6G Wireless Technology

Cybersecurity Threats, Mitigations & Experimental Testbeds

Presented by:
Prof. Sandeep K Shukla

March 2026

THz Communications | AI-Native Security | Open RAN | Post-Quantum Crypto | Zero Trust

Presentation Agenda

01	6G Technology Overview & Key Features
02	6G Architecture & Enabling Technologies
03	6G Use Cases & Deployment Timeline
04	Major Cybersecurity Threats in 6G
05	Risk Ranking: The Most Critical Threats
06	Technology Solutions for Threat Mitigation
07	Administrative Controls & Governance
08	Global 6G Security Testbeds & Research
09	Lessons from Testbed Experiments
10	Conclusions & Recommendations

6G Technology: Key Features

Sixth-generation wireless — targeting commercial deployment by 2030

CYBER MANTHAN
IIIT HYDERABAD

Peak Data Rate

1–10 Tbps

100× faster than 5G

Latency

< 0.1 ms

Sub-millisecond

Frequency

THz Band

100 GHz – 10 THz

AI-Native

Built-in AI

Self-configuring networks

Coverage

Global 3D

Space-Air-Ground-Sea

Security

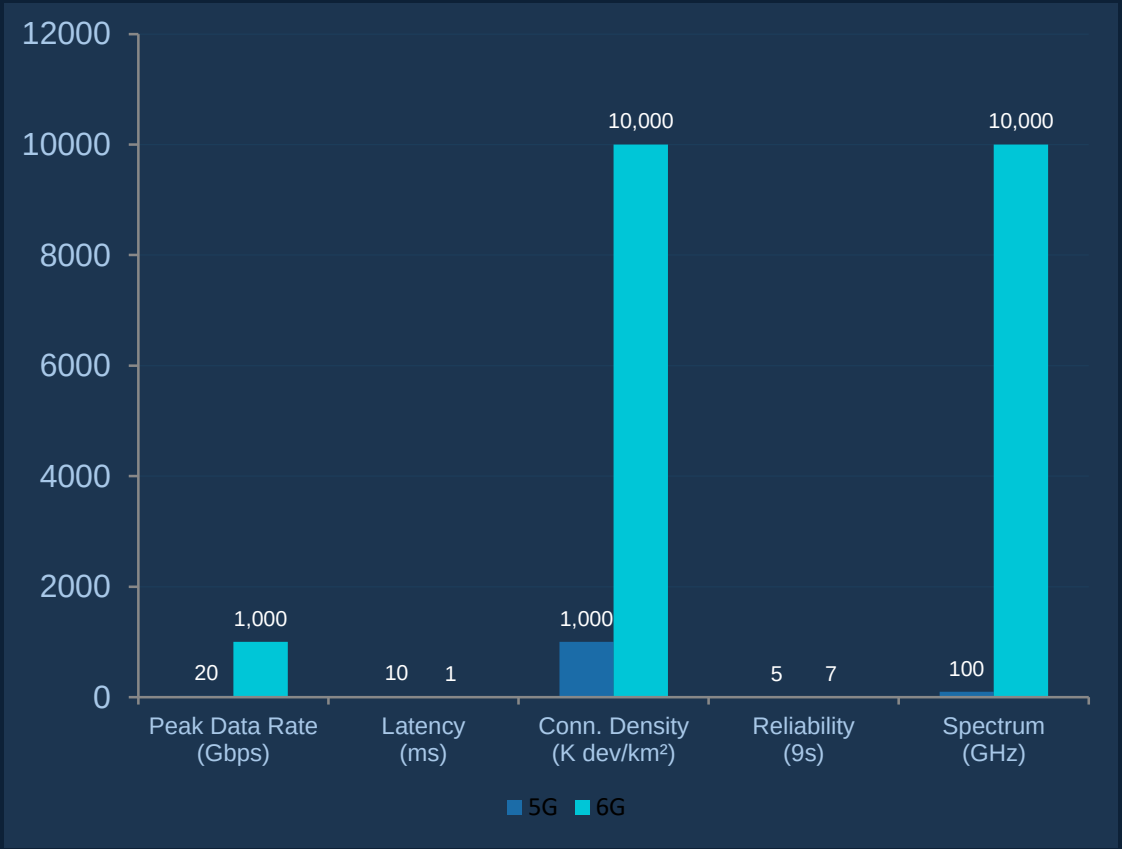
360° Privacy

Security-by-design

6G Architecture & Enabling Technologies

Application Layer	XR/Holographic · Digital Twins · Autonomous Systems · Smart Healthcare
Service & Management	AI/ML Orchestration · Network Slicing · Intent-Based Networking
Network Core	Cloud-Native Core · MEC · Blockchain Trust · Post-Quantum Crypto
RAN (Open RAN)	THz Massive MIMO · RIS Surfaces · O-RAN Disaggregation · xApps/rApps
Physical/Spectrum	Sub-THz 100–300 GHz · mmWave · Optical Wireless · NOMA

5G vs 6G: A Comparative Leap



50× Faster

Peak rates up to 1 Tbps vs 20 Gbps in 5G

10× Lower Latency

Sub-0.1ms enabling real-time holographics

New Spectrum

THz bands (300GHz–3THz), sub-THz, optical

AI-Native Core

Intelligence embedded into the network fabric

3D Coverage

Integrated satellite + aerial + terrestrial

6G Use Cases & Critical Applications

Holographic Communications

Real-time 3D holographic telepresence requiring Tbps throughput

Digital Twins

Real-time virtual replicas of physical infrastructure, cities, and human bodies

Autonomous Vehicles

Ultra-reliable V2X communications with sub-ms latency for safety-critical decisions

Remote Surgery

Haptic feedback and robotic surgery over 6G with guaranteed reliability

Smart Cities & Industry 5.0

Massive IoT deployments with 10M devices/km² in smart manufacturing

Immersive XR/Metaverse

Extended reality requiring persistent Gbps connections and <1ms latency

The Expanding 6G Attack Surface

Each new capability creates a corresponding security challenge

1. **Open RAN Interfaces**
   Disaggregated architecture exposes X2, Xn, F1, E1, O1, A1 interfaces to attack
2. **AI/ML Attack Surface**
   Adversarial inputs, model poisoning, and inference attacks on native AI systems
3. **THz Physical Layer**
   Eavesdropping via directional beams; denial-of-service on line-of-sight links
4. **Massive IoT Nodes**
   Billions of resource-constrained devices become entry points; difficult to patch
5. **Multi-cloud & Edge**
   Distributed compute across untrusted clouds and edge nodes increases exposure
6. **Digital Twin Systems**
   Real-time replicas of critical infrastructure become high-value espionage targets

Major Cybersecurity Threats in 6G

AI/ML Threats

- Model poisoning & adversarial attacks
- Inference attacks on AI-driven RAN
- Generative AI-powered cyberattacks

Quantum Threats

- Breaking RSA/ECC with quantum computers
- Harvest-now-decrypt-later attacks
- Quantum side-channel vulnerabilities

Network Threats

- Open RAN interface exploitation
- DDoS on softwarized network functions
- Supply chain compromise of multi-vendor RAN

Privacy Threats

- Mass surveillance via ubiquitous sensing
- Digital twin data exfiltration
- Cross-border data sovereignty violations

Physical Layer

- THz eavesdropping on LOS links
- Jamming and denial-of-service
- Reconfigurable Intelligent Surface (RIS) spoofing

Endpoint/IoT

- Resource-constrained device exploitation
- Massive botnet formation (billions of nodes)
- Side-channel attacks on edge devices

Deep Dive: AI-Native Network Threats

6G embeds AI into every network layer — creating unprecedented attack vectors

CYBER MANTHAN
IIIT HYDERABAD

Model Poisoning

CRITICAL

Attackers inject malicious training data into federated learning systems used for RAN optimization, corrupting network behavior at scale.

Adversarial Inputs

HIGH

Specially crafted radio signals that fool AI-based intrusion detection systems and spectrum management algorithms.

Inference Attacks

HIGH

By observing AI model outputs, attackers reverse-engineer training data — exposing sensitive user patterns and network topology.

Model Evasion

HIGH

Malicious traffic crafted to bypass ML-based anomaly detection; increasingly effective as GenAI generates evasion patterns.

Data Pipeline Poisoning

CRITICAL

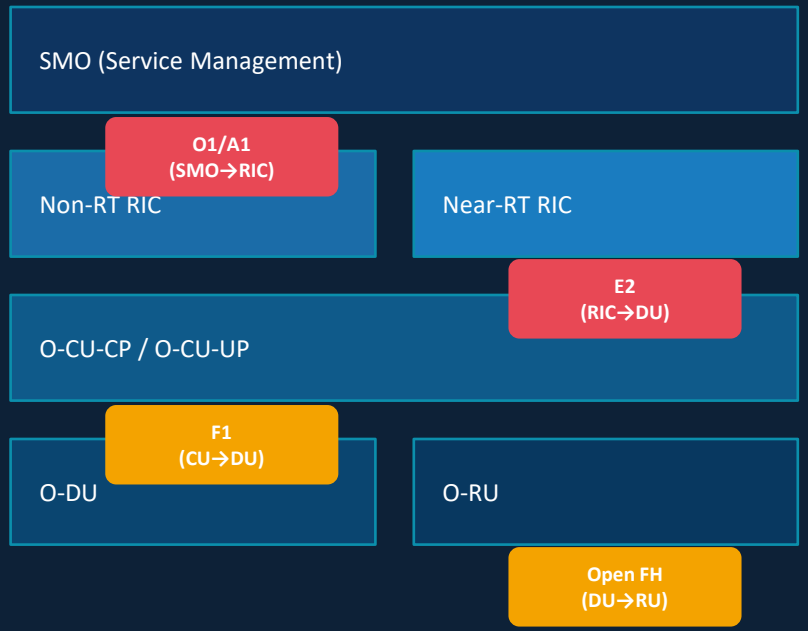
Corrupting the massive telemetry feeds that train 6G network management AI, causing degraded QoS or persistent backdoors.

Rogue AI Agents

EMERGING

Autonomous AI agents embedded in the network could be compromised to act as persistent, self-adapting insider threats.

Open RAN: Expanded Attack Surface



← Open interfaces enable multi-vendor innovation but expand attack surface

Key O-RAN Threat Vectors

xApp/rApp Compromise

Malicious third-party apps injected into Near-RT RIC can manipulate entire RAN behavior

E2 Interface Exploitation

Unauthenticated or weakly authenticated E2 messages can trigger RAN misconfigurations

API Injection Attacks

O-RAN's REST APIs are vulnerable to injection if not properly input-validated

Supply Chain Backdoors

Multi-vendor RAN ecosystem increases exposure to hardware/software supply chain compromise

Man-in-the-Middle on F1

Interception of F1-C/F1-U traffic between CU and DU in disaggregated deployments

Quantum Computing & Physical Layer Threats

Quantum Computing Threats

Shor's Algorithm

Breaks RSA-2048 and ECC-256 — current encryption protecting 6G signaling and data

Grover's Algorithm

Halves the effective security of symmetric keys — AES-128 becomes effectively 64-bit

HNDL Attacks

"Harvest Now, Decrypt Later" — adversaries record encrypted 6G traffic today to decrypt once quantum computers mature

Quantum Sensing

Nation-state actors may use quantum sensors to detect and locate 6G base station emissions with extreme precision

Physical Layer Threats

THz Eavesdropping

Directional THz beams can be intercepted using nearby passive antenna arrays without detection

RIS Spoofing

Reconfigurable Intelligent Surfaces could be rogue-programmed to reflect signals to unintended receivers

Pilot Contamination

In massive MIMO, malicious pilots during channel estimation corrupt beamforming — classic 6G threat

Jamming/DoS

High-powered jamming at THz frequencies can disrupt line-of-sight 6G backhaul links entirely

Privacy & Supply Chain Threats

Privacy Threats

Pervasive Surveillance

6G's ubiquitous sensing (ISAC) enables continuous tracking of individuals via RF fingerprinting — a mass surveillance risk at unprecedented scale.

Digital Twin Exfiltration

Real-time body/building digital twins store intimate data (health, location, behavior). Compromise leads to severe personal privacy violations.

AI Profiling

AI-driven 6G networks build detailed user profiles from aggregated traffic metadata, bypassing traditional privacy protections.

Supply Chain Threats

Multi-Vendor RAN Backdoors

Open RAN's disaggregated multi-vendor architecture multiplies supply chain entry points. Nation-state actors can embed persistent backdoors in chipsets or firmware.

Software Dependency Attacks

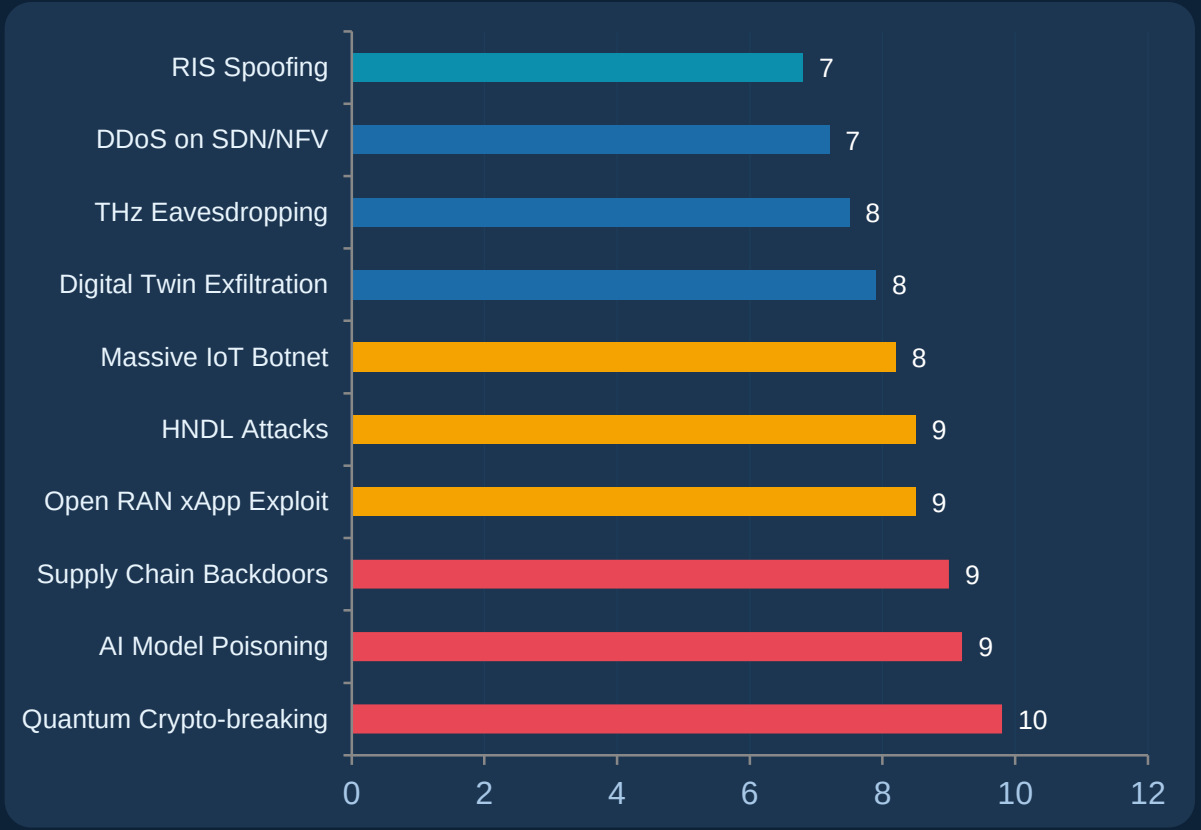
Cloud-native 6G core relies on open-source software stacks. Malicious packages (npm/PyPI-style attacks) can compromise the entire network.

Hardware Trojan in THz Chips

Advanced semiconductor supply chain attacks can embed Trojans in THz transceivers that activate under specific signal conditions.

Risk Ranking: Most Critical 6G Threats

Risk Score = Likelihood × Impact (ITU-T X.805 framework)



CRITICAL (>9.0)

HIGH (8.0–9.0)

SIGNIFICANT (7.0–8.0)

MODERATE (<7.0)

** Based on ETSI GR SAI 002, ITU-T X.805, ENISA 6G Threat Landscape (2025)*

Technology Solutions: Cryptographic & AI Defenses

Post-Quantum Cryptography (PQC)

NIST Standardized 2024

- CRYSTALS-Kyber (ML-KEM): Key encapsulation for 6G signaling
- CRYSTALS-Dilithium (ML-DSA): Digital signatures for authentication
- SPHINCS+ for stateless hash-based signatures in IoT
- Hybrid classical+PQC transition strategy for 6G rollout

AI-Driven Threat Detection

ML-Based IDS

- Deep Learning IDS achieving 99.9% accuracy on NSL-KDD / UNSW-NB15
- Federated Learning for privacy-preserving anomaly detection across nodes
- Graph Neural Networks (GNNs) for detecting lateral movement in 6G core
- Explainable AI (XAI) with SHAP/LIME for interpretable threat alerts

Physical Layer Security (PLS)

PHY-Native

- Beamforming secrecy: Direct signals to legitimate user, null to eavesdropper
- Artificial noise injection into null space to mask THz transmissions
- Channel reciprocity-based secret key generation for 6G links
- OFDM-based covert channels detection using statistical fingerprinting

Quantum Key Distribution (QKD)

Quantum-Safe

- Satellite-based QKD for long-haul 6G backhaul key exchange
- Measurement-Device-Independent (MDI) QKD for metro 6G networks
- Integration with PQC as defense-in-depth strategy
- CV-QKD compatible with standard optical fiber infrastructure

Technology Solutions: Architecture & Network Controls

Zero Trust Architecture (ZTA)

Never-trust-always-verify applied to every 6G component. Micro-segmentation of network slices, continuous re-authentication, and least-privilege access for xApps/rApps in O-RAN environments.

Network Slicing Security

Cryptographic isolation between network slices using slice-specific security policies. TEEs (Trusted Execution Environments) in network functions prevent cross-slice data leakage.

Blockchain-Based Trust

Distributed ledger for immutable audit trails of 6G RAN configuration changes. Smart contracts enforce automated compliance checking of xApp behavior.

End-to-End Encryption (E2EE)

Application-layer E2EE combined with TLS 1.3 for all O-RAN interfaces (O1, A1, E2, F1). Post-quantum TLS extensions being standardized by IETF for 6G deployment.

Security Orchestration (SOAR)

AI-powered SOAR platforms that auto-respond to threats in 6G's softwarized core — isolating compromised VNFs, rerouting slices, and triggering forensic capture in <100ms.

Secure Spectrum Management

AI-based cognitive radio security: detecting rogue transmitters, preventing jamming via frequency hopping, and using ISAC for physical-layer authentication of devices.

Administrative Controls & Governance Frameworks

ITU-T / 3GPP

Standards & Specs

- ✓ 3GPP SA3 6G security specs (TR 33.xxx)
- ✓ ITU-R IMT-2030 security framework (M.2160)
- ✓ ETSI NFV/MEC security specifications

ENISA / EU

Regulatory Framework

- ✓ NIS2 Directive application to 6G CNI
- ✓ EU 6G Security Certification Scheme (EUCS)
- ✓ ENISA 6G Threat Landscape annual reports

NIST / CISA US

National Policy

- ✓ NIST PQC migration guidelines (SP 1800-38)
- ✓ CISA 6G supply chain risk management
- ✓ FCC spectrum security regulations

O-RAN Alliance

Industry Standards

- ✓ O-RAN Security Focus Group (SFG) specs
- ✓ WG11 security architecture for Open RAN
- ✓ Trusted xApp certification program

Key Principle: Security-by-design mandated at every phase — standardization, procurement, deployment, and operations

Operational Security Processes & Best Practices

CYBER MANTHAN
IIIT HYDERABAD

01

Threat Modeling & Risk Assessment

Apply STRIDE/DREAD and MITRE ATT&CK for Mobile to 6G architecture. Map attack paths across O-RAN interfaces, xApps, and cloud-native core before deployment.

02

Supply Chain Due Diligence

SBOM (Software Bill of Materials) for all 6G components. Third-party security audits of RAN vendors. Hardware attestation using TPM chips in all base station equipment.

03

Incident Response for 6G Networks

Dedicated 6G-CSIRT with playbooks for AI model poisoning, quantum-era decryption events, and RAN slice isolation. RTO < 15 minutes for critical infrastructure slices.

04

Continuous Security Monitoring

AI-driven Security Operations Center (SOC) integrating telemetry from O-RAN O1 interface, network function logs, and endpoint sensors across millions of 6G devices.

05

Cryptographic Agility Framework

Design 6G systems to swap crypto algorithms in-service without downtime. Critical for PQC migration as NIST standards evolve. Implement by 2027 for networks deployed in 2030.

06

Red Team / Adversarial Testing

Regular adversarial testing of xApps, O-RAN interfaces, and AI models. Purple team exercises combining ETSI NFV threat vectors with 5G/6G-specific penetration frameworks.

Global 6G Security Research Testbeds

Colosseum (Northeastern U.) — USA

Open RAN security, AI adversarial attacks on RAN

World's largest wireless network emulator. Hosts O-RAN disaggregated testbed. Research on adversarial xApp attacks, spectrum jamming, and ML-based IDS for 6G.

Open6G Center (NE/MIT) — USA

OpenAirInterface 6G stack, security prototyping

Open-source 3GPP-compliant software stack. Tests PQC integration in 6G NAS, AI-based anomaly detection in RIC, and THz physical-layer security experiments.

6G Flagship (Univ. Oulu) — Finland

End-to-end 6G security architecture

EU flagship program testing post-quantum TLS in 6G core, quantum-safe authentication protocols, and AI security frameworks for autonomous 6G management.

Hexa-X Project (Ericsson) — EU

6G security architecture & AI threats

EU Horizon 2020/2021 project. Defined 6G threat taxonomy, tested O-RAN interface security, and developed explainable AI security for network management.

Campus5G (Univ. Edinburgh) — UK

O-RAN security in campus deployment

First campus-wide O-RAN-compliant private testbed. Research on xApp integrity, O1/E2 interface authentication, and AI-RAN anomaly detection at scale.

SONIC Labs / C-DOT India — India

Open RAN security, India 6G initiative

India-UK MoU for Open RAN and AI security research. Tests supply chain security in heterogeneous RAN environments and indigenous 6G security frameworks.

Key Findings from 6G Security Experiments

AI Attack Defense *Colosseum / O-RAN Alliance*	6G-XSec (HotNets'24): Explainable edge security for Open RAN detected adversarial xApp attacks with 96.3% accuracy using random forest + SHAP explanations, enabling operator-interpretable alerts. **Validated AI-based edge security as viable for real O-RAN deployments**
ML-based RAN Security *Open6G / MIT TCCI*	MobiLLM (6GSECC'25): LLM-powered agentic framework for closed-loop threat mitigation in 6G Open RANs demonstrated automated isolation of compromised DU in <200ms upon anomaly detection. **LLMs show promise for real-time 6G security automation**
PQC Integration *6G Flagship Finland*	Successfully integrated CRYSTALS-Kyber KEM into 6G NAS (Non-Access Stratum) authentication, adding <8ms overhead — within acceptable range for 6G's sub-millisecond service requirements. **PQC is technically feasible in 6G signaling with acceptable overhead**
THz Physical Security *Northeastern U. (Keysight)*	130 GHz broadband MIMO experiments revealed that THz beamforming can achieve 32 dB sidelobe suppression, drastically limiting eavesdropping radius to <2m under realistic conditions. **THz directional security is stronger than initially feared**
Protocol Fuzzing *5GReplay / WiSec Community*	AI5GTest (WiSec'25): Automated specification-aware fuzzing of O-RAN components discovered 12 previously unknown vulnerabilities across E2/F1/O1 interfaces in commercial RAN software. **Multi-vendor O-RAN still harbors significant undiscovered vulnerabilities**

Conclusions & The Way Forward

Key Takeaways

- 6G's power (AI-native, THz, Open RAN, massive IoT) dramatically expands the attack surface compared to 5G
- Quantum computing poses an existential threat to current cryptography — PQC migration must begin now, before 6G deployment
- Open RAN's multi-vendor architecture requires mandatory security testing of xApps/rApps and strict interface authentication
- AI-driven defenses (IDS, SOAR, federated learning) are essential but themselves vulnerable to adversarial attacks
- Supply chain security and digital sovereignty are national security imperatives, not optional features
- Testbed research confirms: physical-layer, cryptographic, and AI defenses are technically ready — policy must catch up

Recommended Actions

Start PQC Migration Now

Inventory all cryptographic assets in 5G/6G systems and plan hybrid PQC transition by 2027

Mandate xApp Security Testing

Require formal verification + pen testing of all O-RAN xApps before production deployment

Establish 6G-CSIRT

Create dedicated 6G Incident Response teams with AI-specific playbooks before commercial launch

Fund Testbed Research

Expand funding for Colosseum, Open6G, 6G Flagship, and indigenous platforms like C-DOT/IIT Hyderabad

Cyber MANTHAN | IIIT Hyderabad
Securing the Networks of Tomorrow — Today