Security Concerns for 5G/6G Mobile Network Technology

Col (Dr) Inderjeet Singh
Chief Cyber Officer
Vara Technology

2030 use case examples

Use case scenarios enabled by the network platform

The Internet of Senses

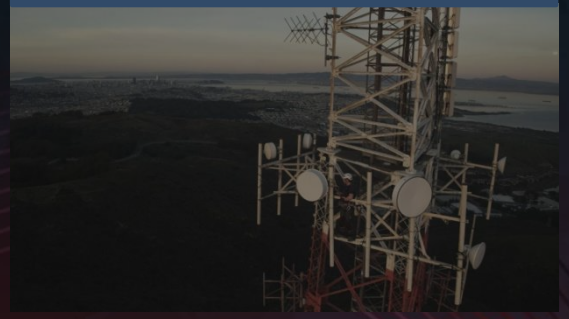
Connected Intelligent Machines

Digitalized & programmable physical world

Connected sustainable world

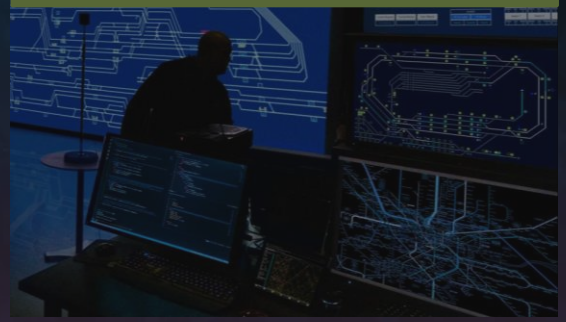
Use case focus

Limitless connectivity



Trustworthy Systems

Cognitive network



Network compute fabric

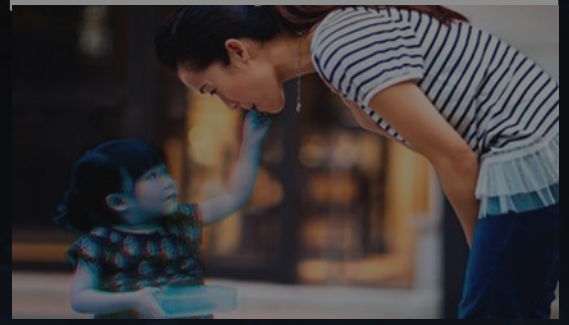
Technology focus

Technology scenarios evolving the network platform

Tech scenarios evolving the network platform

Use case scenarios enabled by the network platform

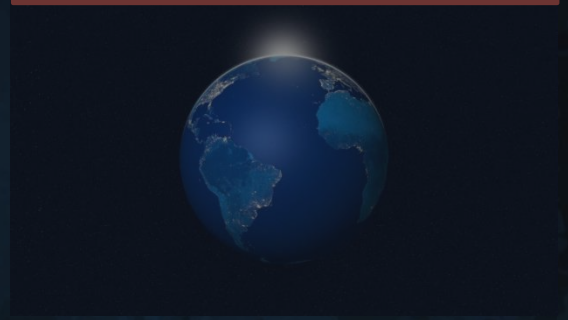
The Internet of Senses



Connected Intelligent Machines

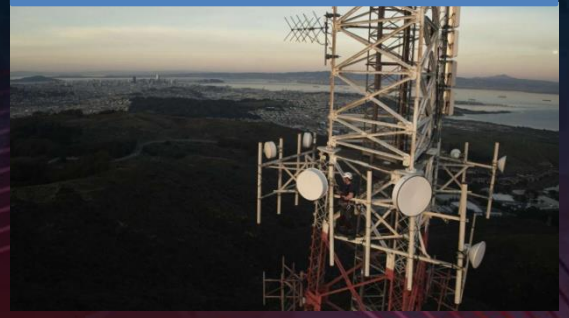
Digitalized & programmable physical world

Connected sustainable world



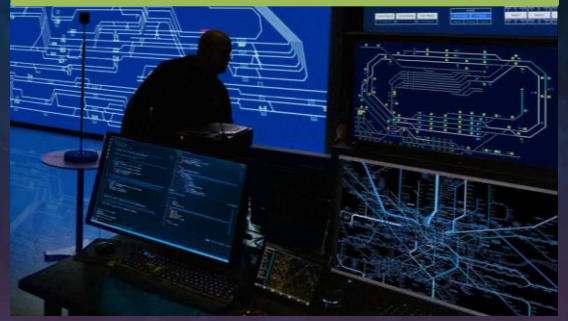
Use case focus

Limitless connectivity

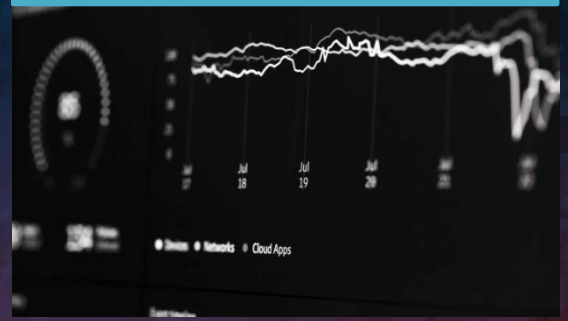


Trustworthy Systems

Cognitive network



Network compute fabric



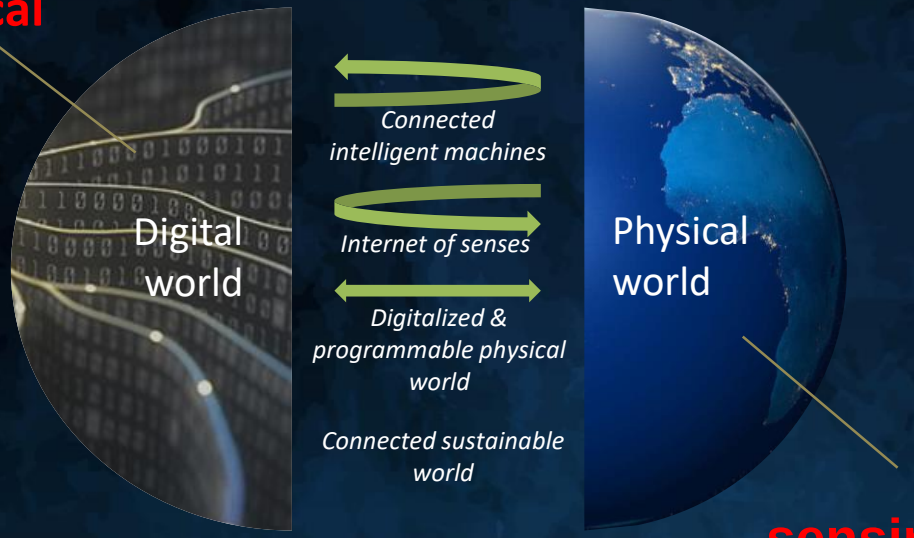
Technology focus

Technology scenarios evolving the network platform

6G – Moving in a cyber-physical continuum

Programmable digital representation of the physical world

Cyber-physical continuum



Vast amounts of sensors embedded in physical world send data to update the digital representation in real time

Actuators in the real world carry out functions that is programmed in the digital representation

The network provides intelligence, ever-present connectivity, and full synchronization in a cyber-physical continuum

The physical world of sensing, action, and experience

Evolution of Mobile Security Landscape from 4G towards 6G

- MAC layer threats
e.g. Mobile ware,
APT/DDoS
Malicious Apps

Mobile Applications

Richer Content (Videos)

4G

LTE, LTE Advanced

2010

- Cyberware and critical infrastructure threats
-SDN/NFV threats
-Cloud computing related threats

URLLC

mMTC

eMBB

Cloud Computing

5G

NR, SDN, NFV, NS

2020

-AI/ML based intelligent attacks
-Zero day attacks
-Quantum attacks
-PHY layer attacks for VLC, THz, etc.

Automation

Connected Intelligence

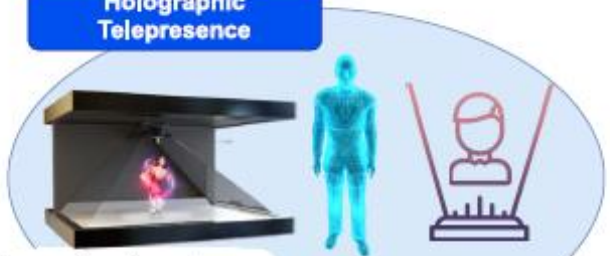
6G

AI/ML, Blockchain, VLC, THz, Quantum computing

2030

Key Security Requirements of Prominent 6G Applications

Holographic Telepresence



- Reduced operational cost
- Diversity of devices
- High Bandwidth
- High Privacy

Extended Reality

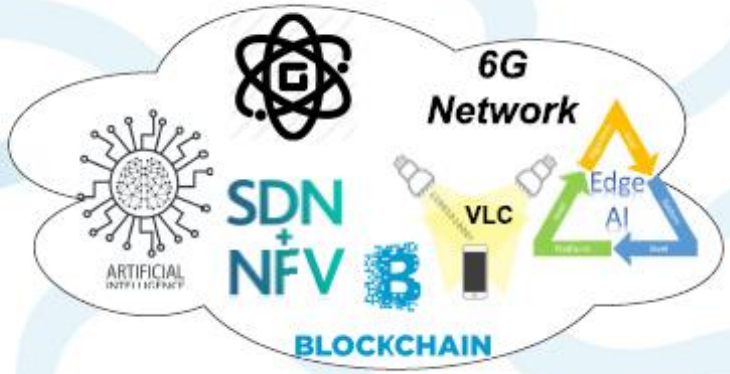
- Reduced operational cost
- Diversity of devices
- Limited Resources
- High Privacy

Connected Autonomous Vehicles (CAV):

- Reduced operational cost
- Diversity of devices
- Interoperability
- Realtime Operation
- High Scalability

UAV based Mobility

- Reduced operational cost
- Diversity of devices
- Interoperability
- Realtime Operation
- High Scalability



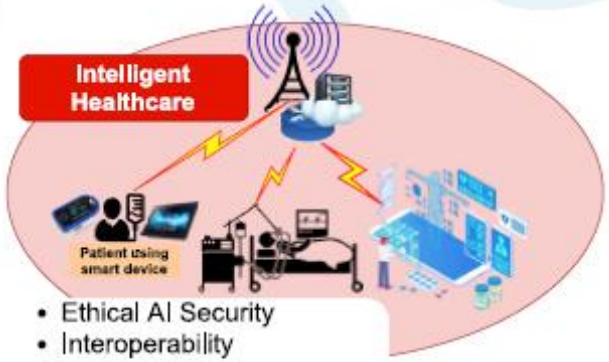
Smart Grid 2.0

- Terrorist Attacks
- Scalable IoT Security
- Physical Tampering
- Intermittent Connectivity

Digital Twin

- Secure Communication
- High Scalability
- IoT data security
- AI security

Intelligent Healthcare



- Ethical AI Security
- Interoperability
- Realtime Operation
- High Privacy
- Sacable IoT data security

Industry 5.0

- Reduced operational cost
- Interoperability
- Realtime Operation
- High Scalability
- IoT data security

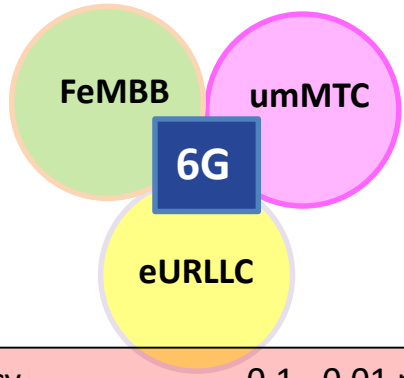
6G Landscape and Security Composition

6G Applications

- Industry 5.0
- UAV based Mobility
- Connected Autonomous
- Vehicles (CAV)
- Smart Grid 2.0
- Collaborative robots
- Hybrid - Intelligent healthcare
- Digital Twin
- Extended Reality

New Security requirements
New Stakeholders
New Attackers

6G Requirements



Latency	0.1 - 0.01 ms
Leal data rate	> 1 tbps
Movability	1000 kmh
Aria traffic capacity	1 Gbm2

6G Landscape and Security Composition

Attack on 6G Architecture (AI compromises, physical attacks, physical layer attacks,...)

Attacks on key 6G technologies (Poisoning attacks, eavesdropping, ...)

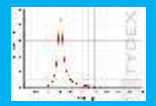
6G Architecture

- Intelligence Network Management
- Edge Intelligence
- Intelligence Radio

6G technologies

- AI
- DLT
- Quantum Communication
- THZ Bands
- VLC




AI/ML threat scope and security issues in 6G networks

Security challenges

- Visibility
- Trustiness
- Ethical and Legal aspects
- Extensibility and viability
- Controlled security tasks
- Adaptability of models

Attacks and threats

- API-based attacks
- Poisoning attacks
- Evasion attacks
- Physical layer attacks
- Model inversion attacks
- AI middleware layer attacks
- Model stealing attacks

6G Security Considerations

Hardware to Applications

Authentication Methods

Quantum Computing Considerations

Optimization

Short-Lived Networks

Asymmetric Cryptography

Cloud

Dynamic Flexible

Credential Storage In End – Device

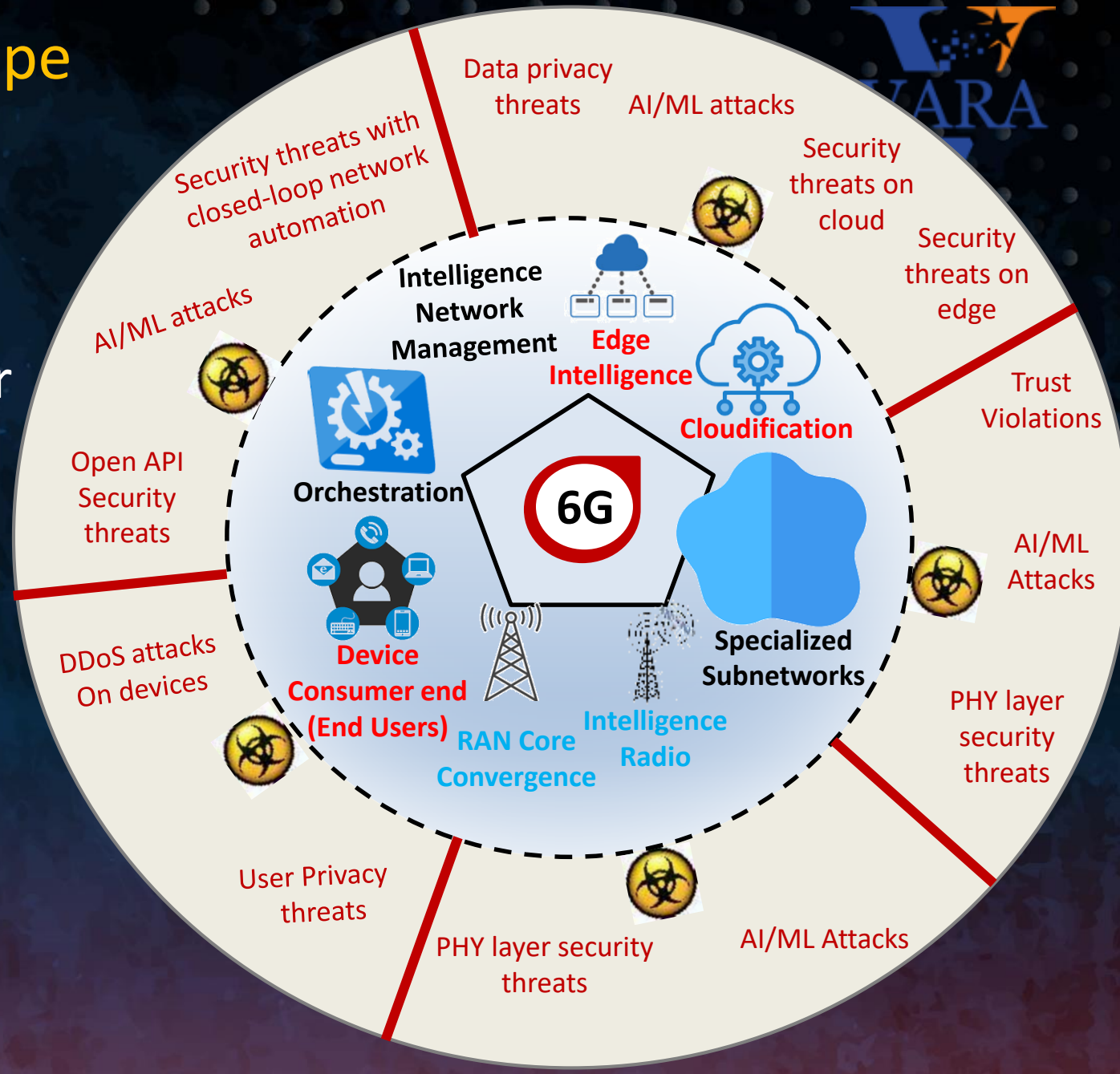
Visibility and configurability

New cryptographic algorithms

Interconnect Security

6G Security Threat Landscape

- 6G architectural innovation, decomposes the data and information architecture into four segments, namely,
  - **Platform**
  - **Functions**
  - **Orchestration**
  - **Specialization**



Thank You

Contact Me on Social Media:

Facebook: InderBarara
Twitter Handle: @InderBarara
LinkedIn: Inder Barara
Website: https://www.cybersleuths.io/

Mobile: +919818005945
Email: inderjit.barara@gmail.com