Mobile Privacy in 2025

Dr. Ravishankar Borgaonkar

Kaitiaki Labs LLP & University of Oxford

21 September 2017

Outline

- Cellular Networks
- 1G to 4G – architecture
- 1G to 4G - vulnerabilities
- 5G architecture
- 5G vision 2025
- Security challenges

Magic of Cellular Networks

- First demonstration in 1877 – Stockholm, Sweden
- “Telephone is the instrument of Devil” **
- Innovations - wireline (1877) to wireless (2017)

- Foundation – **seamless connectivity and low latency**
- Features - quality of service & availability

** & Figure Source- Ericsson History

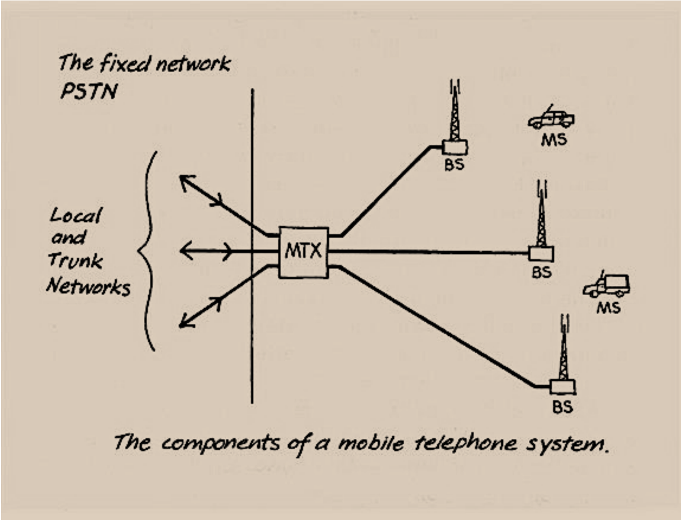
1G Networks to 4G

- No authentication & encryption
- Heavy devices
- No roaming – international calls

1G

- Authentication & encryption
- Smart devices
- Roaming and high speed Internet

4G



The components of a mobile telephone system.

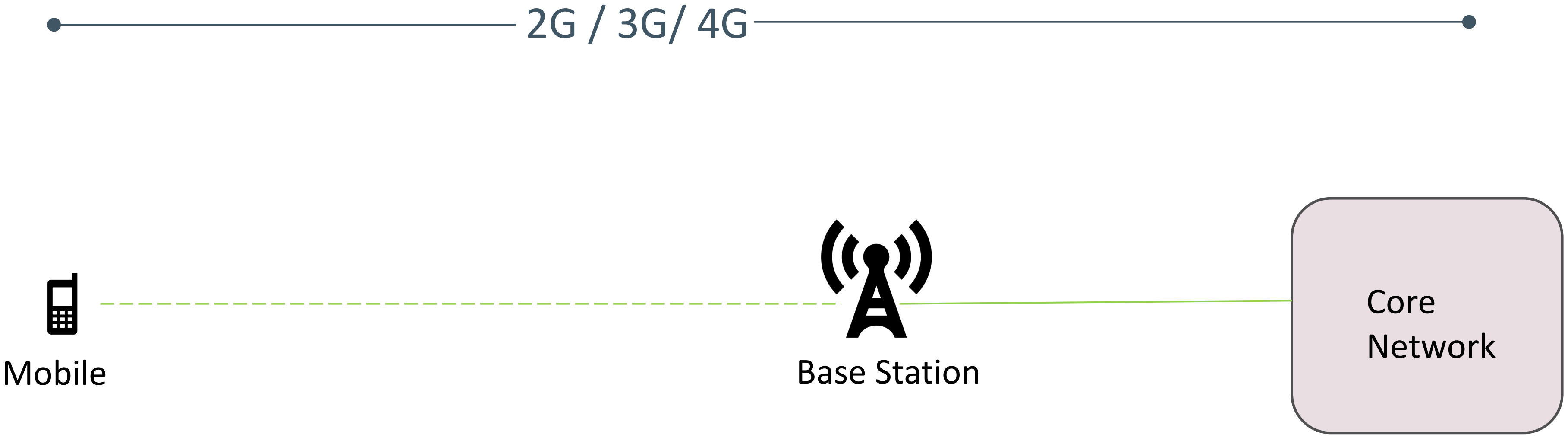
figure- Ericsson History

Design Stakeholders

- Cellular network providers
- End-user equipment vendors
- Standard organizations
- Infrastructure & support services
- Over-The-Top services

vodafone
Telia
Lycamobile
Call the world for less
ERICSSON
HUAWEI
NOKIA
SAMSUNG
oppo
HUAWEI
vivo
G
HUAWEI
QUALCOMM
intel
MEDIATEK
SAMSUNG
G&D
Giesecke & Devrient
Creating Confidence.
gemalto
security to be free
ETSI
World Class Standards
3GPP
A GLOBAL INITIATIVE
GSMA

Secure Cellular Communication



2G / 3G/ 4G

Mobile

Base Station

Core Network

Authentication

Availability

Confidentiality

Integrity

Are we secured?

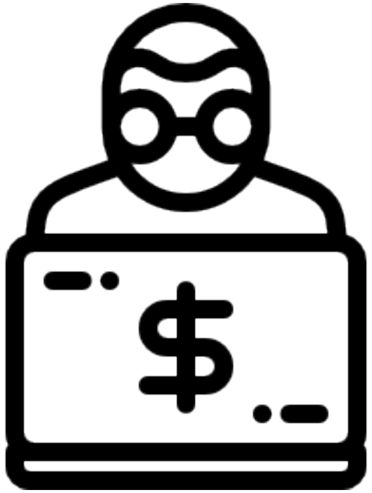
Privacy Assets

- Device information
  - IMEI, identities etc.
  - Location data
  - Sensitive data (for example user health info)

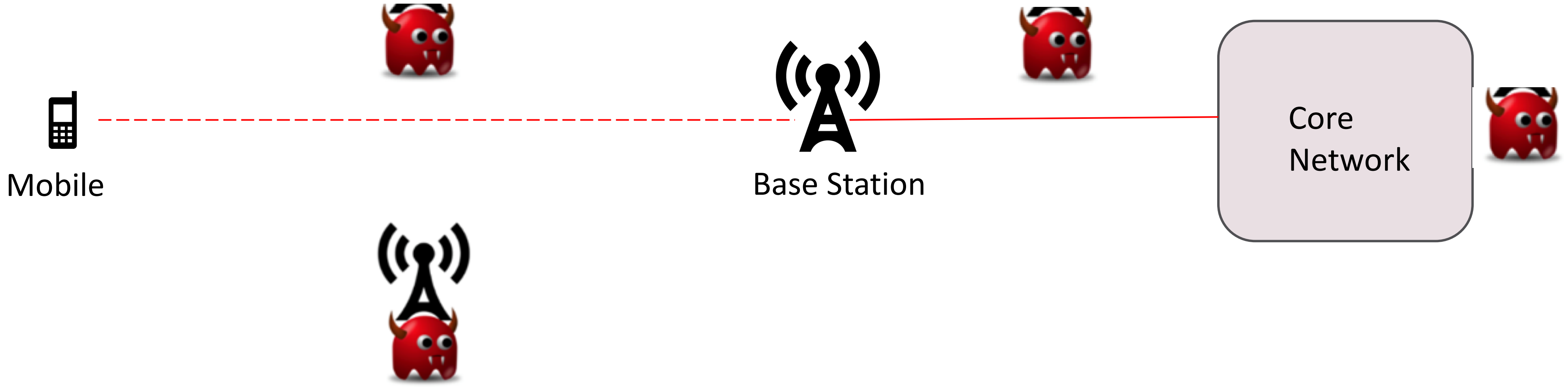
- Personal information
  - IMEI,IMSI, phone number etc.
  - SMS and call/Internet data
  - Location data

Attackers

- Fraudsters
- Cyber criminals
- Insider threats
- Cyber warfare actors (arguable)



Threats and Attacker Model



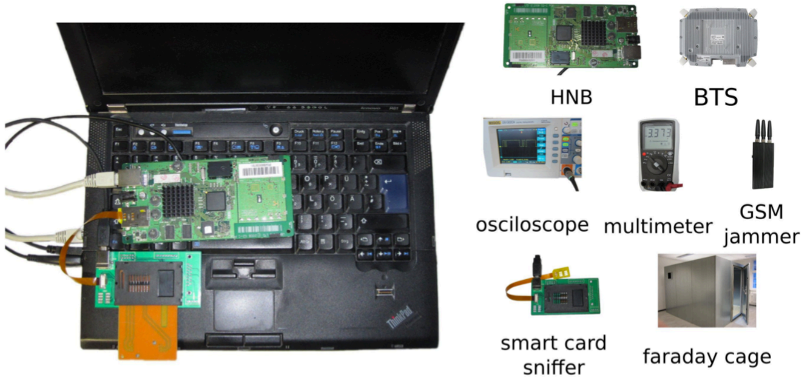
Vulnerabilities & Attacks

Mobile
Base Station

IMSI Catchers

Attacks against 3 operating systems

- Baseband, (U)SIM & Android vulnerabilities



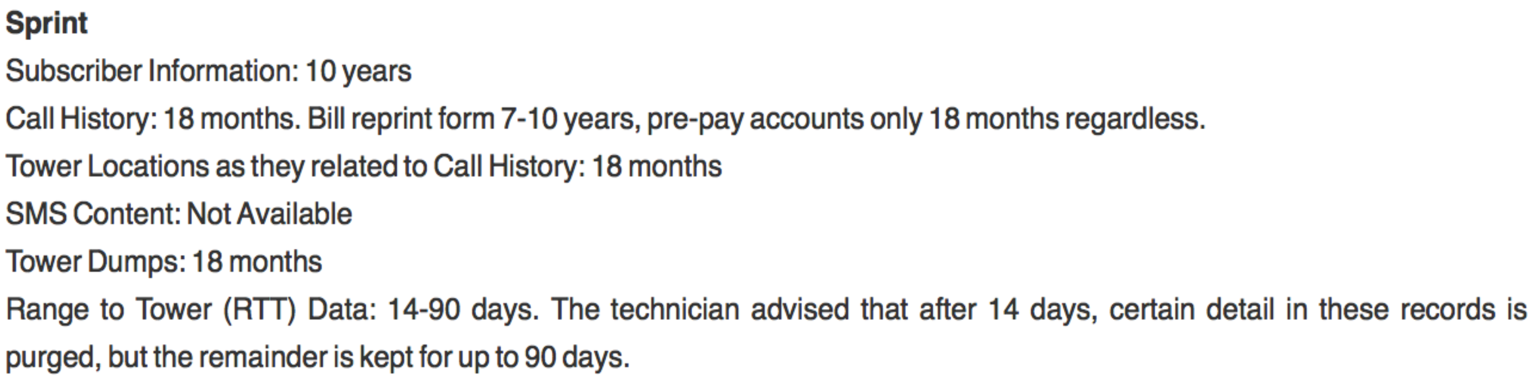
Practical attacks on core network and end-users

- architecture issues and risks

Standards & Regulations

Cellular Security Standards

- Standardization bodies
  - 3GPP (3rd Generation Partnership Project)
  - ETSI (European Telecommunications Standards Institute)
  - GSMA (GSM Association)
  - ITU (International Telecommunication Union)
- Mandatory security and privacy requirements
- International and national regulations (use of encryption, data retention)



Sprint

Subscriber Information: 10 years

Call History: 18 months. Bill reprint form 7-10 years, pre-pay accounts only 18 months regardless.

Tower Locations as they related to Call History: 18 months

SMS Content: Not Available

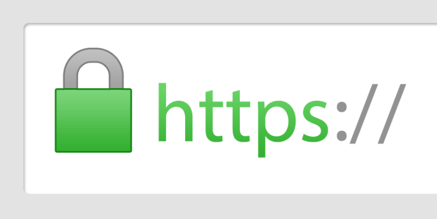
Tower Dumps: 18 months

Range to Tower (RTT) Data: 14-90 days. The technician advised that after 14 days, certain detail in these records is purged, but the remainder is kept for up to 90 days.

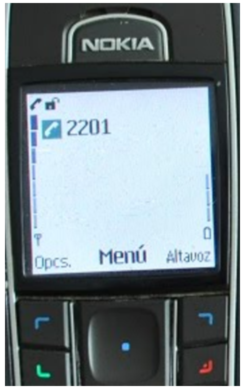
Standards & Deployment Issues

Security Indicators on Mobile

- Padlock symbol for HTTPS



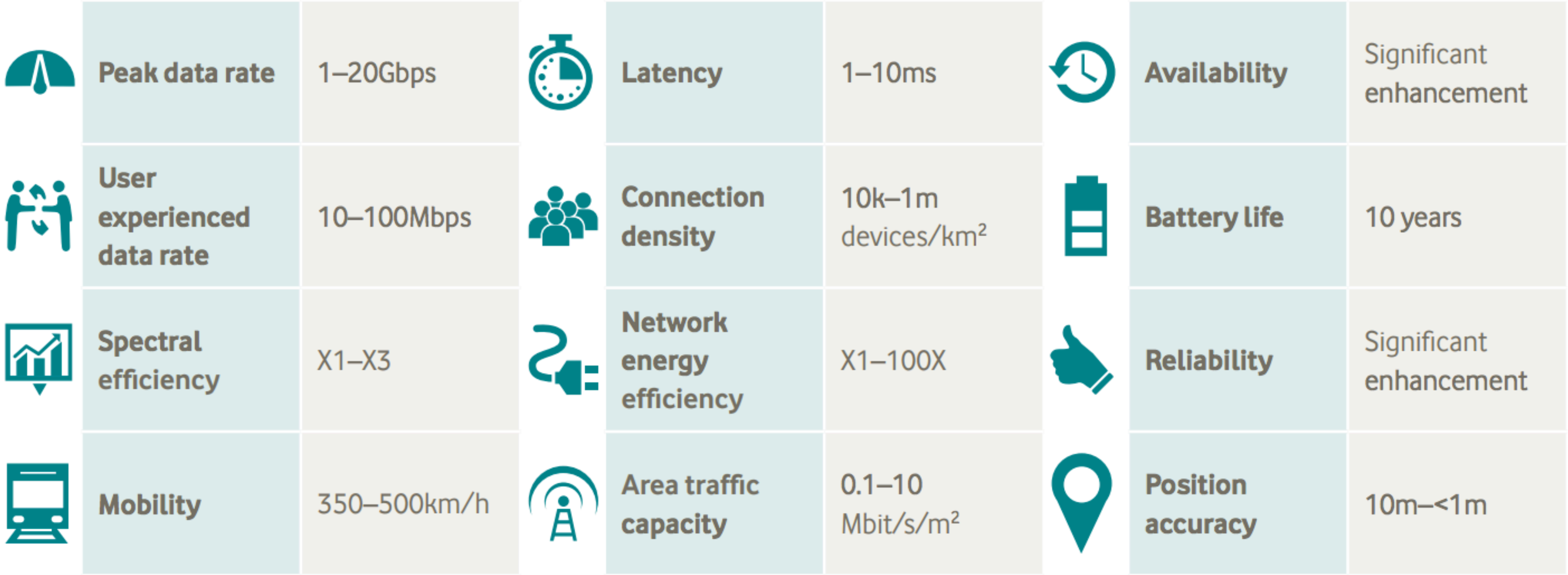
- Have you seen during mobile call lately?



5G Networks

- 5G- Next generation cellular networks
  - Handles more data
  - Connects more devices
  - Low latency
  - More reliability
- 1-10 Gbps speed
- Driven by new use-cases, for example
  - Connected driverless cars
  - Remote surgery

5G Networks Characteristics



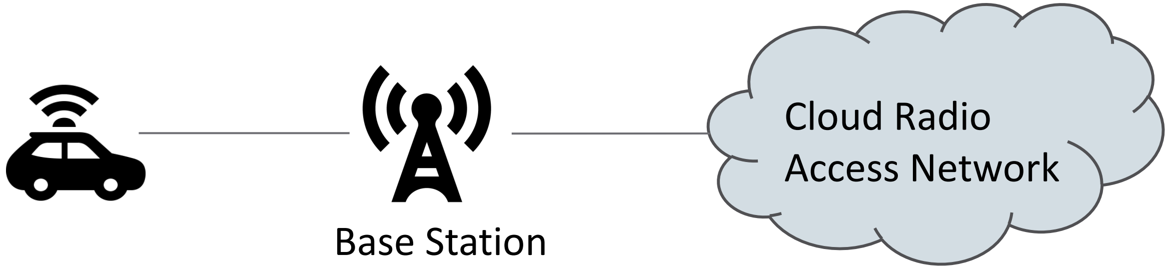
Peak data rate	1–20Gbps	Latency	1–10ms	Availability	Significant enhancement
User experienced data rate	10–100Mbps	Connection density	10k–1m devices/km^2	Battery life	10 years
Spectral efficiency	X1–X3	Network energy efficiency	X1–100X	Reliability	Significant enhancement
Mobility	350–500km/h	Area traffic capacity	0.1–10 Mbit/s/m^2	Position accuracy	10m–<1m

Figure Source- Vodafone

Cloud-Native 5G Architecture

Moving towards network softwarization and programmability

- Radio network
- Network clouds
- SDN (Software-Defined Networks)
- NFV (Network Functions Virtualization)



Vision 2025 – 5G

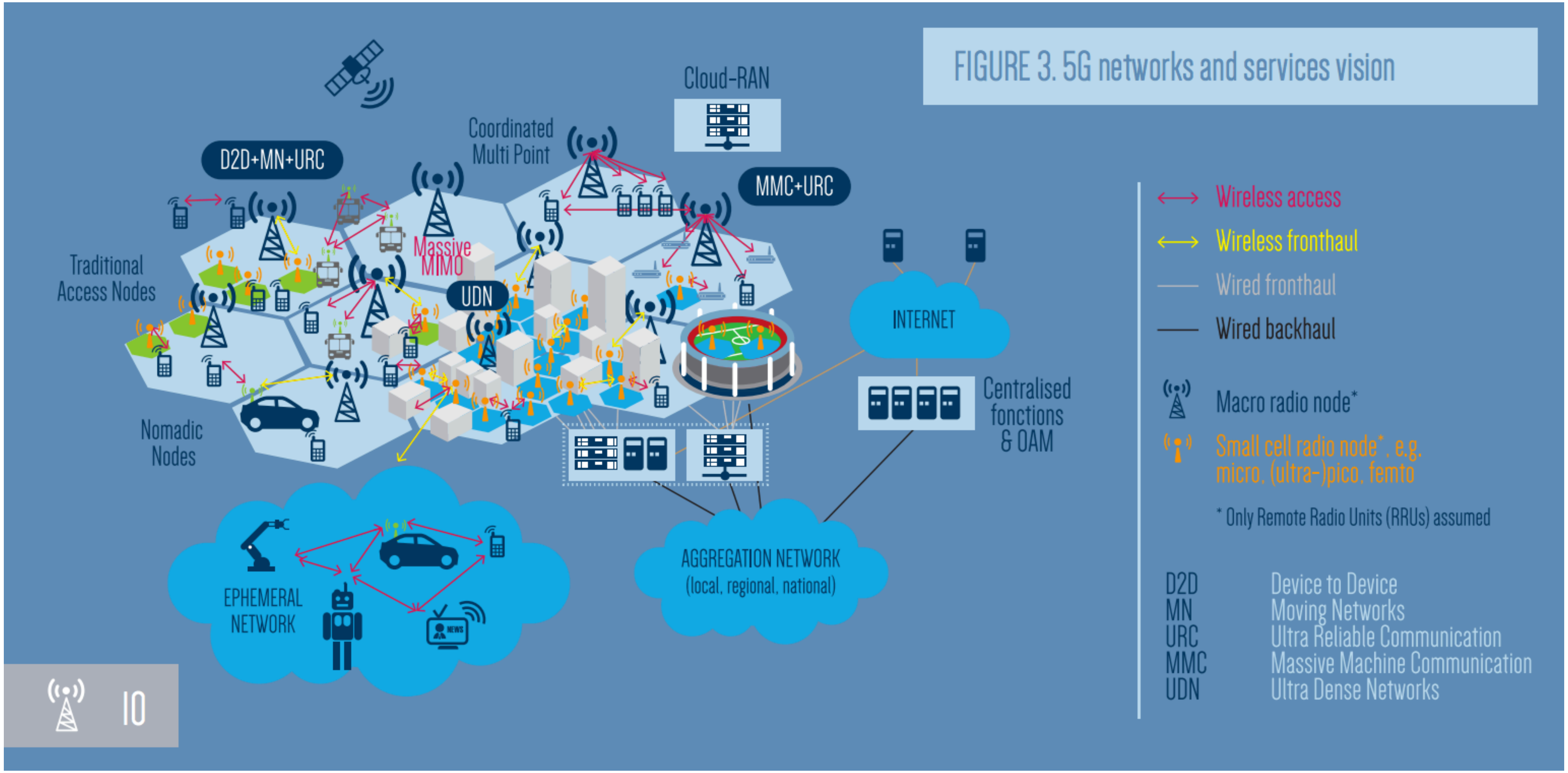
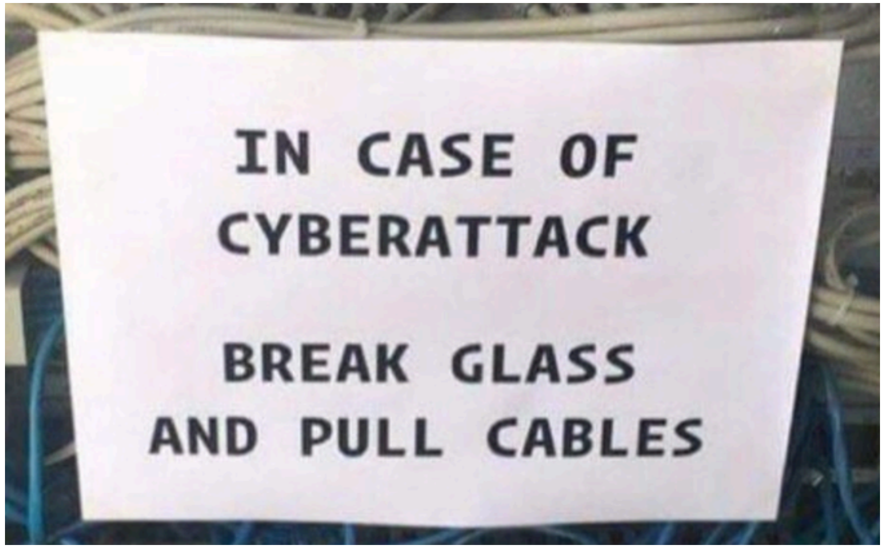


FIGURE 3. 5G networks and services vision
Cloud-RAN
Coordinated Multi Point
D2D+MN+URC
MMC+URC
Traditional Access Nodes
Massive MIMO
UDN
Nomadic Nodes
INTERNET
Centralised fonctions & OAM
EPHEMERAL NETWORK
NEWS
AGGREGATION NETWORK (local, regional, national)
Wireless access
Wireless fronthaul
Wired fronthaul
Wired backhaul
Macro radio node*
Small cell radio node*, e.g. micro, (ultra-)pico, femto
* Only Remote Radio Units (RRUs) assumed
D2D Device to Device
MN Moving Networks
URC Ultra Reliable Communication
MMC Massive Machine Communication
UDN Ultra Dense Networks
10

Figure Source- 5GPPP Project

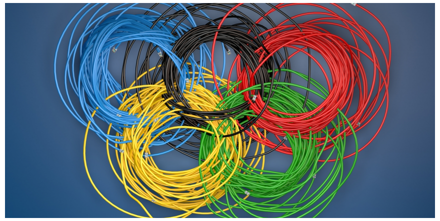
5G Devices in 2025?

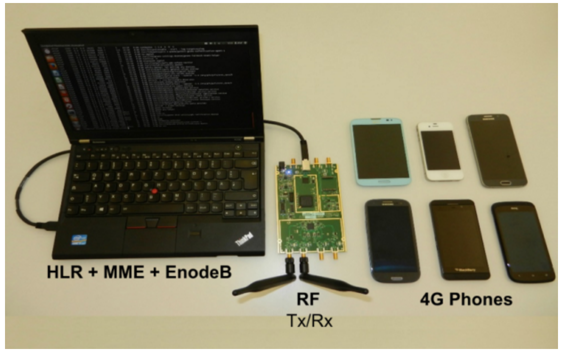
- Non-removable USIM cards - eSIM era
- Non-removable battery
- Change cellular operator without going to a shop and USIM
- Always connected (5G speed > WiFi speed)
- Small cells – connected to clouds

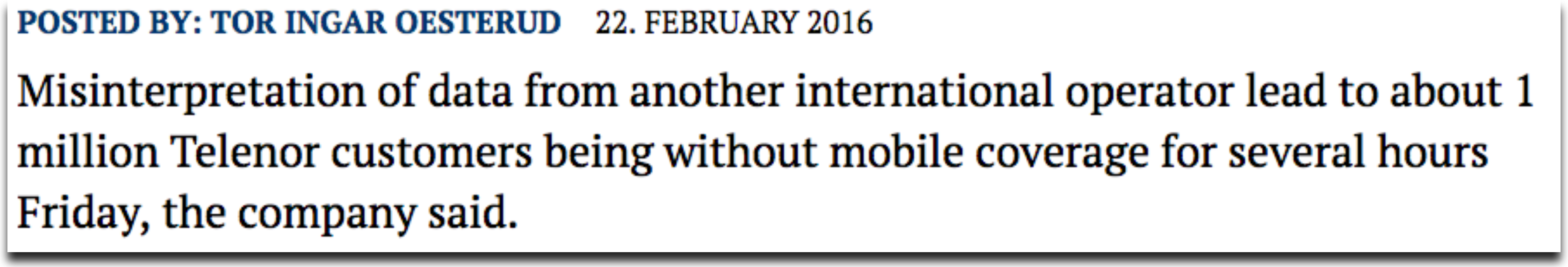


Current Cellular Network Issues

- Privacy engineering
- OS and Baseband software update
- Targeted attacks
- Capability to detect threats







POSTED BY: TOR INGAR OESTERUD 22. FEBRUARY 2016

Misinterpretation of data from another international operator lead to about 1 million Telenor customers being without mobile coverage for several hours Friday, the company said.

5G Privacy Challenges for 2025

- Radio interface security
  - Essential for delivery drones and self-driving connected cars
- Mandatory security measures in the network
  - Protection of cellular data in third party services (cloud)
  - Quantum safe cryptography techniques
- Regulatory framework
  - Privacy awareness and laws
  - Effective policies and enforcements
  - Data retention
- DoS attacks
- Security in SDN and NFV

Thank You.

Questions