SOFTWARE TECHNOLOGY
PARKS OF INDIA

ADVANCING CONNECTIVITY

& CYBERSECURITY

Securing India's Digital Future in the AI-Native 6G Era

AGENDA

What We'll Cover Today

01 **6G Architecture & Evolution**

Beyond 5G: spectrum, latency, Tbps-era connectivity

02 **AI-Native Network Intelligence**

Embedded ML at RAN, core and device layers

03 **6G Use Cases**

Industry 5.0, XR, autonomous vehicles, smart agriculture

04 **Cybersecurity Threat Landscape**

New attack surfaces in 6G ecosystems

05 **Defense-in-Depth Framework**

Multi-layer SOC architecture by STPI

06 **Security Standards & PQC**

Zero Trust, Post-Quantum Crypto, 3GPP R20

07 **India's 6G Journey**

STPI's strategic role

08 **STPI’s SOC as a Service & Why STPI**

24×7 STPI managed security operations

STPI & ITS SERVICES

India's Premier IT/ITES Enabler under MeitY, Government of India

SOFTWARE TECHNOLOGY PARKS OF INDIA

Established in 1991, as an autonomous society under the Ministry of Electronics & Information Technology, Government of India, with the objective of encouraging, promoting and boosting the software exports from India.

SERVICES PROVIDED BY STPI

- Statutory Services - STP/EHTP Scheme
- Incubation Services
- High Speed Data Communication Services
- Startup Promotional Services
  - Centres of Entrepreneurship (CoEs)
  - Next Generation Incubation Scheme (NGIS)
- Project Management & Consultancy Services
- Data Centre Services
- Security Operations Centre Services
  - Vulnerable Assessment and Penetration Testing (VAPT)
- BPO Promotion Scheme
- EMC 2.0 Scheme

एसटीपीआई
STPI

6G ARCHITECTURE

Evolution Beyond 5G — Key Technical Parameters

Parameter	5G (Current)	6G (Target)
Peak Data Rate	20 Gbps	**1 Tbps**
Latency	~1 ms	**< 0.1 ms**
Connection Density	10^6 devices/km²	**10^7 devices/km²**
Spectrum	Sub-6GHz / mmWave	**THz + Sub-THz bands**
Energy Efficiency	Baseline	**100× improvement**
AI Integration	Peripheral/Optional	**Native, embedded at RAN**

Source: ITU-R IMT-2030 Framework | 3GPP Release 20 Roadmap

AI-NATIVE INTELLIGENCE

Embedded ML Across the 6G Stack

01 Radio Access Network (RAN)

- AI-driven beam management & interference nulling
- Federated learning across distributed RAN nodes
- Self-optimizing antenna arrays (Massive MIMO+)

02 Core Network & Orchestration

- Intent-Based Networking (IBN) for autonomous SLA
- Predictive slice allocation using deep RL
- Real-time anomaly detection in control plane

03 Edge & Device Intelligence

- Split inference: model across device + edge
- Semantic communications — transmit meaning, not bits
- On-device continual learning with privacy guarantees

6G positions AI not as an add-on — but as the foundational control plane of the network.

6G CONNECTIVITY USE CASES

High-Impact Verticals Enabled by 6G

Industry 5.0

< 0.1ms

Haptic control, digital twin sync, zero-latency automation

Remote Surgery

99.9999%

Ultra-reliable tele-operated robotics & real-time imaging

Autonomous Vehicles

$10^7/km^2$

V2X mesh networking, cooperative perception systems

XR & Holographics

1 Tbps

Immersive digital-physical convergence at scale

Smart Agriculture

10× density

Precision IoT, soil-to-cloud real-time telemetry

Critical Infrastructure

Zero Trust

Secure SCADA, grid monitoring, national security networks

CYBERSECURITY THREAT LANDSCAPE 2025

New Attack Surfaces in 6G Ecosystems & Modern Threats

$4.88M	$10.5T	46%	30%
Avg Data Breach Cost (IBM 2025)	Annual Cybercrime Cost Globally	Ransomware Surge Industrial Q1 2025	Supply Chain Breach Involvement

CRITICAL

AI Model Poisoning

Adversarial data injection into federated learning nodes disrupts 6G network optimization.

CRITICAL

Quantum Decryption Threat

Harvest-now-decrypt-later: current ciphertext at risk from future quantum systems.

HIGH

THz Channel Eavesdropping

Terahertz line-of-sight links vulnerable to highly directional passive interception.

HIGH

Hyperscale IoT Botnet Attacks

10M+ compromised edge devices enabling unprecedented DDoS amplification.

HIGH

Ransomware & RaaS

Triple extortion: encrypt + leak + DDoS. Avg ransom $5.08M. LockBit 4.0, Cl0p.

MEDIUM

Slice Isolation Failure

Cross-tenant data leakage through network slice misconfigurations in shared core.

DEFENSE-IN-DEPTH

Multi-Layer Security Architecture — Protecting Every Layer

01

PERIMETER LAYER

Anti-DDoS | NGFW | IPS/IDS | SWG

Stops: DDoS Floods / Port Scans

02

NETWORK LAYER

UTM | Internal Firewall | NAC | VPN/ZTNA

Stops: Lateral Movement / MITM

03

APPLICATION LAYER

WAF | API Security | VAPT | Secure SDLC

Stops: SQLi / XSS / API Abuse

04

ENDPOINT LAYER

EDR | XDR | DLP | Antivirus | MDM

Stops: Ransomware / Malware / Data Leak

05

IDENTITY LAYER

PIM | PAM | IDAM | MFA | SSO

Stops: Privilege Escalation / BEC

PERIMETER & NETWORK SECURITY

Layers 1 & 2 — First Line of Defence

[L1] Anti-DDoS / Anti-DoS

- Volumetric & protocol attack mitigation
- Rate limiting & traffic scrubbing
- Always-on + on-demand cloud scrubbing

[L1] Next-Gen Firewall (NGFW)

- Deep packet inspection (DPI)
- Application-aware policy enforcement
- Geo-blocking & IP reputation filtering

[L1] IPS / IDS

- Signature + anomaly-based detection
- Real-time inline packet analysis
- Zero-day behavior analysis

[L1] Secure Web Gateway

- URL filtering & content inspection
- SSL/TLS deep inspection
- Malware sandboxing for attachments

[L2] Internal Firewall & UTM

- East-west traffic & micro-segmentation
- All-in-one: AV + anti-spam + URL filter
- Centralised policy management

[L2] NAC & VPN/ZTNA

- Device posture & health checks (802.1X)
- Guest & BYOD network isolation
- Zero Trust Network Access (ZTNA)

APPLICATION & ENDPOINT SECURITY

Layers 3 & 4 — Securing Apps, APIs, and Every Device

[L3] WAF — Web Application Firewall

- OWASP Top 10 & bot mitigation
- Virtual patching (zero-day cover)
- SSL offloading & real-time alerts

[L3] API Security

- API discovery & schema validation
- Rate limiting & throttling
- Sensitive data masking

[L3] VAPT (CERT-In Empanelled)

- Network, web app & cloud pen testing
- Red team / adversary simulation
- Detailed remediation reports

[L4] EDR / XDR

- Behavioural AI-based threat detection
- Cross-layer attack correlation
- Automated isolation & forensics

[L4] DLP — Data Loss Prevention

- Classify & protect PII, PCI, IP data
- Block unauthorised USB/file transfers
- Email & cloud upload monitoring

[L4] MDM — Mobile Device Mgmt

- BYOD & corporate device policy
- Remote wipe & lock capability
- Continuous compliance posture checks

IDENTITY & CLOUD SECURITY

Layers 5 & 6 — Zero Trust Starts with Identity

LAYER 5 — IDENTITY & ACCESS MANAGEMENT

PIM — Privileged Identity Mgmt

- Just-in-time (JIT) privileged access
- Session recording & full audit trail
- Privileged account vaulting

PAM — Privileged Access Mgmt

- Password vaulting & auto-rotation
- Dual control for critical operations
- Break-glass emergency access

IDAM & MFA

- Centralised user lifecycle management
- RBAC/ABAC policy enforcement
- OTP, biometric & FIDO2 hardware token

LAYER 6 — CLOUD & DATA SECURITY

CSPM — Cloud Posture Mgmt

- Continuous compliance scanning (AWS/Azure/GCP)
- Misconfiguration detection & auto-remediation
- CIS Benchmarks & DPDP Act alignment

CASB — Cloud Access Broker

- Shadow IT discovery & SaaS visibility
- Data security policy enforcement
- Threat protection for cloud apps

Encryption & Disaster Recovery

- Data at rest & in transit encryption
- Immutable backups & air-gapped recovery
- RTO/RPO-aligned DR planning

SECURITY FRAMEWORKS & STANDARDS

Defensive Architecture for 6G Networks

Zero Trust Architecture (ZTA)

Never trust, always verify

- Micro-segmentation for every 6G network slice
- NIST SP 800-207 in network-native contexts
- Continuous identity verification at all layers
- Least-privilege access enforcement

Post-Quantum Cryptography

NIST FIPS 203/204/205 — Finalized 2024

- CRYSTALS-Kyber for key encapsulation (KEM)
- CRYSTALS-Dilithium for digital signatures
- Hybrid TLS for migration transition period
- 256-bit quantum-safe key lengths

3GPP Release 20 Security

Formal threat modelling for AI-native RAN

- Privacy-preserving auth via SUPI/SUCI schemes
- AI/ML model integrity verification
- End-to-end slice security framework
- <10ms PQC handshake overhead target

Principle: Security must be designed in — not bolted on — at every 6G protocol layer.

India's 6G Journey

STPI's Strategic Role

- Incubation of 6G deep-tech startups via CoE
- CoE for secure connectivity & cybersecurity research
- Talent pipeline: 6G Security Engineers & spectrum specialists via SAHAYAK
- Improving Cyber Security Posture: Security and Compliance Audits, SoC

SOC AS A SERVICE

24×7×365 Security Operations Centre — Managed by STPI

24×7	<5 min	26,500+	99.9%
Monitoring	MTTD	Devices	Availability

Log & SIEM Integration

- 100+ log source types supported
- Real-time event processing (EPS)
- ML-driven threat detection & correlation
- Long-term log retention & archiving

Incident Monitoring

- Continuous 24×7×365 analyst coverage
- Behavioural analytics & anomaly detection
- Intelligent triage: Critical/High/Medium/Low
- Defined L1/L2/L3 escalation workflows

Threat Intelligence

- Nation-state reports & OSINT feeds
- Dark Web monitoring & IOC feeds
- CVE & vulnerability advisories
- Intel-driven hunting playbooks

Incident Response (NIST)

- Detect → Contain → Eradicate → Recover
- Automated playbooks & isolation
- Forensic root cause analysis
- Post-incident report & lessons learnt

WHY STPI FOR CYBERSECURITY

Differentiators & Complete Security Portfolio

Government Backing

Autonomous society under MeitY — trusted by IT/ITES units across India

CERT-In Empanelled

Certified for security audits, VAPT, and incident response

70+ Offices

Pan-India presence ensures local support, compliance coverage, and rapid response

End-to-End Services

Connectivity to SOC, Cloud Security, VAPT, and compliance under one roof

Emerging Tech CoEs

Deep expertise in security, AI-native networks, and quantum-resilient architectures

Regulatory Alignment

DPDP , CERT-In compliance built in, NCIIPC

THANK YOU

www.stpi.in

Key Takeaways

- 6G is a paradigm shift — not an incremental upgrade
- AI embedded at RAN/core enables self-healing networks
- Expanded attack surface demands proactive architecture
- PQC & Zero Trust are mandatory for 6G protocol stacks
- India's 6G Journey — STPI plays a catalytic role