



Lt Gen M Unnikrishnan Nair (retd)

Chairman – 63SATS Cybertech &
Former National Cyber Security
Coordinator Government of India

India is entering a defining phase in the evolution of GCCs. What began as a model focused on cost efficiency has steadily transformed into a powerful engine of innovation, technology development, and strategic decision-making for global enterprises. Today, India's GCC ecosystem is being shaped by three defining pillars - being smart, skilled, and scalable - as organizations increasingly rely on these centers to drive digital transformation and enterprise growth.

However, as GCCs become more technology-driven and deeply integrated into global operations, the importance of cybersecurity has grown significantly. The rapid adoption of artificial intelligence, cloud platforms, and interconnected digital systems has expanded the threat surface for organizations worldwide. More concerning is the weaponisation of AI, where cyber adversaries are using advanced technologies to launch highly sophisticated attacks, ranging from AI-generated phishing campaigns and deepfake impersonation to automated vulnerability exploitation.

At the same time, the current geopolitical landscape is adding another layer of complexity. Rising regional tensions, economic uncertainties, and the growing convergence of cyber and kinetic conflicts have demonstrated that digital infrastructure is increasingly becoming a strategic target. For multinational organizations operating GCCs, geopolitical disruptions can translate into cyber espionage, ransomware campaigns, or coordinated attacks aimed at disrupting business continuity.

In this evolving environment, cybersecurity can no longer be treated as a support function. It must be embedded as a strategic pillar of GCC operations. Organizations must move toward security-first architectures, adopting zero-trust frameworks, strengthening threat intelligence capabilities, and ensuring continuous monitoring of digital environments. Equally critical is building a skilled cybersecurity workforce and embedding a culture of cyber awareness across teams.

India's GCC ecosystem has the talent, scale, and technological depth to lead the next phase of global enterprise transformation. Ensuring that these centers remain secure, resilient, and trusted will be essential to sustaining that leadership.

At 63SATS, we believe that protecting digital infrastructure requires a proactive and intelligence-led approach. Through advanced threat monitoring, real-time incident response, and integrated cybersecurity solutions, 63SATS supports organizations in strengthening their cyber resilience. As GCCs continue to evolve into strategic nerve centers for global enterprises, robust cybersecurity will remain central to enabling their safe and sustainable growth.