Institute for Infocomm Research
A*STAR I²R

Envisioning a Secure, Hyper-Connected Future: Cybersecurity for 5G, 6G & Beyond

Marcus Tan
Head of Cybersecurity Department
Institute for Infocomm Research (I²R)
A*STAR, Singapore
14 Nov 2025


ENVISIONING A SECURE, HYPER-CONNECTED FUTURE
CYBERSECURITY FOR 5G, 6G & BEYOND
Securing the backbone of our digital society


5G AND 6G: POWERING FUTURE ECONOMIES
5G AND 6G SECURITY IS NATIONAL SECURITY

WE'RE ALREADY BUILDING THE FUTURE—BUT CAN WE SECURE IT?

- 5G global adoption status
- 6G expected ~2030, standards in motion

OPPORTUNITY TO FIX GAPS EARLY

4G TO 5G

FROM HARDWARE TO SOFTWARE — EVERY LAYER IS NOW A TARGET

4G

Hardware-Centric

Proprietary Hardware and Software

HARDWARE

SOFTWARE

5G

Software-Centric

Expanded Attack Surface

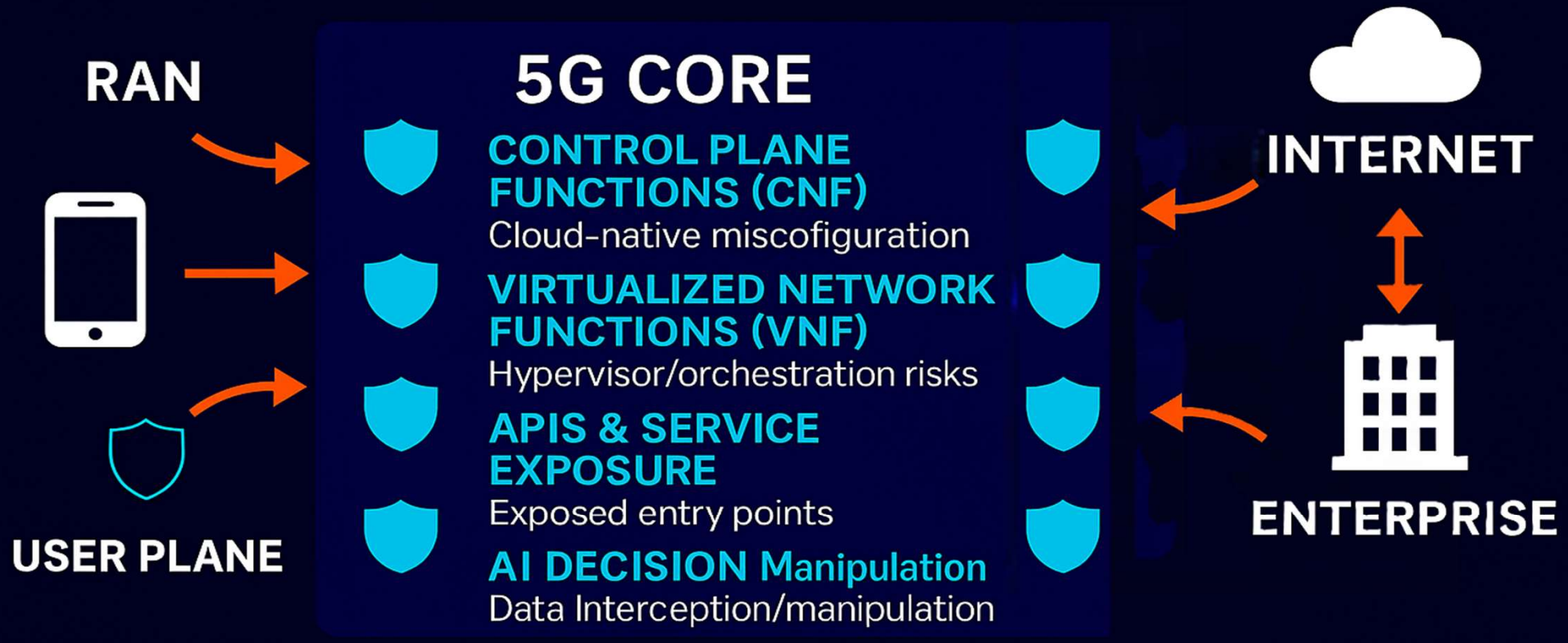
CNF

VNF

API

New Vulnerabilities Introduced

DEFENDING A VASTLY EXPANDED 5G ATTACK SURFACE



5G core connects both to RAN and the Internet—must defend from both directions.

UNIQUE CHALLENGES IN 5G

URLLC

Stricter reliability and latency requiremets

5G CORE

API & Service Exposure

Higher risk of insec-ure interfaces

AI Decision Manipulation

Subtle manipulation of input telemetry to influence

Massive IoT

Potential for large-scale botnets

Slice Misconfiguration

Faulty isolation between network slices

PRIVATE 5G OPPORTUNITIES

OT/IT Convergence

Merging of OT + IT
= new vulnerabilities

Market Opportunity

Multi-billion-dollar
private 5G market

PRIVATE 5G CORE

Private 5G as a Service (P5GaaS)

5G Service Providers or Telcos

Enterprise Infrastructure Integration

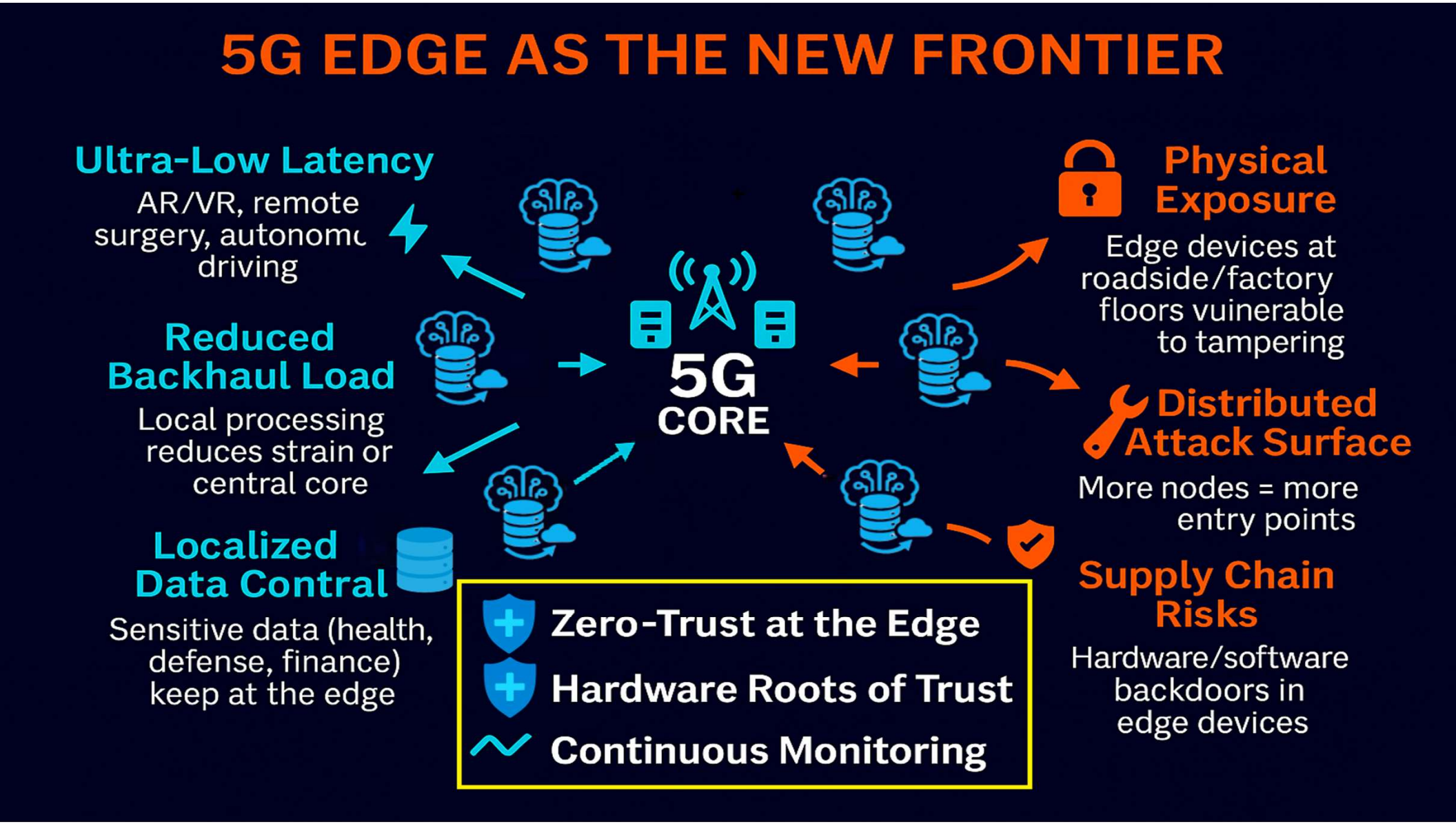
Becomes part of core
enterprise systems

Skill Gap & Risks

Enterprises lack
telco-grade expertise

Enterprises are becoming their own telcos - unlocking values but also inheriting security responsibilities

5G EDGE AS THE NEW FRONTIER



5G TO 6G

FROM 5G TO 6G – AI BECOMES CENTRAL TO NETWORKS

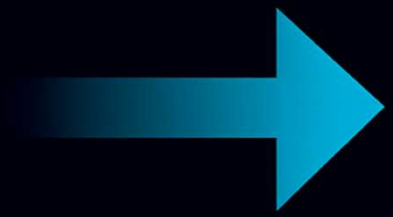
5G

Software-Centric

Expanded Attack Surface

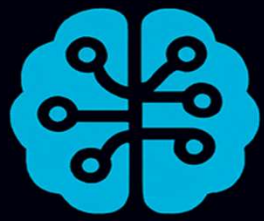
Optional Helper

SOFTWARE



6G

AI-Native by Design



Real-Time Autonomous Resource Management

AI-Driven Air Interface Optimization

Native AI Model Hosting and Training at the Edge

RISKS

POTENTIAL 6G AI VULNERABILITIES (1)

AI Model Poisoning

Attackers inject malicious samples into training pipelines to corrupt AI models

Adversarial Input Exploits

Carefully crafted RF signals are designecd to deceive AI classifiers

Model Extraction & IP Theft

Reverse-engineering AI models to capture proprietary network control logic

AI Decision Manipulation

Subtle manipulation of input telemetry to influence AI thresholds

POTENTIAL 6G AI VULNERABILITIES (2)

Bias & Discrimination Risks

Embedded biases in AI-driven QoS/resource allocation

Over-Reliance on AI Autonomy

AI failures go unchecked due to human detachment

AI Supply Chain Risks

Pre-trained models or update pakages being tampered in upstream

Privacy Leakage from Edge AI Training

Training at edge may leak sensitive user data

OTHER 5G/6G PRIVACY & SECURITY CHALLENGES

User Privacy – ISAC

Threat : Continuous sensing without consent

Impact: Mass surveillance at infrastructure scale

Roaming Security – 5G to 4G or lower

Enforce consistent security policies (ciphering, keys, integrity)

Ensure slice-level policies survive roaming / fallback

CRITICAL: Uniform security policies across mixed generations of networks

DEFENCE & RESILIENCE

WHEN THE BRAIN OF THE NETWORK IS UNDER ATTACK

AI-DRIVEN DEFENSE

AI augments perimeter defenses with adaptive learning and rapid response

ADVERSARIAL MACHINE LEARNING

Detecting and defending against AI-optimized evasion techniques

POISONED MODELS

Identifying and isolating manipulated training data or infected endpoints

When the brain falters, the entire nervous system—the network—faces jeopardy.

ZERO TRUST AS THE SECURITY BACKONE

MULTI-SLICE TRUST
Independent policies
for IoT, enterprise, URLLC

ADAPTIVE POLICIES
Adjust rules
dynamically to threats

CONTINUOUS AUTHENTICATION
Verify identity
in real time

LOW-LATENCY CONSTRAINT (URLLC)
Security must not
add delays

Telecom Cybersecurity Innovation Centre (TCIC)

Telecom Cybersecurity Innovation Centre (TCIC)

TELECOM CYBERSECURITY INNOVATION CENTRE (TCIC)

Funding Source: Cybersecurity Agency of Singapore (CSA); through the Cybersecurity Research Programme Office (CRPO)

Duration : 1 Jan 2025 – 30 Jun 2026 (18 months for Phase 1)

Principal Investigator : A*STAR Institute for Infocomm Research (I^2R)

Collaborator : ST Engineering. Global technology, defence & engineering powerhouse headquartered in Singapore. Specialise in Aerospace, Smart City Solutions, Defense, Digital Tech and Cybersecurity.

Key Feature : 5G Cybersecurity end-to-end, from R&D all the way to translation & commercialisation.

R&D → Commercialisation

TCIC Project Objective

Tagline : ***Building Resilience and Trust in Singapore's Telecom Infrastructure***

Unlike other IT security vendor solutions which are enterprise IT centric, our Private 5G Cybersecurity Solution helps private 5G service operators & critical infrastructure owners who want to detect & mitigate cyber threats in real-time by leveraging AI-driven analytics on telecom infrastructure traffic & enhancing the resilience of their 5G networks.

Scope :

To design & develop the following technologies for Private 5G Networks :

- 5G Attack Platform
- 5G Security Integrated Platform

R&D → Commercialisation

TCIC Work Packages

Work Package 1 : ***5G Cybersec R&D Development Environment***

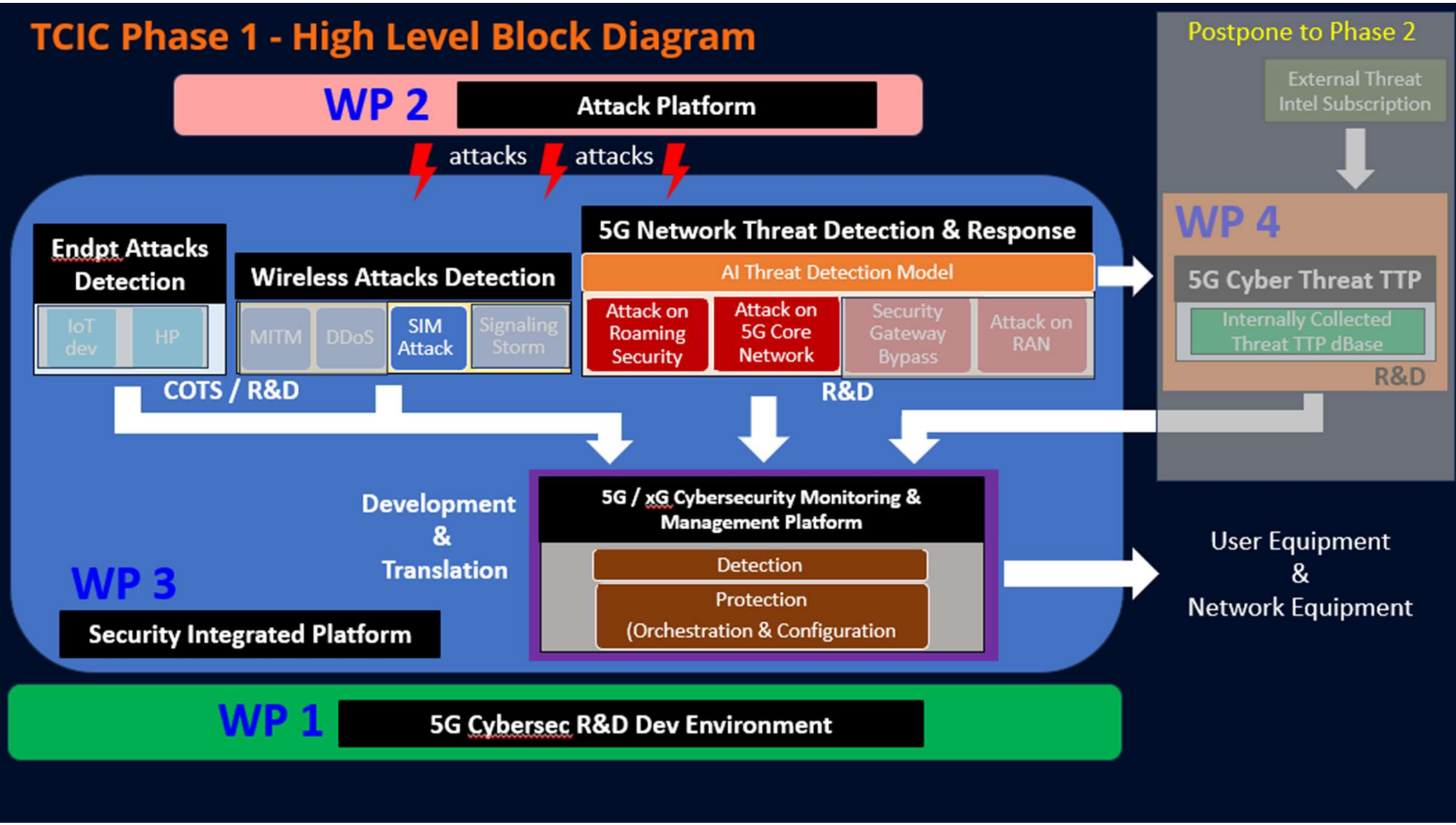
The underlying hardware + software infra for other work packages to build upon.
CD/CI environment to facilitate R&D, translation to commercialization.

Work Package 2 : ***5G Attack Platform***

- Platform to implement various attacks applicable to 5G networks
- Extensible for future attack implementation
- Commercialisation target : 5G Security Audit Platform

Work Package 3 : ***5G Security Integrated Platform***

- Network Threat Detection & Response (Signature + AI-based)
- Cybersecurity Monitoring, Orchestration & Configuration (Agentic AI)
- Commercialisation target : Cybersecurity solution for Private 5G SOC


TCIC Phase 1 - High Level Block Diagram
WP 2
Attack Platform
attacks
attacks
Endpt Attacks Detection
IoT dev
HP
Wireless Attacks Detection
MITM
DDoS
SIM Attack
Signaling Storm
5G Network Threat Detection & Response
AI Threat Detection Model
Attack on Roaming Security
Attack on 5G Core Network
Security Gateway Bypass
Attack on RAN
COTS / R&D
R&D
Postpone to Phase 2
External Threat Intel Subscription
WP 4
5G Cyber Threat TTP
Internally Collected Threat TTP dBase
R&D
Development & Translation
WP 3
Security Integrated Platform
5G / xG Cybersecurity Monitoring & Management Platform
Detection
Protection (Orchestration & Configuration
User Equipment & Network Equipment
WP 1
5G Cybersec R&D Dev Environment

STATUS

Work Package 1 : ***5G Cybersec R&D Development Environment***

Infra is up and available for R&D work in WP 2 & 3.

Work Package 2 : ***5G Attack Platform***

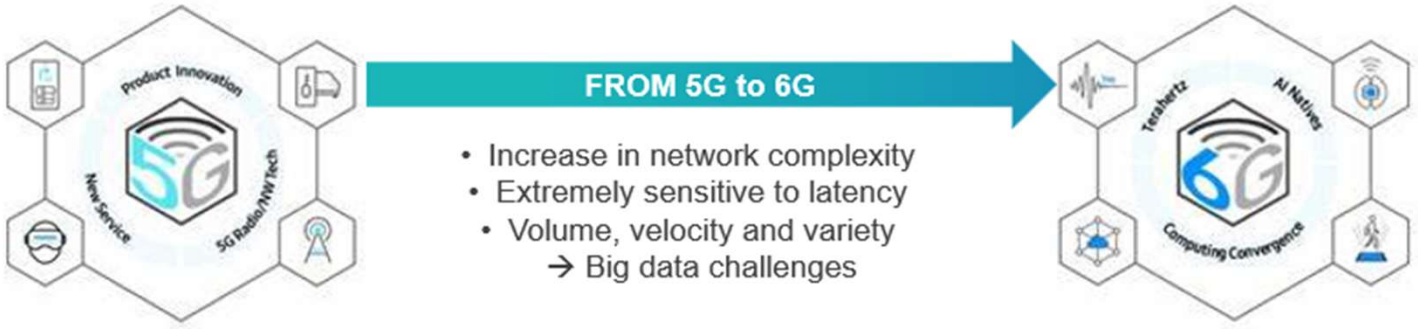
- 2 attacks implemented, others in progress

Work Package 3 : ***5G Security Integrated Platform***

- Work in progress

VISION FOR TCIC

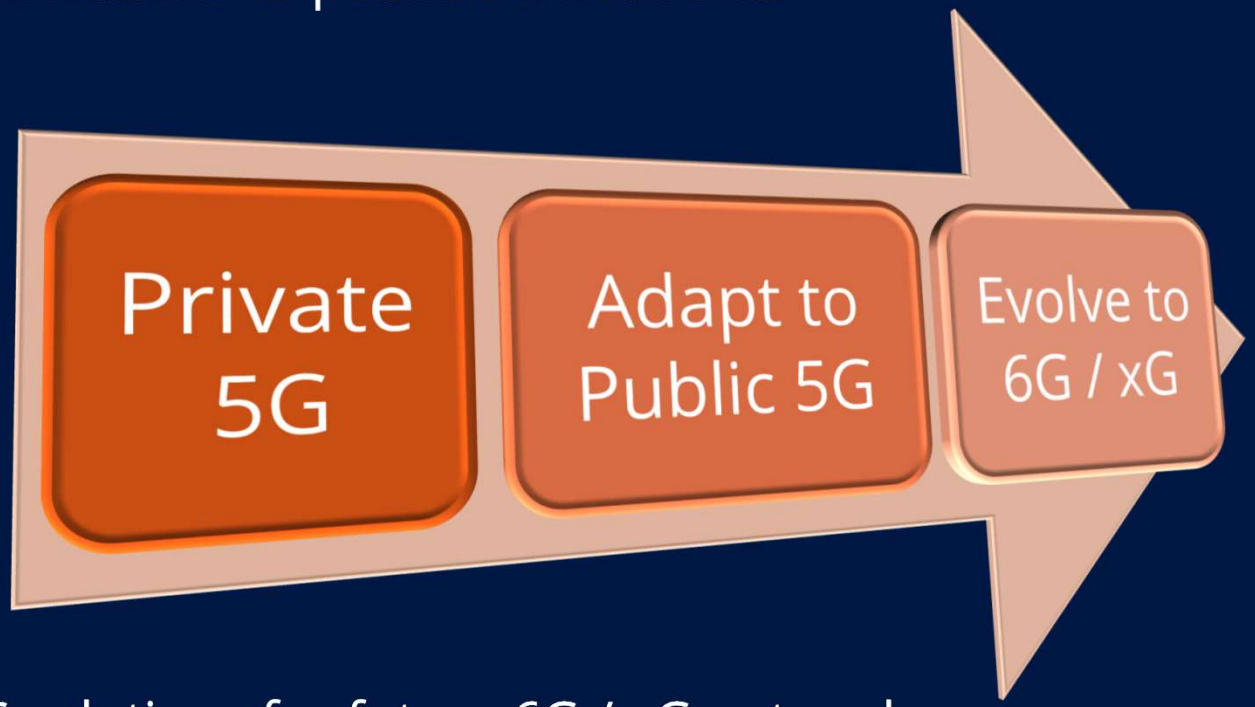
As a National Centre of Excellence in Telecom / Mobile Network Cybersecurity R&T in Singapore



Telecom Cybersecurity Innovation Centre (TCIC) A leading R&T and innovation hub in cybersecurity for 5G and beyond, advancing cybersecurity technologies and end-to-end network visibility to secure the smart cities.

MISSION FOR TCIC

- To adapt TCIC solutions to public 5G networks

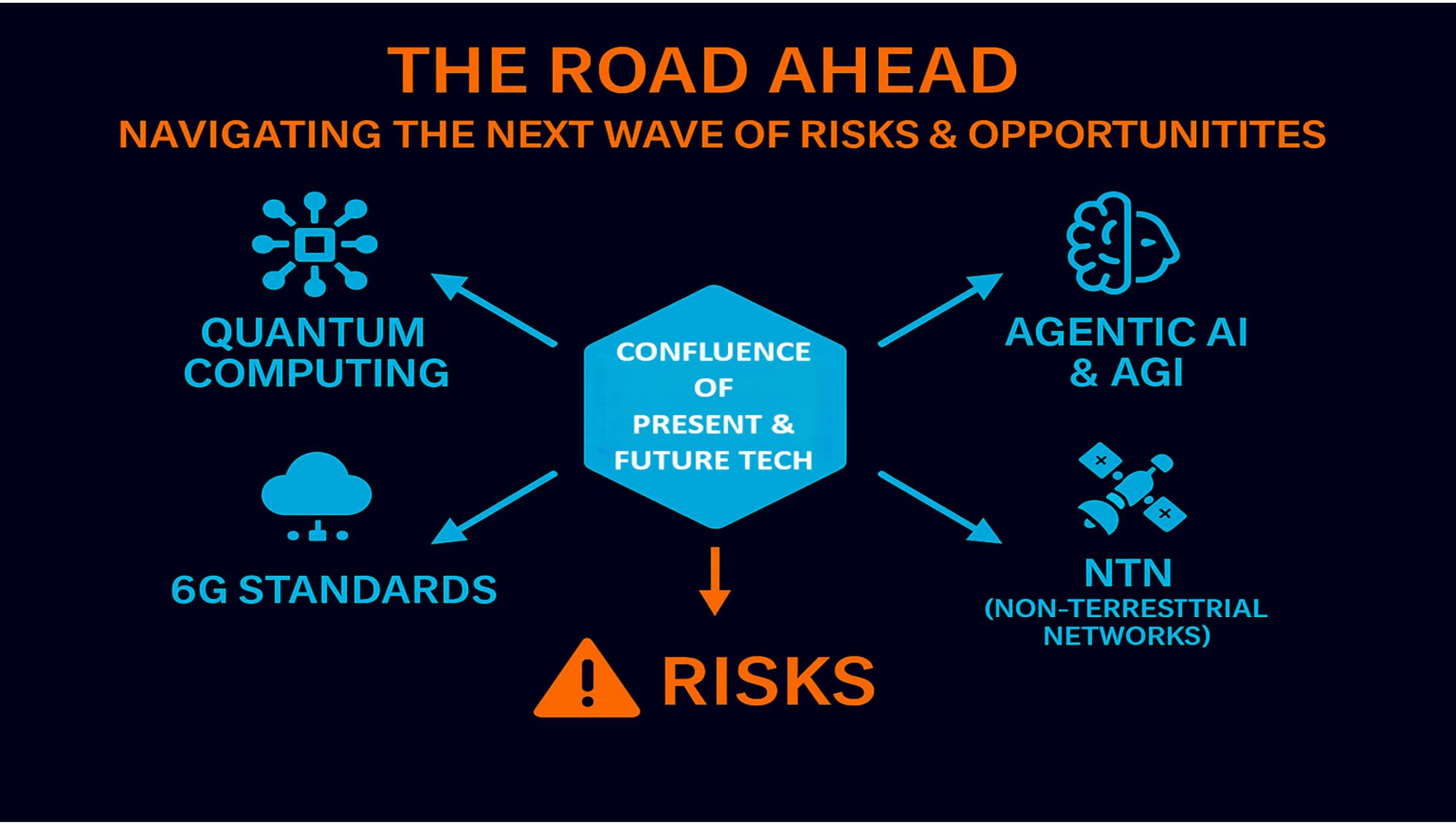


- To evolve TCIC solutions for future 6G / xG networks

Conclusion

THE ROAD AHEAD

NAVIGATING THE NEXT WAVE OF RISKS & OPPORTUNITITES



FINAL TAKEAWAYS

Key Opportunities

Hyper-connected future, faster speed, multiple devices, intelligent services

Key Risks

- AI Risks
- Security policy consistency across nodes, layers & networks
- User privacy leakage
- Emerging new attacks

Securing the Future of Communication

Institute for Infocomm Research
A*STAR I²R

THANK YOU

ASTARSG ASTAR-SG