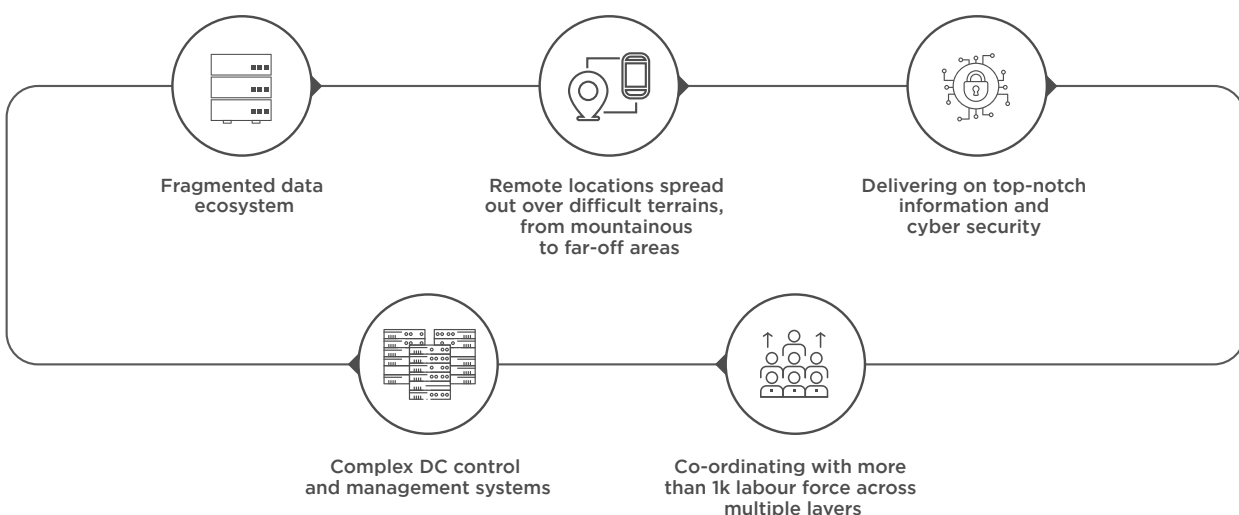# Delivering an advanced and highly secure Data Centre ecosystem

PROJECT BACKGROUND

This case study enumerates how STL built a smart next-gen communication infrastructure to enable a platform for new-age technologies and customised enterprise applications, with an advanced security ecosystem for one of the largest defence organisations. In the journey of concept, design, implementation and commissioning, STL mitigated several challenges and built 12 data centres, spanning across 33 civil locations, covering 131k sqft of built-up area.

Legacy data centres needed to be modernized to achieve mission-critical outcomes for the defence client. This entailed a sophisticated design and planning exercise to deliver an advanced, integrated and highly secure data centre ecosystem.

CHALLENGES THAT WE FACED (AND MITIGATED)

Fragmented data ecosystem

Remote locations spread out over difficult terrains, from mountainous to far-off areas

Delivering on top-notch information and cyber security

Complex DC control and management systems

Co-ordinating with more than 1k labour force across multiple layers

STL SOLUTION TO DELIVER EXCELLENCE

STL took the challenge of building next-gen data centres along Indian coastal borders including Lakshadweep & Port Blair islands. 12 data centres were constructed including four main data centres, one disaster recovery centre, four near-line data centres, and three satellite data centres.

The data centres were built using MPLS Segment-routing, leaf-spine architecture, multi-layered redundancy failovers, with geo-redundancy for natural disasters and wartime situations

The data centres were equipped with multi-layer technology-led perimeter security to prevent any sort of physical or Cyber-attacks not only at present but also in future.

.

These data centres enabled a plethora of applications at various locations:
• Private cloud with multi-tenancy to host IaaS, PaaS (at Karwar)
• Unified Network Management System (NMS) (between Mumbai and Vizag) for central monitoring of assets from the Network Operating System (NOC), fault management & assets patch management
• Security management (SIEM) for centralised events/incidents policy monitoring from SOC (between Vizag & Delhi)
• Content Delivery Network (CDN) for central repository & streaming of live events, conferences, seminars, images, and classroom lectures, etc. (between Delhi & Kochi)
• Big data analytics to enable mission critical analysis (at Mumbai)

IMPACT DELIVERED

12

Greenfield data centres for next-gen defence applications)

Highly Secure

Private cloud equipped with physical and cyber security

99.95%

Network availability for inter Data Centre connectivity

Geo redundancy

To ensure continuity and security