without costly overhauls or vendor dependencies.

We are addressing the interoperability challenge by making solutions modular and open, allowing easy integration and expansion.

Achieving a future of innovation and sovereignty

In conclusion, as organisations in highly regulated sectors continue to navigate the complexities of cloud adoption, sovereign cloud solutions, such as GDC, are becoming increasingly essential. The insights shared during the *Manthan* make it clear that building trust with sovereign cloud solutions is a strategic and practical necessity in today's geopolitical landscape.

Tailored cloud solutions are essential as they balance regulatory compliance, operational control and cutting-edge technology to drive secure, mission-critical workloads forward.

As India continues to innovate and adopt new digital solutions, the role of trust-first policies will become even more critical. By prioritising sovereignty, transparency and accountability, India is securing its digital future and setting a global standard for digital governance.

Key takeaways

- **Sovereign cloud solutions are essential for regulated sectors:** Sovereign cloud platforms, such as GDC, are vital for industries dealing with sensitive data. By ensuring that data and operations remain within national borders, these solutions offer the control needed to protect critical workloads.
- **Open-source software reduces vendor lock-in:** By using open-source software, organisations can maintain control over their technology stack without being tied to proprietary systems. This flexibility is critical for sectors that require full autonomy.
- **Geopolitical risks demand operational sovereignty:** In an unpredictable geopolitical environment, organisations must ensure that they can operate independently. GDC's AirGap technology provides the operational sovereignty needed for secure, mission-critical operations.
- **Modular and flexible cloud infrastructure:** Google's GDC platform addresses the challenge of integration by offering a modular approach that allows organisations to scale and evolve their operations without vendor lock-in.

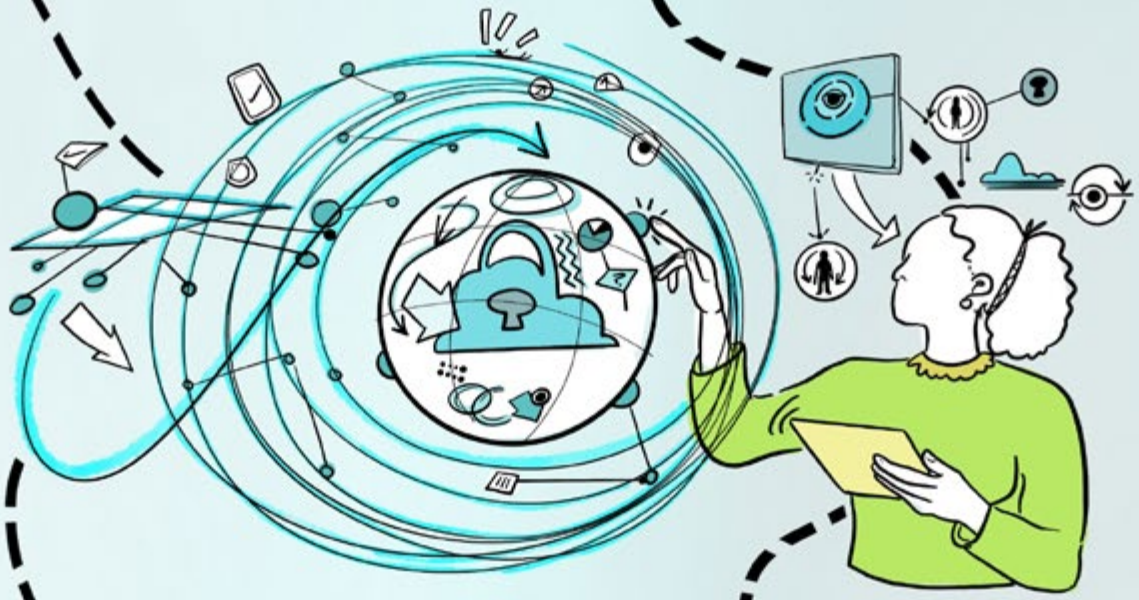
BUILDING TRUST WITH SOVEREIGN CLOUD POLICY, TECHNOLOGY AND STRATEGY

SOVEREIGN CLOUD SOLUTION FOR GOVERNMENT

- FOR REGULATED INDUSTRIES SUCH AS DEFENCE
- GDC - SECURED AND CONTROLLED ENVIRONMENT
- AIR-GAPPED INFRASTRUCTURE AND OPEN-SOURCE SOFTWARE

ADDRESSING INTEROPERABILITY CHALLENGES

- NEED FOR OPEN STANDARDS AND PROTOCOLS
- TRAINING AND DEVELOPMENT
- INITIATIVES SUCH AS CNAPS AND GOJI



MAKE IN INDIA AND SECURITY

- REDUCED DEPENDENCY ON FOREIGN SUPPLIERS
- INTEGRATING LOCALLY-SOURCED COMPONENTS VIA GOOGLE

BALANCING INNOVATION WITH CONTROL

- TRADE-OFFS BETWEEN USING ADVANCED TECHNOLOGIES AND CONTROL OVER DATA AND OPERATIONS

6c. Decoding and optimising modern SOCs

Robust SOCs combine technology, skilled employees and advanced processes to handle the complexities of modern cybersecurity.

With the rapid digitisation globally, strong cybersecurity measures have also grown in importance. Entities in the public sector, charged with sensitive data and critical operations, are increasingly coming under cyberattacks. Complex threats, particularly those backed by states and using AI, are on the rise, making traditional Security Operations Centres (SOCs) increasingly insufficient.

In particular, the rapid growth of India's DPI has positioned it as the second-largest mobile and internet market worldwide. As a result, governments will adopt technologies such as cloud computing, Operational Technology (OT) and Industrial Control Systems (ICS), requiring modern SOCs to adjust their techniques to protect these highly connected environments against targeted threats.

Manthan: Demystifying Modern SOCs in Hybrid and Hyperconnected Environments

Participants:

Dr M. K. Sharma, Group Captain, Indian Air Force; Kamal Kumar Agarwal, DDG (Quantum Tech), TEC, Department of Telecom; Bhupesh Janoti, Senior Programme Manager, Data Security Council of India (DSCI); Vineet Kshirsagar, Palo Alto (Alliance); Ankush Charagi, Palo Alto (Alliance); Brig. N. R. Pandey, Indian Army; Manish Anand, Indian Army; Lt Col S. Anirudha Rao, Indian Army; Shaleen Khetarpal, CISO, BSES; Sunil Kumar, CISO, Power Grid Corporation of India Limited; Sanjay Kumar, CISO, IREDA; Col Nishant Rathee, Indian Army; Brig. S. Balakrishnan, Indian Army.

Gurus:

Gaurav Shukla, Partner, Deloitte India; Anand Tiwari, Partner, Deloitte India

This *Manthan* brought together Deloitte and other industry experts for a compelling discussion on the complexities, components, challenges and strategies shaping the evolution of SOCs in India's digital ecosystem.

The changing landscape of cybersecurity

The traditional SOC model was designed for a simpler IT environment, but the integration of cloud, OT and ICS has introduced a complex threat landscape. Public sector organisations now handle vast amounts of sensitive data, including data from biometric systems and national digital payment platforms. India processes one of the highest volumes of digital payment transactions globally, making it a prime target for cybercriminals.

Today, SOCs must defend against APTs and state-sponsored cyberattacks. Experts from the DSCI emphasize that the modern digital infrastructure demands SOCs capable of monitoring real-time data and integrating advanced technologies for threat detection and response. Neglecting to act leaves our infrastructure at risk, as the costs of recovering from catastrophic cyberattacks are significantly

higher than the minimal investment required by cybercriminals to launch such attacks.

Core components of a modern SOC

A modern SOC must go beyond securing IT systems; it must also integrate cloud platforms, OT devices and physical security systems. Key components include the following:

- **Comprehensive log ingestion and monitoring:** With the growing diversity of systems, SOCs must ingest data from multiple sources, such as the cloud, OT and ICS, to maintain a complete view of security events. Real-time monitoring is essential to identify unauthorised access or anomalous behaviours.
- **Advanced threat intelligence and incident response:** AI-powered threat intelligence allows SOCs to anticipate potential attacks and respond rapidly. Automation of routine tasks enables faster and more accurate detection and mitigation, improving overall SOC efficiency.
- **Automation and AI integration:** Automation is critical for managing large volumes of security data. AI-driven systems can sift through security logs, flag potential risks and trigger initial response actions, allowing employees to focus on strategic decision-making.
- **Skilled workforce:** A skilled workforce is essential despite the rise of automation. SOC teams must stay updated on evolving cyberthreats and technologies. Continuous learning is necessary to manage complex hybrid environments and use AI effectively.

Air-gap networking in high-security environments

Air-gapped networks offer protection but require vigilant monitoring to prevent breaches through vendor systems or indirect connections.

Air-gapped networking is often used in highly sensitive environments, such as government or industrial operations, where systems are physically isolated from external networks. While this creates a robust layer of protection, air-gapped systems are not immune to breaches. This was highlighted by the case of a European utility company with air-gapped infrastructure. The company experienced a severe cyberattack when a vendor's laptop, temporarily connected for troubleshooting, became the entry point. The breach demonstrated the vulnerabilities that exist, even in supposedly isolated systems.

Additionally, modern adversaries may exploit physical methods, such as USB malware or wireless attacks, via drones, making it necessary to monitor air-gapped environments with the same vigilance as interconnected ones. Strong policies, regular auditing and endpoint visibility are essential to managing these risks. Even air-gapped systems require layered defences and comprehensive monitoring to ensure security.

Integration with broader cybersecurity frameworks

Modern SOCs must collaborate across departments and with external stakeholders, particularly in government entities where coordination is crucial. Public sector organisations often manage diverse datasets, making it necessary to integrate SOC operations into a larger national or sector-wide cybersecurity framework.

To achieve this, Indian SOCs must protect critical digital infrastructure by securing a range of public-facing services, such as biometric systems and digital payment gateways. This involves close collaboration with private companies and regulatory bodies, ensuring that SOC strategies align with broader cybersecurity objectives.

Compliance and regulatory requirements

Public sector organisations face unique cybersecurity challenges, making a robust SOC essential for protecting mission-critical data and infrastructure.

Public sector SOCs face stringent regulatory requirements for data protection. Ensuring compliance with these laws is essential, and modern SOCs must be built with these regulations in mind. Failing to do so can result in fines, operational shutdowns and reputational damage.

A participant made a compelling comparison, likening an SOC to a casino environment. Unlike a checkpoint that only verifies credentials, a SOC should continuously monitor user behaviour, detecting anomalies such as a card counter at a table rather than relying solely on static access controls. The key takeaway was that modern threats are more than just entering through the front door; they also exhibit unusual behaviour once inside.

The discussion then shifted to threat tolerance, emphasizing that organisations must define their risk appetite and visibility requirements to avoid overwhelming security operations. The need for behavioural baselining was highlighted, stressing the importance of understanding what “normal” behaviour looks like for users and systems so deviations can be identified early, especially in light of how easily stolen credentials and default passwords can be exploited if ignored.

SOCs must continuously audit their practices to stay aligned with changing regulatory frameworks, particularly regarding data privacy laws. This requires SOCs to balance real-time threat management with ongoing regulatory obligations.

Addressing blind spots and blurred visibility

Blind spots are more prevalent now because of the sheer amount of available data. As we are all so focused on the bigger picture, our attention is now being drawn away from more specific cybersecurity issues.

In hyperconnected environments, SOCs face two major visibility challenges, namely blind spots and blurred visibility. Blind spots arise in areas that are not properly monitored, such as testing environments left exposed to external networks. Meanwhile, blurred visibility occurs when SOCs are overwhelmed by vast amounts of data from multiple endpoints, making it difficult to focus on critical threats.

The participants collectively emphasized that a modern SoC is no longer just a reactive setup; it must detect, respond and adapt in the near real time.

As cyberthreats evolve, SOCs need tools to sift through large volumes of data and isolate high-priority incidents. Proactive measures, such as Attack Surface Management (ASM) and endpoint detection, can mitigate these risks. SOCs must have visibility across network layers, especially in hybrid and hyperconnected environments where the attack surface is constantly expanding.

Evolving threats and adaptive strategies

Cybersecurity today requires more than just defence; it demands continuous evolution, integration and constant understanding of how threats evolve.

Gaurav Shukla

Cyberthreats continue to evolve, requiring SOCs to remain agile and adaptive. The zero-trust model, where every action within the network is treated as potentially hostile, has gained traction in this context. SOCs implementing zero-trust principles can better safeguard their systems by treating each network interaction cautiously.

A forward-looking approach to cybersecurity is essential, as the potential impact of quantum computing on cryptographic systems is unpredictable. Speakers warned of “harvest now, decrypt later” strategies, in which attackers steal encrypted data today in anticipation of future decryption capabilities. This underscores the need for organisations to future-proof their SoC designs, recognising that today’s encryption may not remain secure in the quantum computing era.

SOCs must also anticipate new attack vectors, such as AI-driven cyberattacks and develop proactive defences to combat these evolving threats. Modern adversaries will quickly outpace a static SOC, making continuous adaptation key to an effective defence.

Key takeaways

- **Paradigm shift:** Traditional SOC models are inadequate in today's interconnected environments. Modern SOCs must integrate cloud, OT and IT systems to safeguard against sophisticated threats.
- **Comprehensive monitoring:** Effective SOCs ingest data from multiple sources, enabling comprehensive visibility and early detection of security incidents.
- **Advanced threat intelligence and AI integration:** AI-driven threat intelligence and automation are essential for rapid, accurate detection and response.
- **Air-gap networking:** While effective for sensitive environments, air-gapped systems are not foolproof. SOCs must monitor and secure even isolated networks to avoid breaches through indirect or physical methods.
- **Skilled workforce:** Automation does not replace the need for skilled cybersecurity professionals, who are critical in managing complex environments and adaptive strategies.
- **Quantum computing and cybersecurity risks:** Quantum computing challenges encryption, requiring organisations to future-proof SoC designs against potential threats.
- **Proactive defence and zero-trust approach:** SOCs must adopt proactive strategies, including zero-trust principles, to stay ahead of evolving threats.

DEMYSTIFYING MODERN SOCs IN HYBRID AND HYPERCONNECTED ENVIRONMENTS

UNDERSTANDING THE PARADIGM SHIFT

- INTEGRATION OF CLOUD, OT AND IT SYSTEMS

ADVANCED THREAT INTELLIGENCE AND AI INTEGRATION

- RAPID, ACCURATE DETECTION AND RESPONSE

SKILLED WORKFORCE

- MANAGING COMPLEX ENVIRONMENTS AND ADAPTIVE STRATEGIES

PROACTIVE DEFENCE AND ZERO-TRUST

- ADOPTING MEASURES TO STAY AHEAD OF EVOLVING THREATS

6d. Ensuring fair and timely justice for all

Arjun Ram Meghwal
Minister of State, Ministry of Law and Justice (Independent Charge), Government of India

A modern justice system is the foundation of Viksit Bharat, and India's legal transformation is paving the way for timely, accessible justice for all.

A critical transformation is underway to make India's justice system more efficient, more accessible and more user-friendly. Holistic reforms in the Indian Penal Code (IPC) and Criminal Procedure Code (CPC) require modernising legislation to create a system that provides timely and fair resolutions. Embracing technology-driven initiatives, including e-courts and digital documentation, aims to streamline case management, reduce delays and foster transparency.

The key to this transformation is a focus on a user-centric approach and changes that work towards ensuring justice for all citizens. Unbundling dispute resolution into distinct stages, from advisory to resolution, allows users to navigate legal processes more intuitively. Technology solutions such as language translation tools and online dispute resolution platforms break down linguistic and geographical barriers, making justice more inclusive.

These innovations reflect a broader vision of society's evolving empowerment and trust in its justice system, nurtured by core tenets of transparency and accessibility. These efforts, working together, are creating a framework for a fair, resilient and open justice system for everyone.

Leaders Speak: Law and Justice – A Transformation Story
Speaker:
Arjun Ram Meghwal, Minister of State, Ministry of Law and Justice (Independent Charge), Government of India

Moderator:
Ajay Singh, Partner, Deloitte India
The Honourable Minister, Arjun Ram Meghwal kicked-off the discussion

> *Modernising the IPC and other foundational laws is essential to creating a justice system that reflects today's realities and aspirations.*
>
> **Arjun Ram Meghwal**
> **Minister of State, Ministry of Law and Justice (Independent Charge), Government of India**

with an insightful overview of India's legal evolution, referencing pivotal milestones such as the capital's shift from Kolkata to Delhi and

the influence of British legal reforms on India's governance framework. Recognising the need to adapt to contemporary demands, he advocated for the modernisation of the IPC, CPC and the Indian Evidence Act. These are legal codes which have barely been amended since colonial times and desperately demand to be adjusted to more modern socio-economic standards that reflect modern judicial processes.

Modernising these frameworks includes setting timelines for investigations, trials and case resolutions to combat the systemic delays that often hamper justice delivery. This theme emphasized the importance of updating traditional structures to meet India's goal of becoming a fully developed nation by 2047.

Using technology to enhance justice delivery

From e-courts to updated legal codes, India is reshaping its justice system to meet the demands of a fast-evolving society.

Technological integration emerged as a crucial pillar of India's legal transformation, especially in addressing the issues of backlog and delay. The e-Court project and the implementation of digital platforms for court proceedings, document management and prison systems were proposed as key solutions to increase efficiency and transparency in the justice delivery process. These digital platforms aim to streamline case management, improve document accessibility and allow for real-time monitoring of cases, thus significantly reducing the wait time for resolutions.

Additionally, technology in investigative procedures and data sharing among law enforcement agencies was discussed to support inter-agency collaboration and reduce procedural redundancies. The esteemed minister stressed the potential of these technological changes to create a more accessible and transparent justice system for citizens, promoting trust and accountability within the legal framework.

Capacity building for law enforcement and judicial officers

For legal reforms to succeed, we need empowered police and judicial officers trained to handle modernised processes and digital tools.

Arjun Ram Meghwal
Minister of State, Ministry of Law and Justice (Independent Charge), Government of India

For legal reforms to be effective, capacity-building initiatives were deemed essential to equip police, judicial officers and other legal professionals with the necessary skills and knowledge to implement modern practices. Training programmes focused on digital literacy, new investigative techniques and updated procedural guidelines are pivotal for achieving a uniform understanding of reformed legal processes across the country.

This focus on capacity building is about going beyond theoretical changes and bringing about real improvement. By empowering those on the frontlines of law enforcement and justice, India can put its legal system in a position to adjust more naturally to a fast-paced, digital society.

Future-focused initiatives for a resilient justice system

Clear timelines for investigations and trials are critical—delayed justice must become a thing of the past in a truly developed India.

Arjun Ram Meghwal
Minister of State, Ministry of Law and Justice (Independent Charge), Government of India

Looking ahead, the overall discussion underscored several initiatives aimed at creating a more resilient and adaptable justice system. The e-Court project was highlighted as an important step in digitalising courtrooms, thereby enabling remote hearings and enhancing accessibility. Future projects are expected to improve coordination among federal and state agencies, especially in handling high-stakes cases that require efficient data sharing and collaboration.

Additionally, establishing procedural timelines for specific case types, such as sexual harassment cases and privacy-related matters, was discussed to ensure timely justice. These forward-looking initiatives aim to uphold citizens' rights and foster a judicial system that is prepared for both current and emerging challenges.

Manthan: Envisioning a User-centric Justice System

Participants:
Krishnakumar Thiagarajan, eGov; Keerthana Medarametla, Agami; Ayushi Singhal, Agami; Atul Singh, Customs Dept.; Partha Sarathy Bhaskar, CPGRAMS, DARPG; Hemakshi Meghani, Indian School of Democracy; Rohit Sharma, Law Firm Ready; Amita Katragadda, Cyril Amarchand Mangaldas; Aditya Prasanna Bhattacharya, Vidhi; Daksh Aggarwal, Vidhi; Hitesh Kukreja, Indus Action; Chitra Rawat, Indus Action; Deeksha Gujral, iProbono; Pravash Prashun Pandey, J-S (eCourts), DoJ; Gaurav Masaldan, J-S (Admin, Legal Reforms), DoJ; Justice Sanjay Kishan Kaul, Retd SC Judge; Justice Gautam Patel, Bombay HC; Arghya Sengupta, Vidhi; Bikkrama Daulat Singh, Convergence Foundation; Shikha Hundal, UNDP & DoJ (Consultant); Tarun Cherukuri, Indus Action; Joseph Phookat, Staram; Aaditeshwar Seth, IIT-D / Gramvani; Dr Ashutosh Modi, IIT Kanpur; Nusrat Khan, UNDP; Sandip Garg, IBBI; Gaurab Banerjee, SC Senior Advocate; Narinder Singh, Tax Policy Research Unit; Pankaj Gupta, AWS

Guru:
Sreeram Ananthasayanam, Partner, Deloitte India

Building a justice system that listens, learns and adapts is essential for meeting the real needs of Indian citizens.

Central to the framework is unbundling the dispute resolution process to make it more user-focused. This approach categorises legal interactions into phases which include prevention, advisory, preparation, initiation, resolution and enforcement. It emphasizes the need to address specific user needs at each stage. Whether it is through legal advice, document management or securing resolutions, each phase is designed to serve the end user efficiently.

Key stakeholders, such as lawyers, counsellors, mediators and even MSME facilitation councils, play specialised roles across these stages. The framework also identifies gaps where new participants, such as community paralegals and mediators, can fill essential roles, making justice more accessible and affordable for individuals, particularly those from underserved communities.

Enhancing accessibility through technology

Tools such as Jugalbandi and online dispute resolution break down barriers, ensuring justice is accessible regardless of language or location.

The panel discussed how technology can streamline and simplify the legal journey for users. Solutions such as language translation tools, online dispute resolution platforms and real-time advisory services are examples of how technology addresses barriers in legal accessibility, particularly for users with limited language proficiency or those in remote areas.

For example, the Jugalbandi tool enables users to access legal information in their native languages, breaking down language barriers that often inhibit understanding and engagement with the justice system. By enabling online dispute resolution, the framework promotes quicker resolutions for specific disputes, such as labour and real estate cases, making the legal process faster, less intimidating and more accessible.

Building trust and ensuring consistency in information sharing

Trust is built through transparency, where standardised information sharing across platforms allows users to receive consistent and reliable guidance.

Trust and credibility are foundational for any user-centric justice system. The new framework aims to establish consistent, reliable information-sharing mechanisms by implementing APIs and open information exchange protocols between different services. This approach encourages transparency, ensuring that users have access to accurate and verified legal information.

By establishing common registries and promoting interoperability between systems, users can easily authenticate documents, access discovery resources and manage case information. Furthermore, consistent information-sharing fosters transparency, reducing discrepancies and encouraging citizens to engage more openly with the justice process.

Adaptability and real-time feedback for continuous improvement

Feedback-driven improvement means our justice system can evolve in real-time, adapting to unique regional and social contexts.

Continuous improvement is integral to building a justice system that evolves with user needs. The *Manthan* delved deeper into the importance of ongoing feedback from users, which enables the framework to adapt in real time and better address specific regional or situational requirements. Through feedback loops, the framework can be stress-tested in various contexts, such as domestic violence and labour disputes, ensuring that it remains flexible and responsive.

Experimenting with new solutions and learning from initial implementations are central to this approach. The framework encourages participants to share insights and challenges, facilitating a community-driven evolution that allows the system to adapt quickly and effectively to unique case demands.

Addressing digital divides and fostering community-driven solutions

Inclusive justice means reaching users, even those without digital access, through community-driven support and offline resources.

A user-centric justice system must address the digital divide that excludes users without access to smartphones or internet connectivity. The panellists emphasized solutions such as toll-free numbers and community-driven initiatives to ensure inclusivity. By integrating paralegals, community agents and other grassroots-level participants, the system can reach a broader demographic, particularly in rural or underserved areas.

Community agents play a crucial role in helping users navigate the justice system, providing support in local languages and offering legal advice through accessible means. These strategies ensure that technology doesn't leave anyone behind, fostering inclusivity even for those who may not be digitally connected.

Key takeaways

- **Overhauling foundational legal frameworks:** Updating the Indian Penal Code, Criminal Procedure Code and Indian Evidence Act to reflect today's social realities is critical for efficient governance and swift justice delivery.
- **Embracing technological innovation:** The e-Court project and digital platforms for case management, documentation and prison systems are pivotal to reducing case backlogs and improving transparency.
- **Empowering legal professionals:** Capacity-building programmes for police, judicial officers and other legal professionals ensure that modernisation efforts are effectively implemented at every level of the justice system.
- **Future-ready justice initiatives**: Projects such as e-Courts and inter-agency coordination mechanisms aim to build a resilient justice system capable of addressing both present and future needs.
- **Timelines for justice delivery:** Implementing clear timelines for investigations and case resolutions is essential for reducing procedural delays and ensuring timely justice.
- **Unbundling for user focus:** The justice system is streamlined through unbundling phases of dispute resolution, addressing specific user needs at each stage for a smoother, more effective experience.
- **Using technology for accessibility:** Language translation tools, online dispute resolution platforms and real-time advisories make legal resources more accessible, especially for underserved communities.
- **Building trust with consistent information:** The framework establishes a trustworthy, consistent justice system that encourages user engagement through open APIs, common registries and transparent information sharing.
- **Adaptability through feedback:** Ongoing user feedback allows the framework to adapt to specific contexts and unique user needs, ensuring flexibility in a fast-evolving society.
- **Bridging the digital divide:** Community-driven solutions, such as toll-free numbers and local agents, address the digital divide, ensuring inclusivity for users, even those in remote areas.

ENVISIONING A "USER-CENTRIC" JUSTICE SYSTEM

BRIDGING THE DIGITAL DIVIDE

- HYBRIDISED ONLINE AND OFFLINE ACCESS
- TOLL-FREE NUMBERS OR COMMUNITY-DRIVEN INITIATIVES

TECHNOLOGY FOR ACCESSIBILITY

- ODR PLATFORMS
- LANGUAGE TRANSLATION TOOLS

USER-CENTRIC LEGAL FRAMEWORK

- BREAKING DOWN COMPLEX LEGAL PROCESSES INTO MANAGEABLE STAGES
- TRANSPARENCY AND ACCESSIBILITY

CUSTOMISATION FOR CONTEXT

- ADAPTABLE LEGAL SERVICES SUPPORTED BY LOCAL AGENTS AND PARALEGALS