SINTEF

5G Security in the Information Age

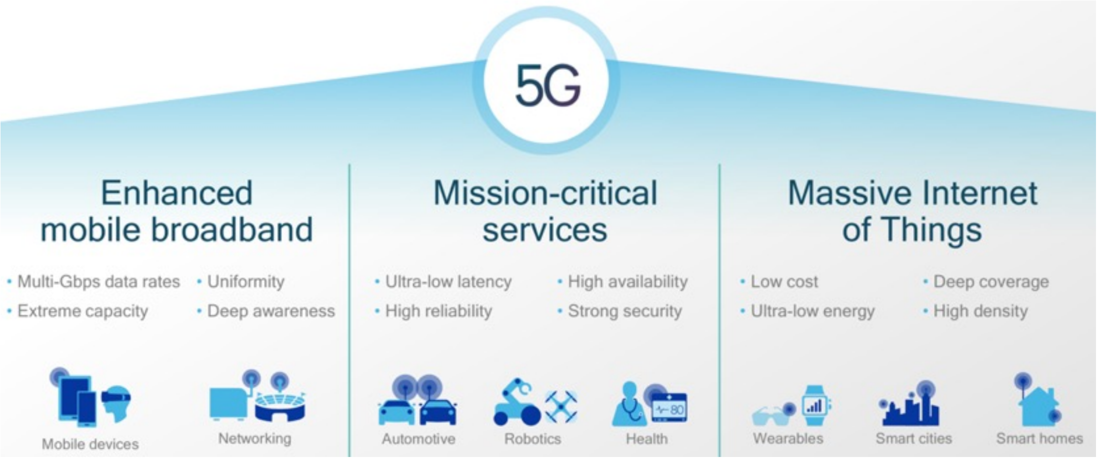
Dr. Ravishankar Borgaonkar, Senior Research Scientist, SINTEF Digital

FINSE Winter School , 29 April 2022, Norway

Source: Equinix

5G Networks

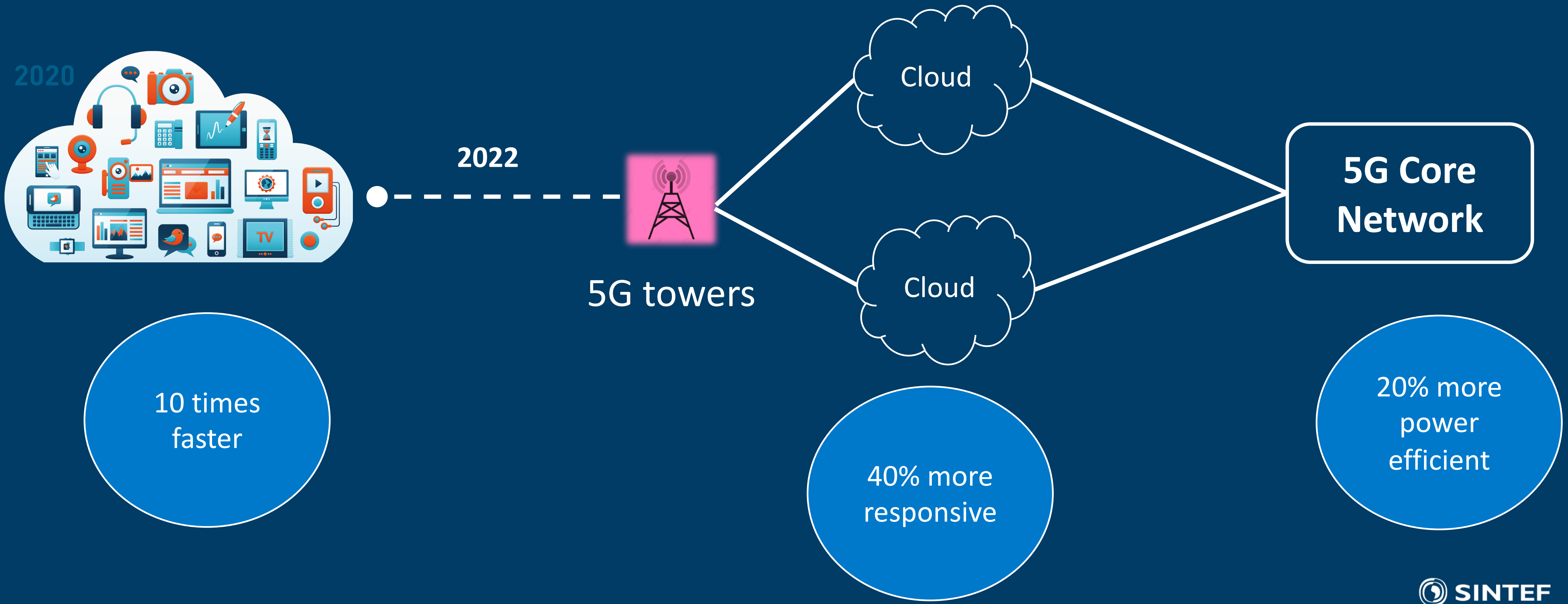
- Ultra-high bandwidth (~2 GB)
- Enhanced network capacity
- Ultra-low latency
- Reduced power consumption in the infrastructure
- Low battery for IoT devices



Source: Qualcomm

Vehicle to drive digitalization phase & realize a gigabit networked-society!

5G Cellular Networks



2020

2022

5G towers

Cloud

Cloud

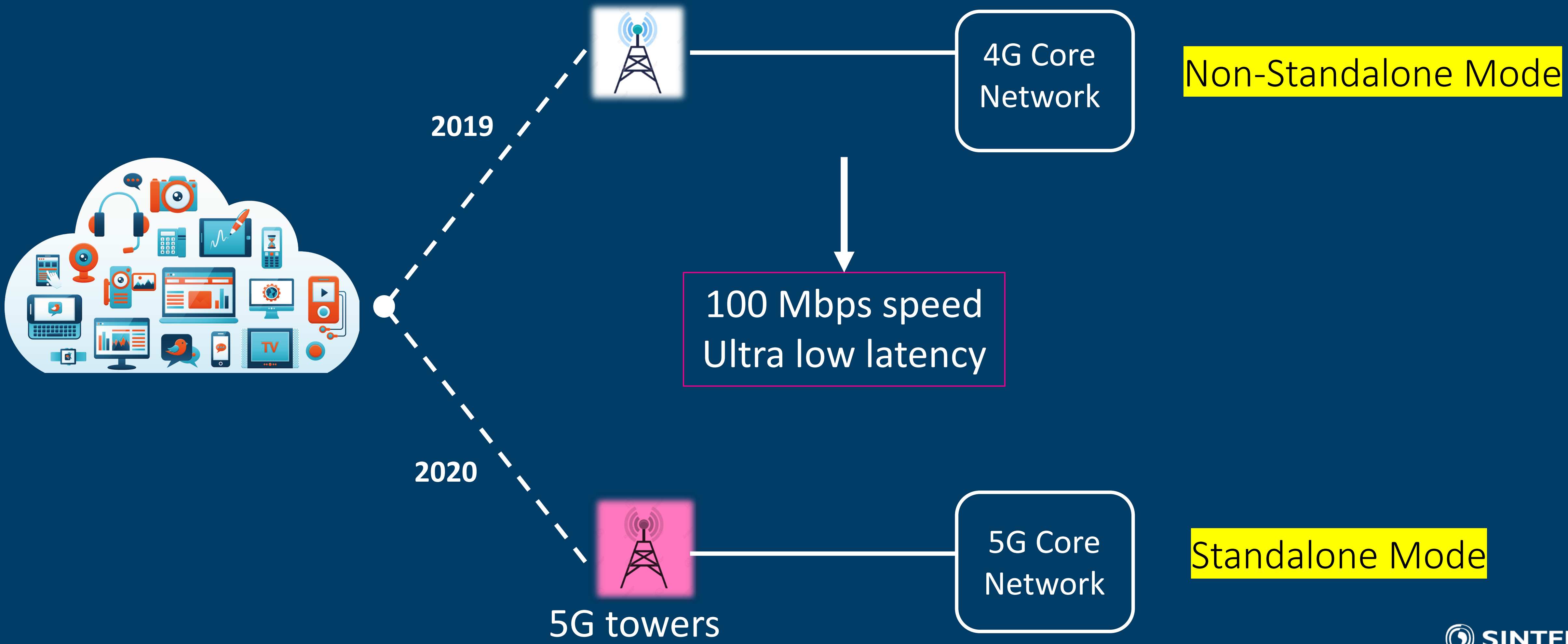
5G Core Network

10 times faster

40% more responsive

20% more power efficient

5G Deployments



2019

4G Core Network

Non-Standalone Mode

100 Mbps speed
Ultra low latency

2020

5G towers

5G Core Network

Standalone Mode

5G Networks

Vehicle to drive digitalization phase & realize a gigabit networked-society!

National critical infrastructure?

5G Future

Vehicle to drive digitalization phase & realize a gigabit networked-society!

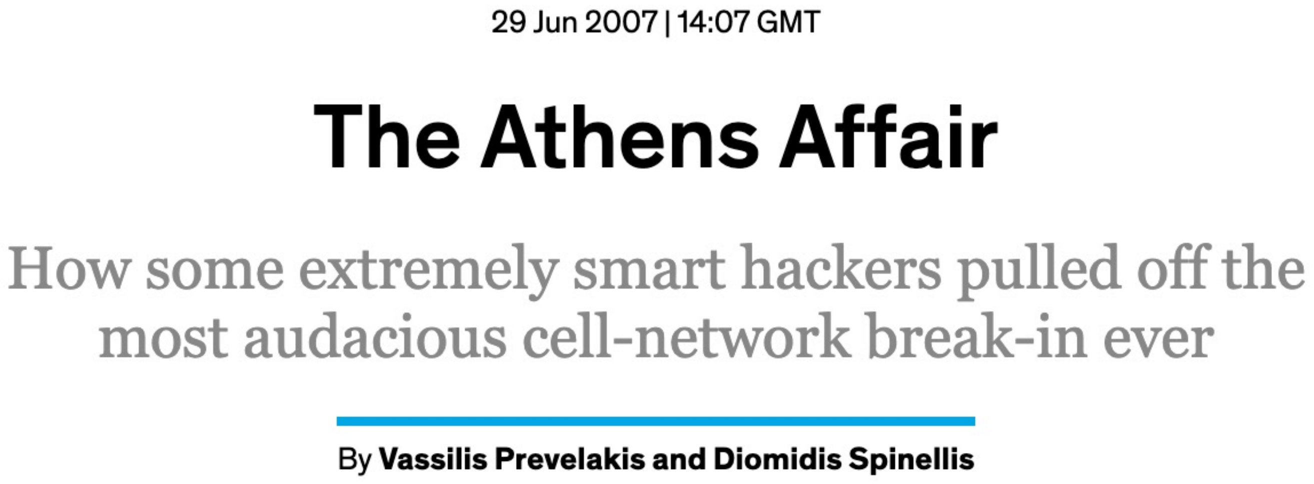
100 Mbps

5 Gbps

National Critical Infrastructure!

Image Sources: Internet

History of incidents – Greek Wiretapping Scandal

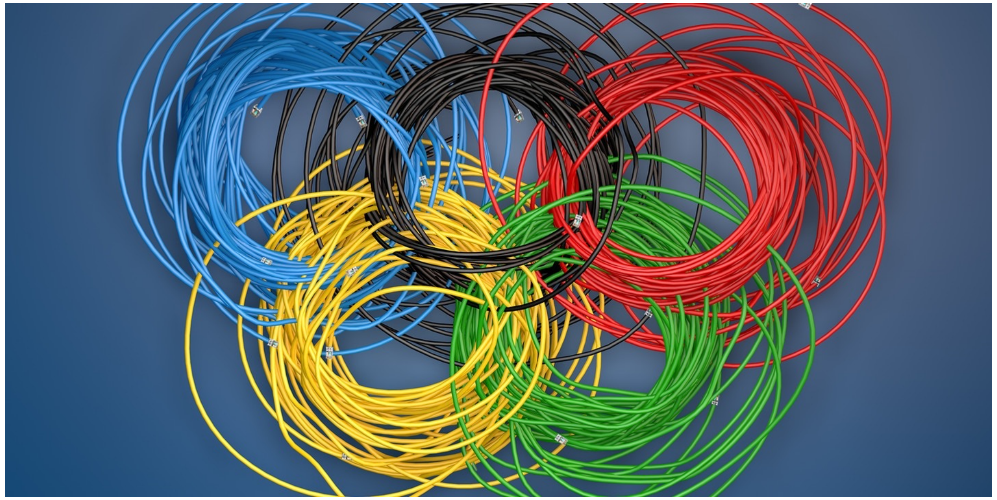


29 Jun 2007 | 14:07 GMT

The Athens Affair

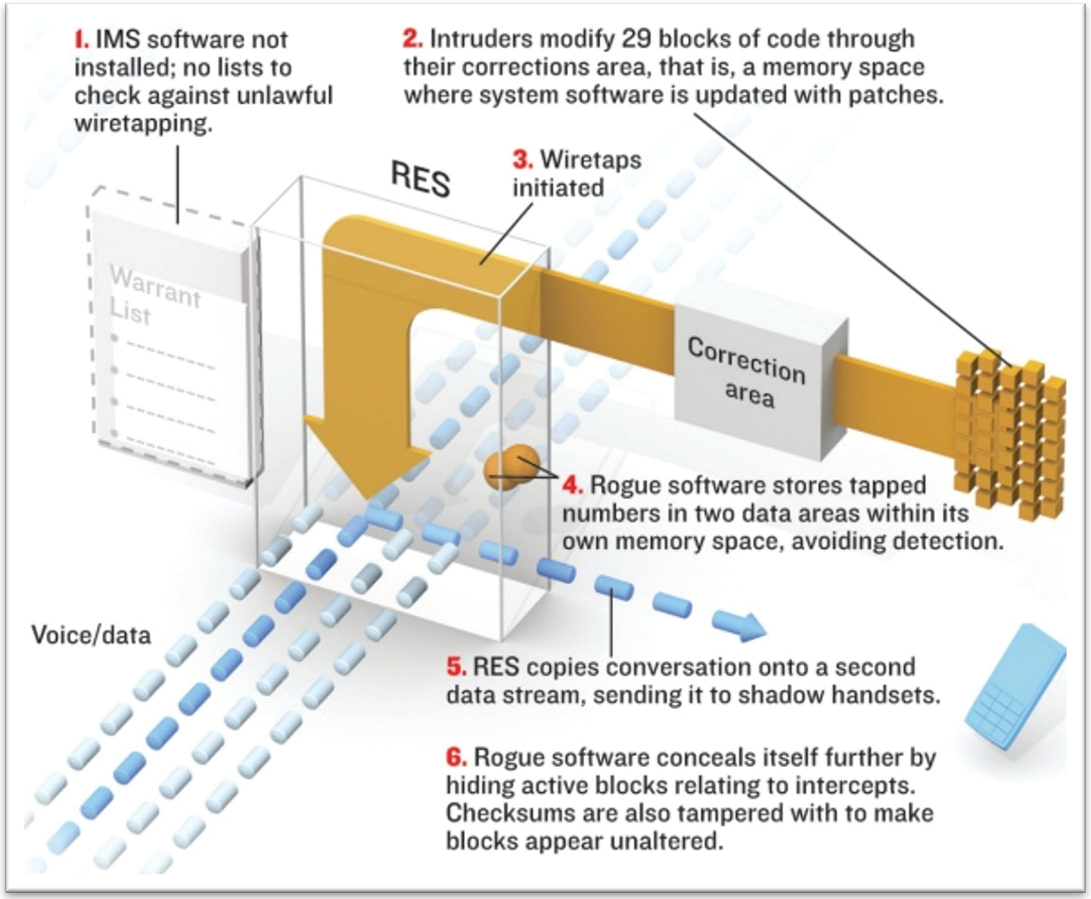
How some extremely smart hackers pulled off the most audacious cell-network break-in ever

By **Vassilis Prevelakis and Diomidis Spinellis**



Source: The Intercept

Greek Wiretapping Scandal



1. IMS software not installed; no lists to check against unlawful wiretapping.

2. Intruders modify 29 blocks of code through their corrections area, that is, a memory space where system software is updated with patches.

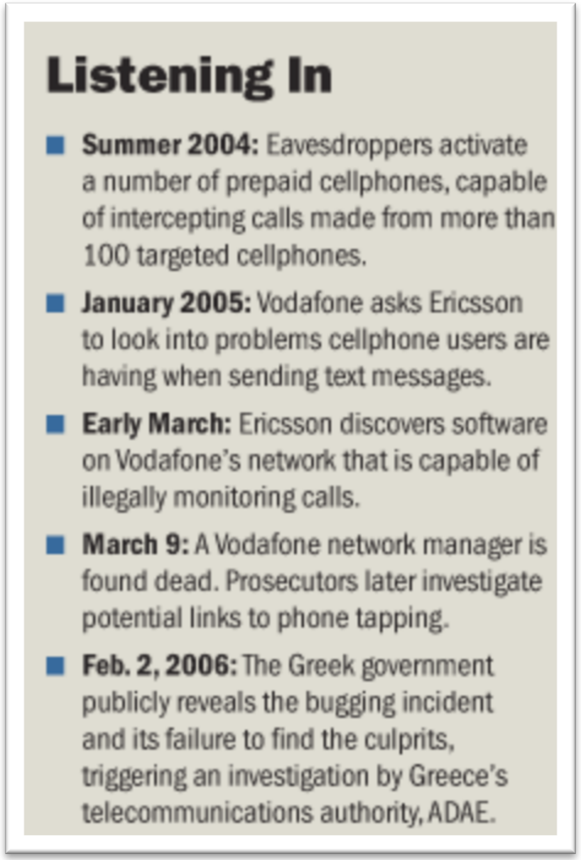
3. Wiretaps initiated

4. Rogue software stores tapped numbers in two data areas within its own memory space, avoiding detection.

5. RES copies conversation onto a second data stream, sending it to shadow handsets.

6. Rogue software conceals itself further by hiding active blocks relating to intercepts. Checksums are also tampered with to make blocks appear unaltered.

Source: IEEE



Listening In

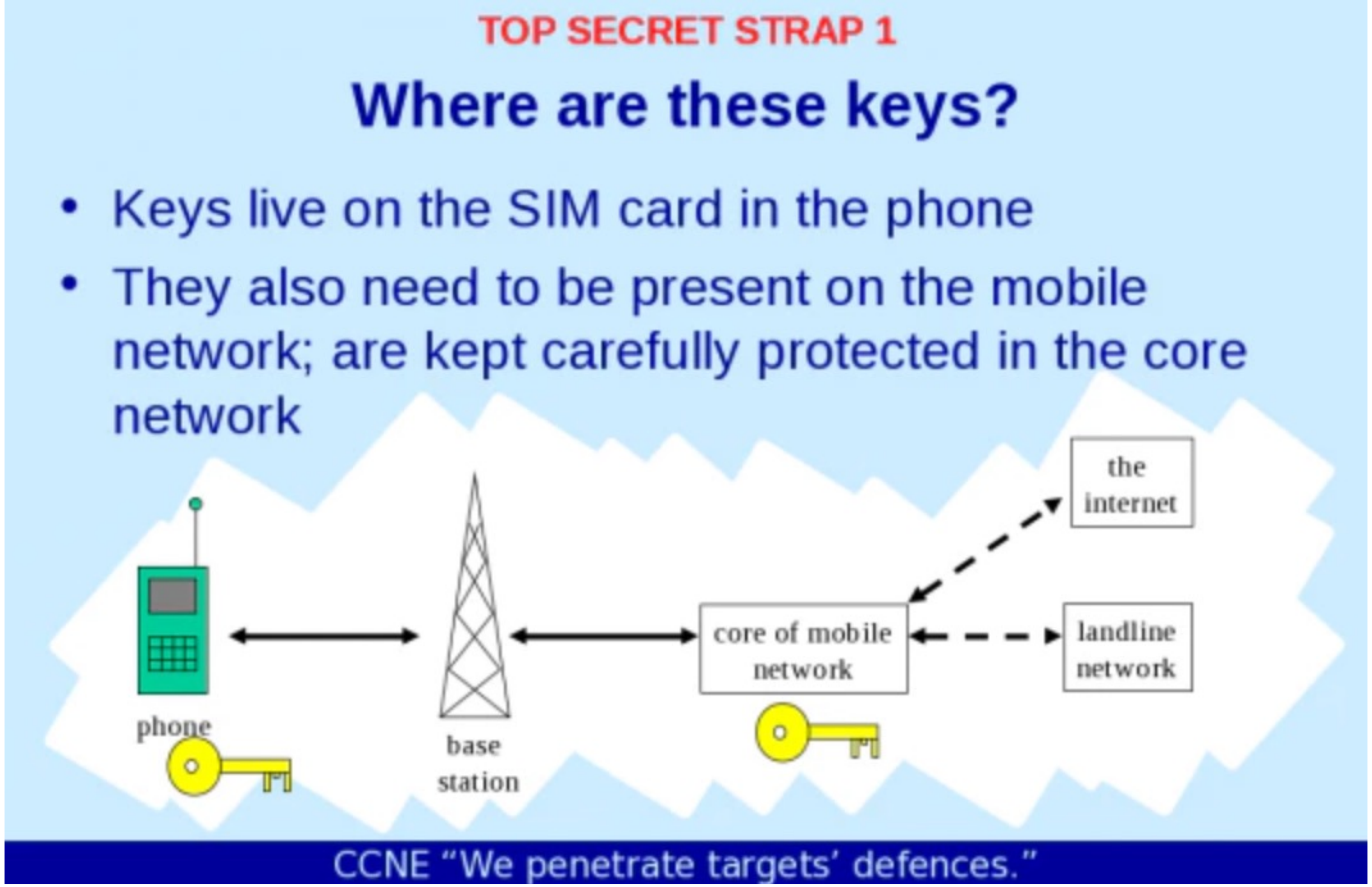
- **Summer 2004:** Eavesdroppers activate a number of prepaid cellphones, capable of intercepting calls made from more than 100 targeted cellphones.
- **January 2005:** Vodafone asks Ericsson to look into problems cellphone users are having when sending text messages.
- **Early March:** Ericsson discovers software on Vodafone's network that is capable of illegally monitoring calls.
- **March 9:** A Vodafone network manager is found dead. Prosecutors later investigate potential links to phone tapping.
- **Feb. 2, 2006:** The Greek government publicly reveals the bugging incident and its failure to find the culprits, triggering an investigation by Greece's telecommunications authority, ADAE.

Source: WSJ

History of incidents – SNOWDEN NSA Briefcase

Source: The HackerNews

SNOWDEN NSA Briefcase



TOP SECRET STRAP 1

Where are these keys?

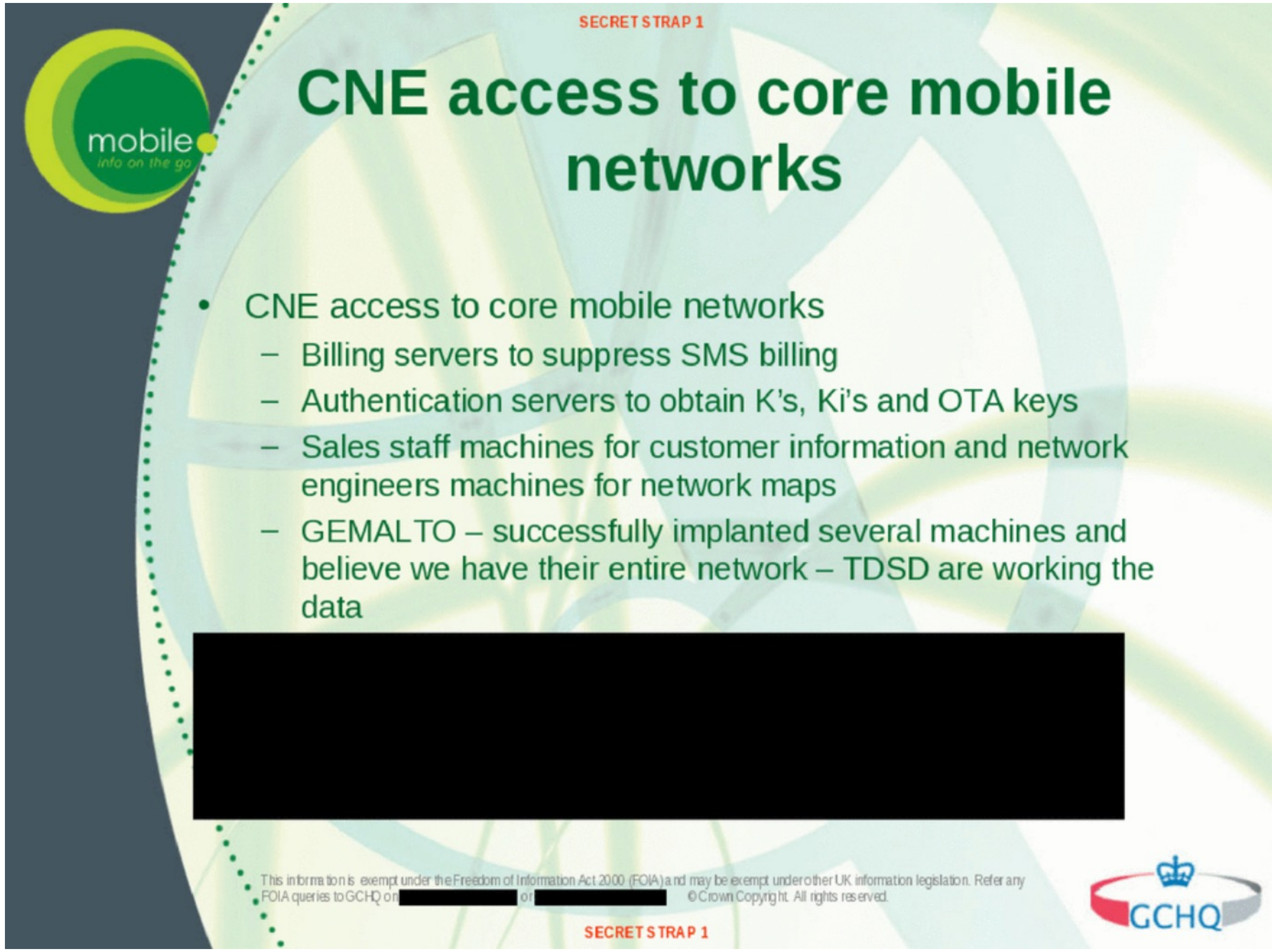
- Keys live on the SIM card in the phone
- They also need to be present on the mobile network; are kept carefully protected in the core network

phone
base station
core of mobile network
the internet
landline network

CCNE "We penetrate targets' defences."

Source: The Intercept

SNOWDEN NSA Briefcase



SECRET STRAP 1

CNE access to core mobile networks

- CNE access to core mobile networks
  - Billing servers to suppress SMS billing
  - Authentication servers to obtain K's, Ki's and OTA keys
  - Sales staff machines for customer information and network engineers machines for network maps
  - GEMALTO – successfully implanted several machines and believe we have their entire network – TDSD are working the data

[redacted]

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [redacted] or [redacted] ©Crown Copyright. All rights reserved.

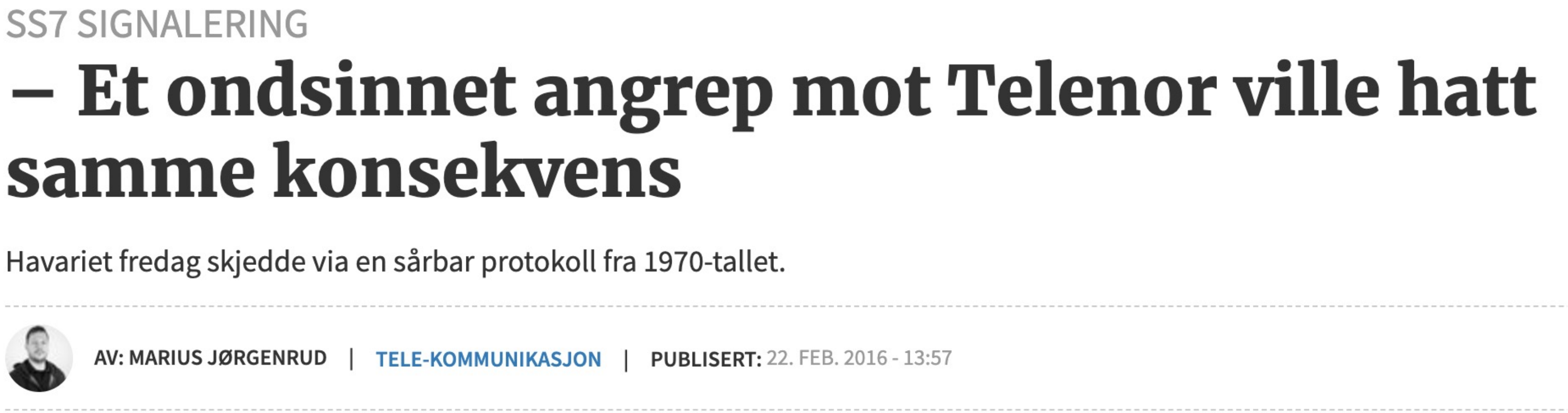
SECRET STRAP 1

Source: The Intercept

History of incidents – Design Vulnerabilities

- Weak encryption algorithms (2G)
- SS7 related issues (2G/3G/4G)
- Tracking and Interception (2G/3G/4G)
- …….
- ….

History of incidents – Configurational/Operational mistakes

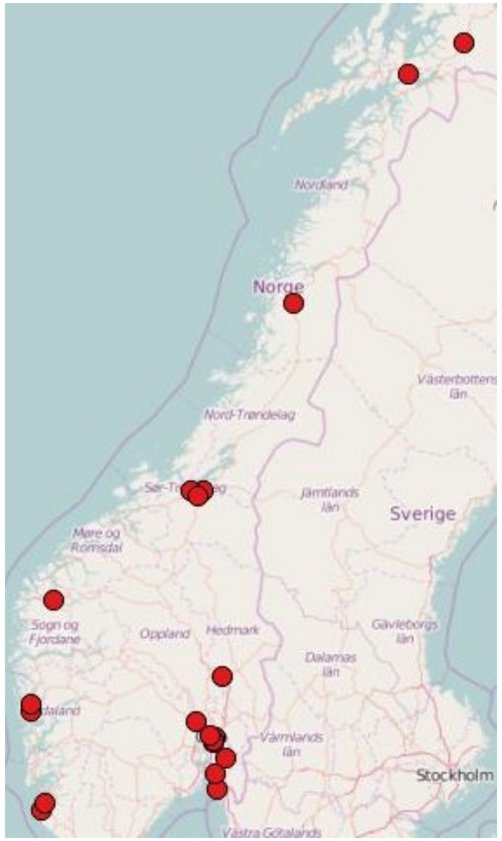


SS7 SIGNALERING

– Et ondsinnet angrep mot Telenor ville hatt samme konsekvens

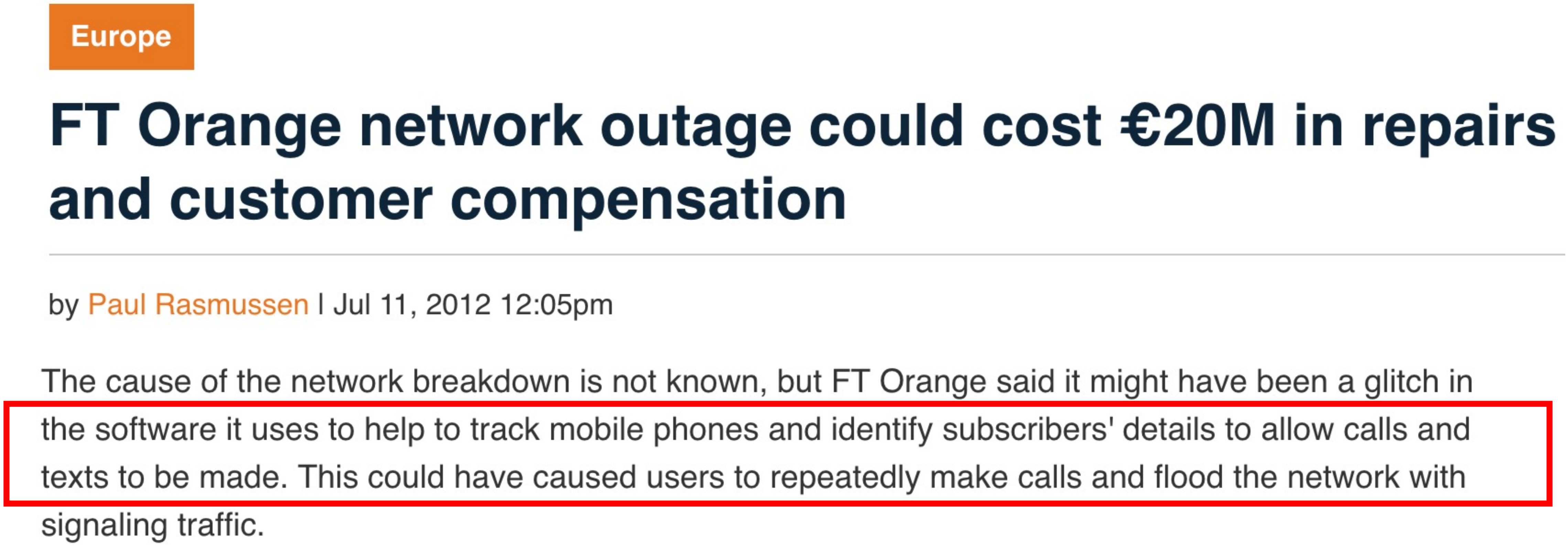
Havariet fredag skjedde via en sårbar protokoll fra 1970-tallet.

AV: MARIUS JØRGENRUD | TELE-KOMMUNIKASJON | PUBLISERT: 22. FEB. 2016 - 13:57



Source: nntb.no

Configurational/Operational mistakes



Europe

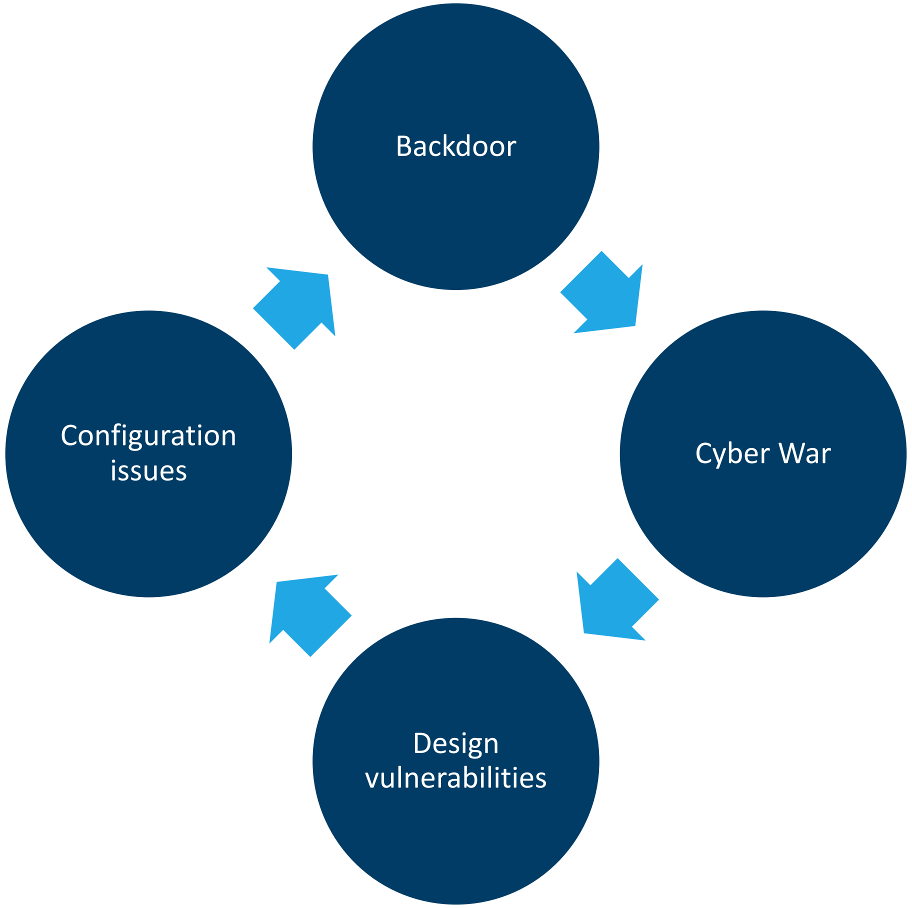
FT Orange network outage could cost €20M in repairs and customer compensation

by Paul Rasmussen | Jul 11, 2012 12:05pm

The cause of the network breakdown is not known, but FT Orange said it might have been a glitch in the software it uses to help to track mobile phones and identify subscribers' details to allow calls and texts to be made. This could have caused users to repeatedly make calls and flood the network with signaling traffic.

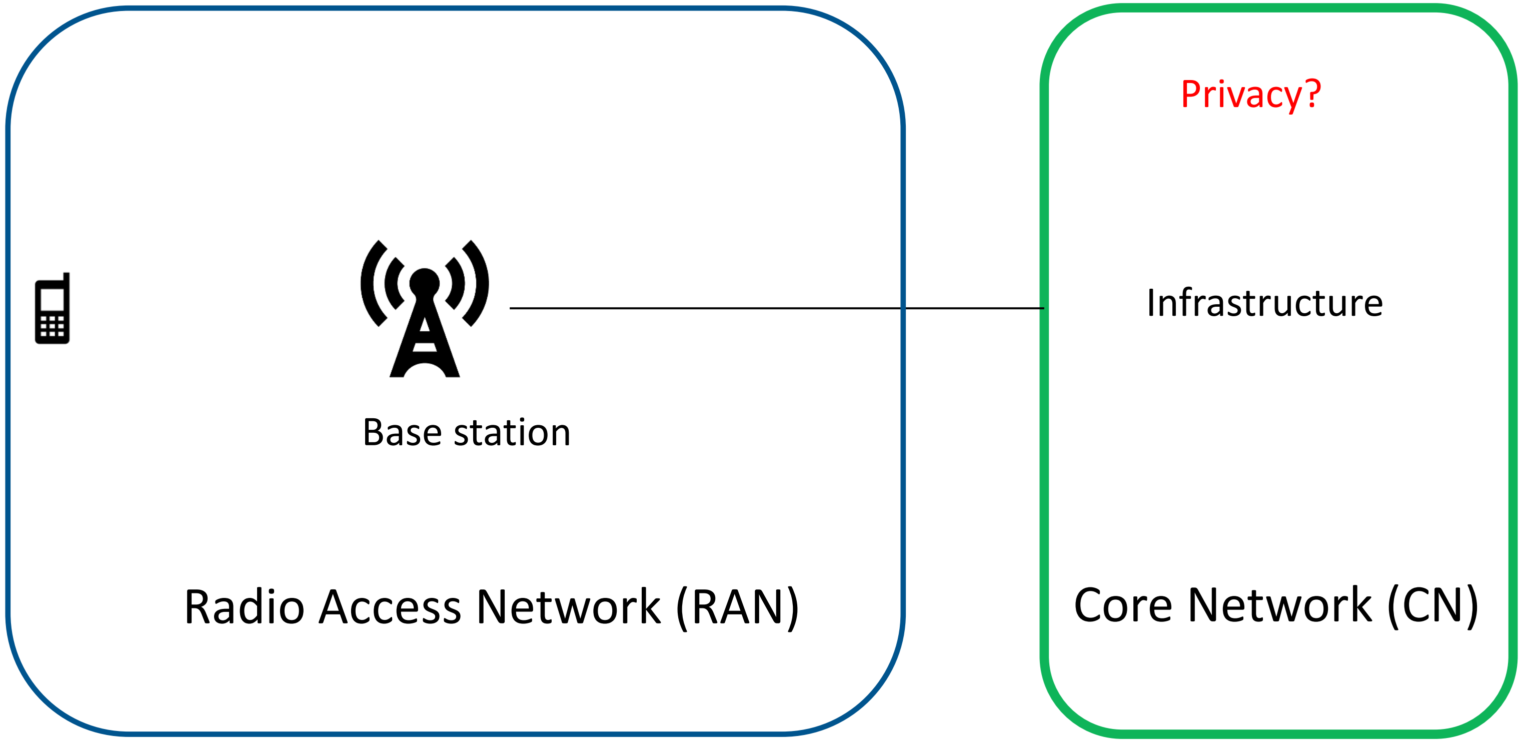
Summary of incidents

- Greek wiretapping -> backdoor
- NSA leaks -> Nation state cyber war
- SS7 issues -> design vulnerabilities
- Service outages -> configuration issues



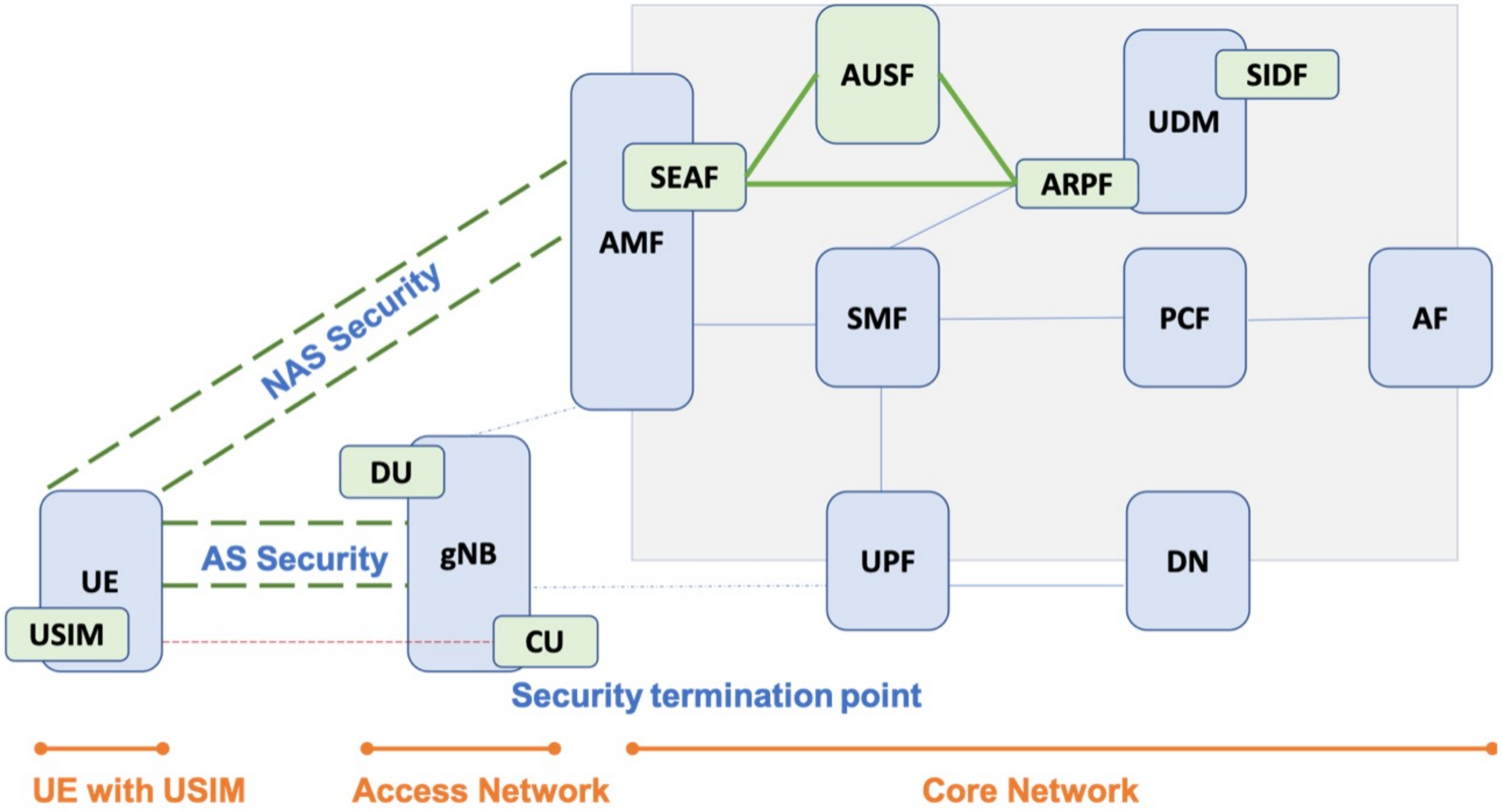
Let’s look into 5G Architecture & Security

Architecture in General



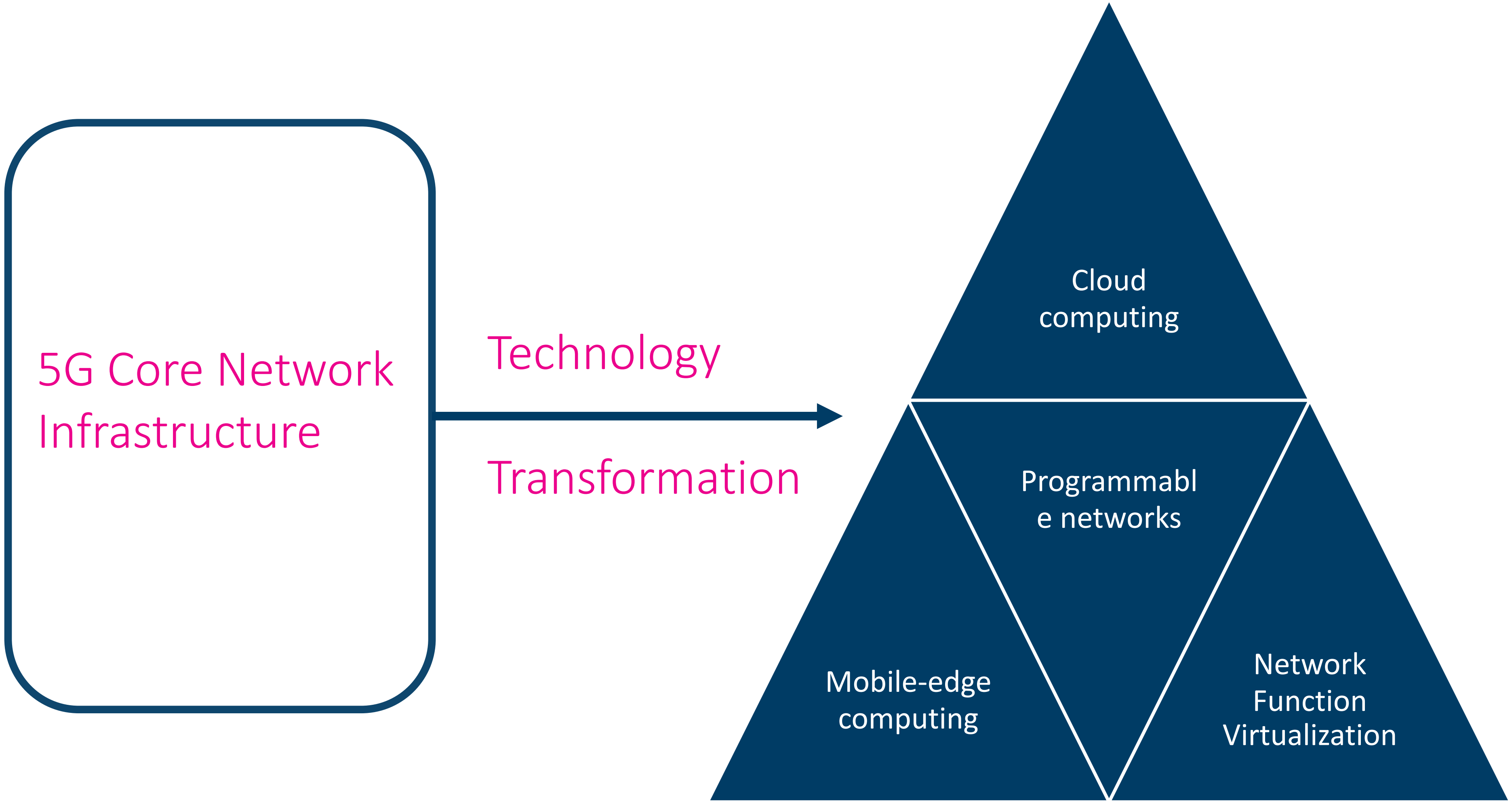
Note: picture provides an abstract view only

5G Architecture

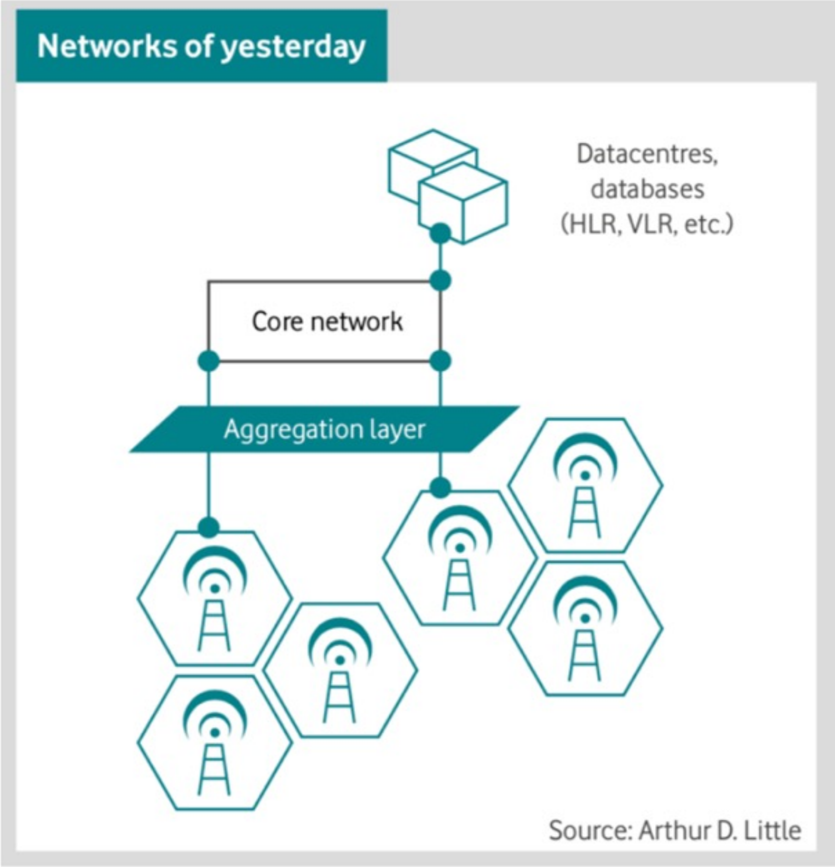


SINTEF

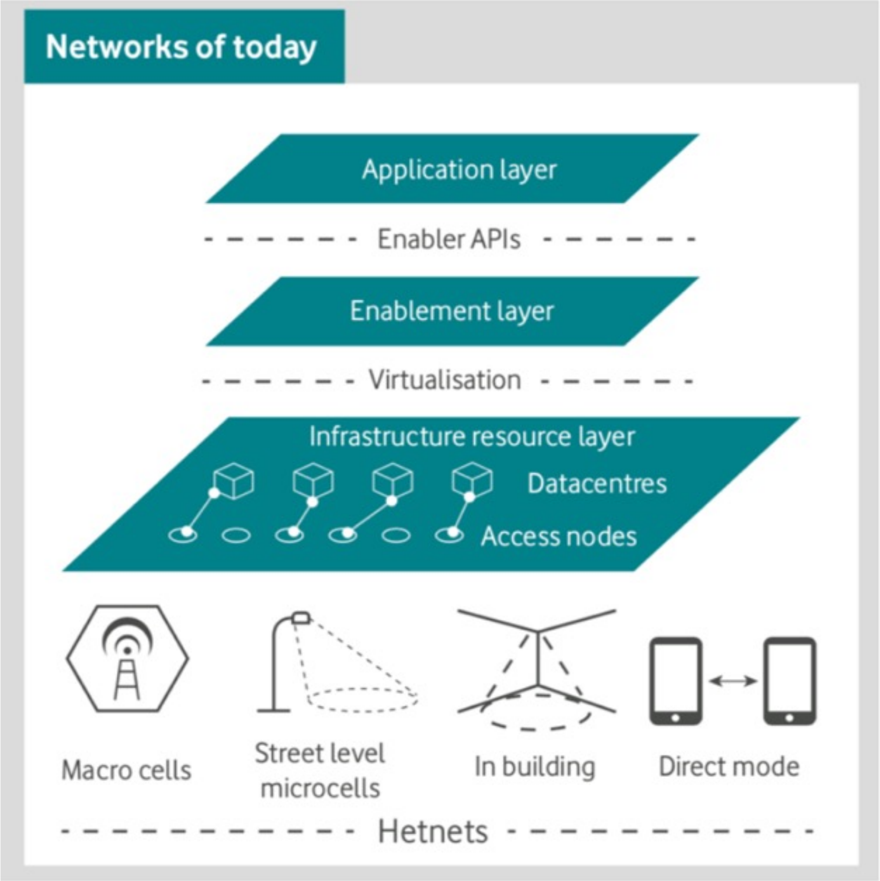
5G Architecture



Comparison with previous generations

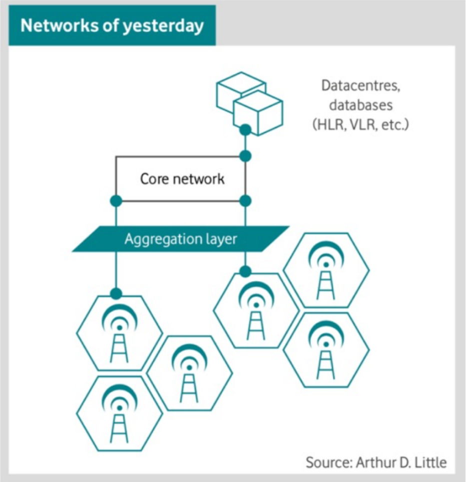


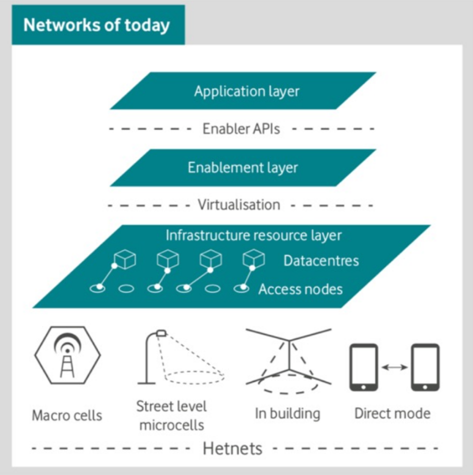
Source: Arthur D. Little



Comparison with previous generations

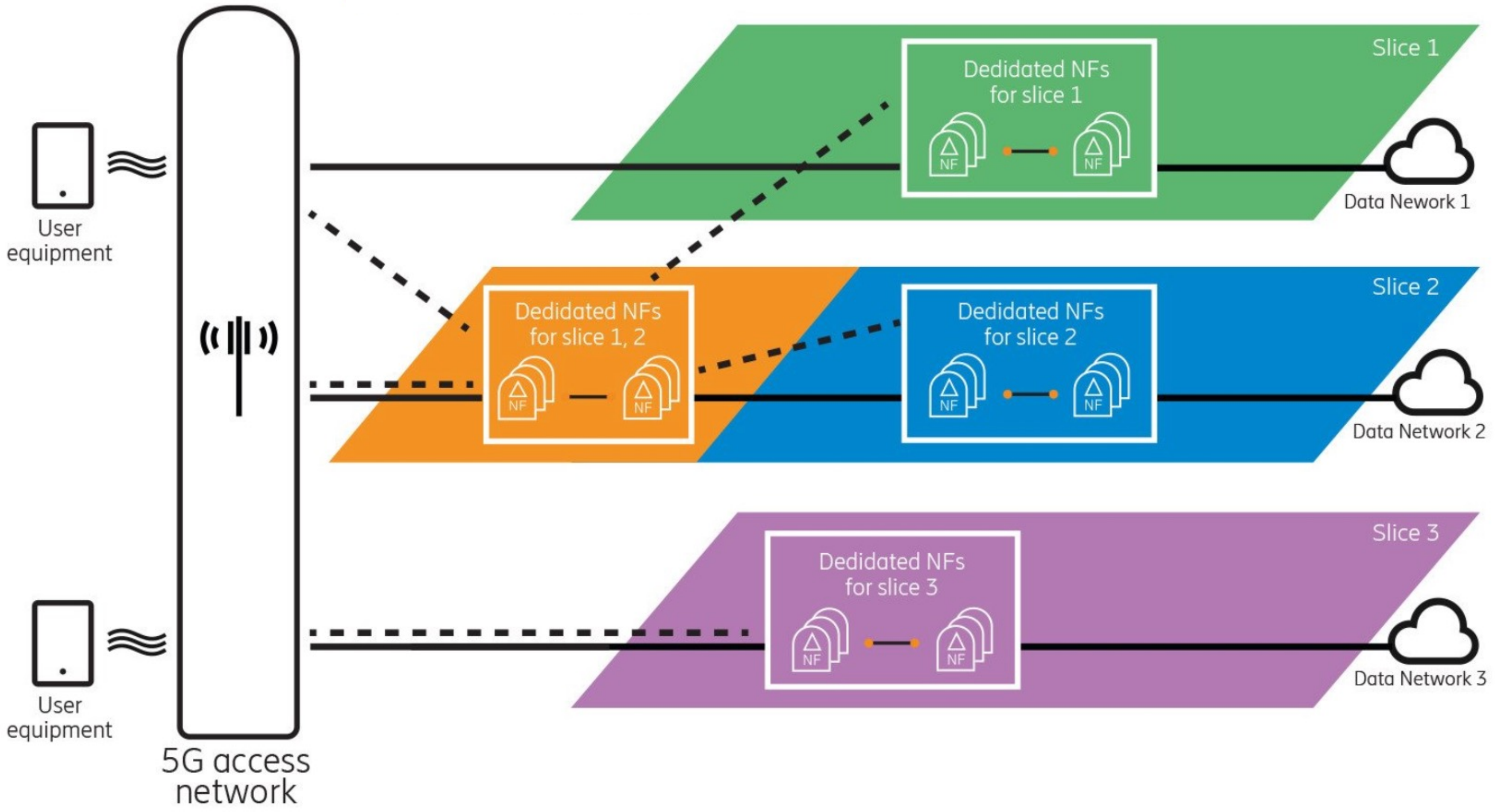
- Separated CN & RAN
- Dedicated IT hardware/software
- Propriety signalling protocols (Diameter/SS7)
- Difficult to modify for new services





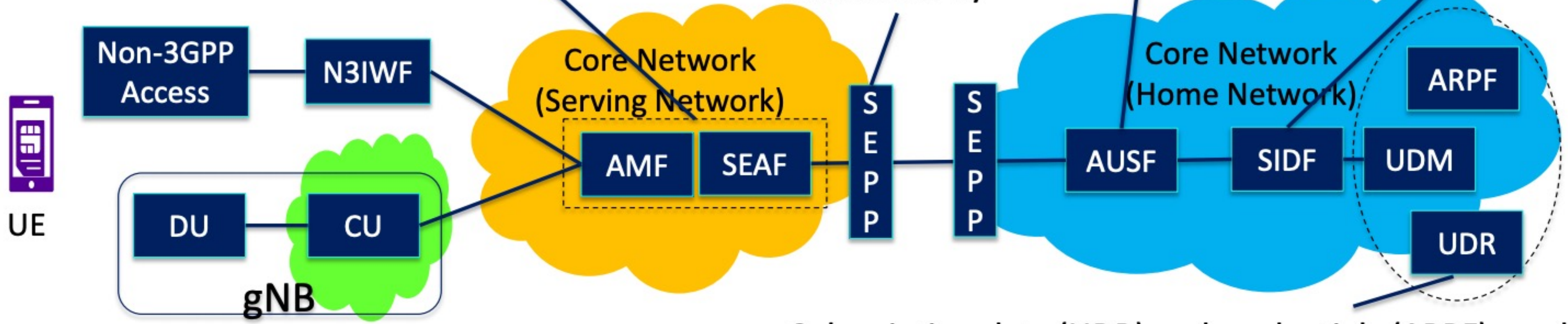
- Less separated CN & RAN
- Configurable Software/hardware
- Web based signalling protocols (HTTP, TLS, REST)
- APIs for creating new services

Illustration from the vendor



Source: Ericsson

Security Functions in 5G Architecture



Serving network root key is derived at SEAF
NAS security terminates in AMF

Interconnect traffic security

Verifies UE authentication & stores key for future re-use

Subscription identity de-concealment

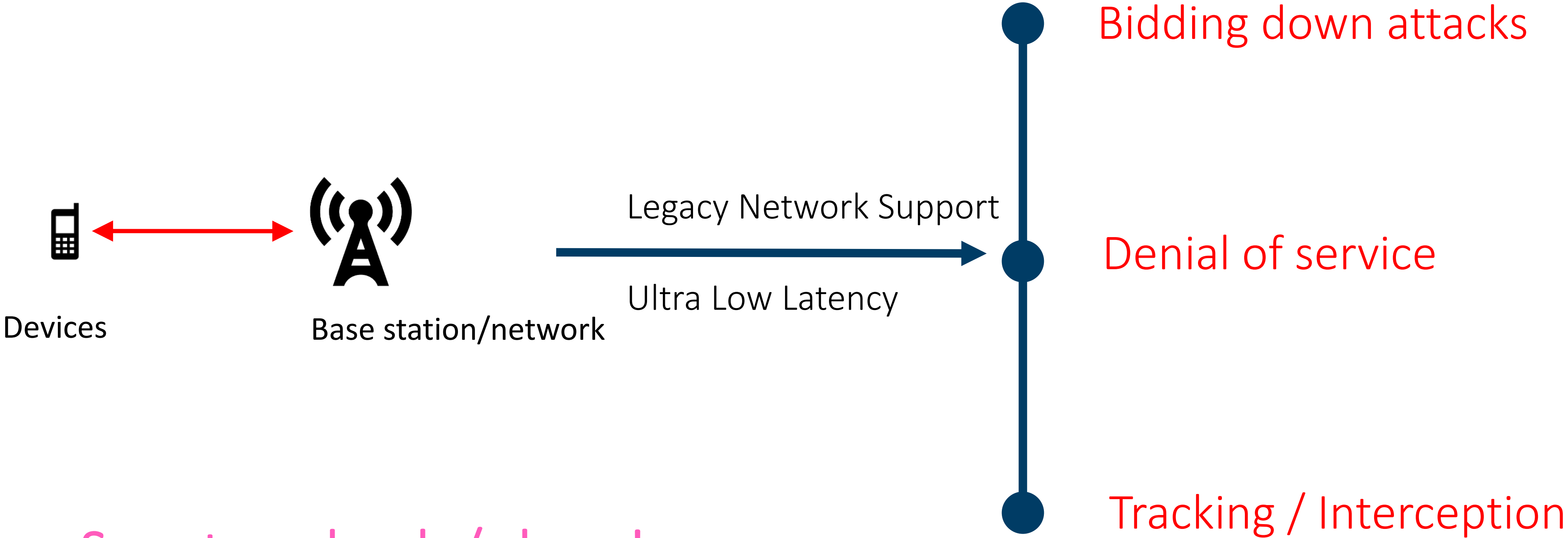
AS terminates at CU & N3IWF
No security function is performed at DU

Subscription data (UDR) and credentials (ARPF) used by UDM for authentication credential generation, user identification etc.

Source: Anand Prasad, RSA 2019

5G Security Issues

Increased Attack Surface



Devices

Base station/network

Legacy Network Support

Ultra Low Latency

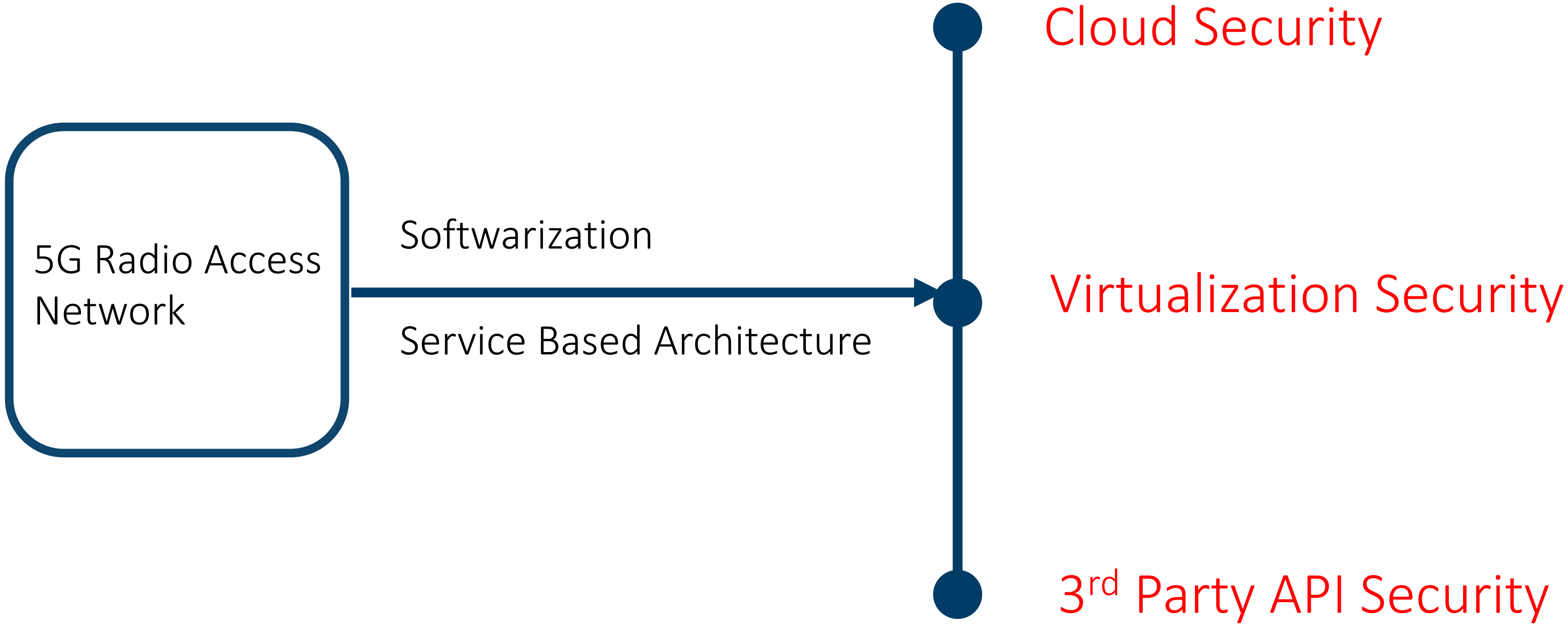
Bidding down attacks

Denial of service

Tracking / Interception

Smart == dumb / slave !

Increased Attack Surface



5G Radio Access Network

Softwarization

Service Based Architecture

Cloud Security

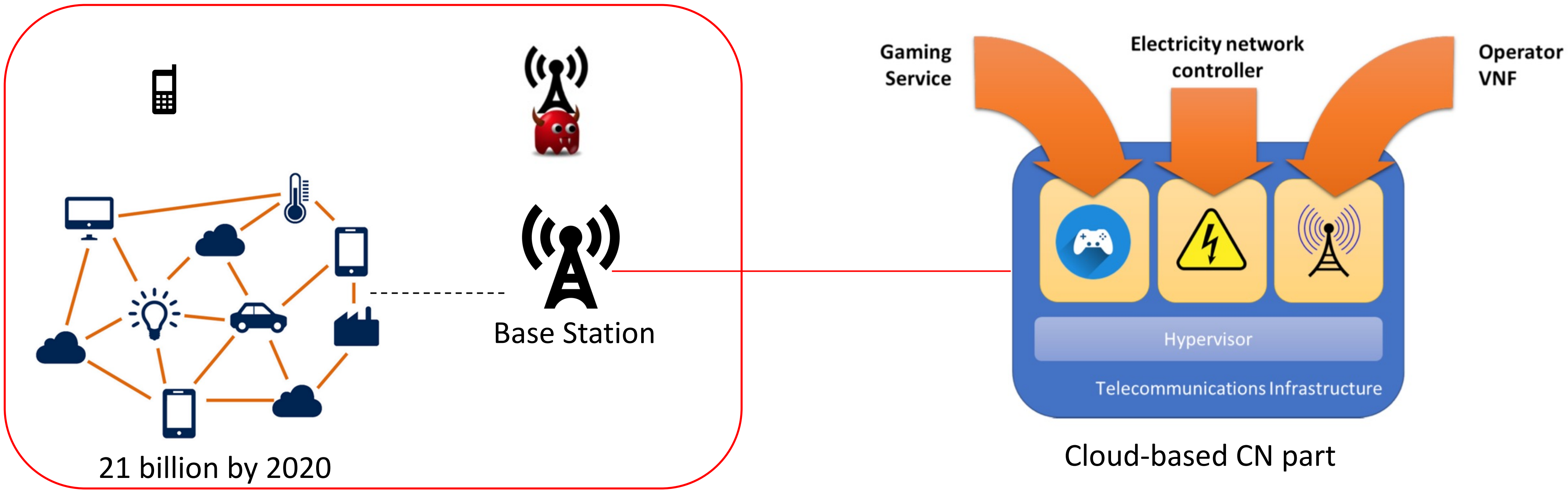
Virtualization Security

3rd Party API Security

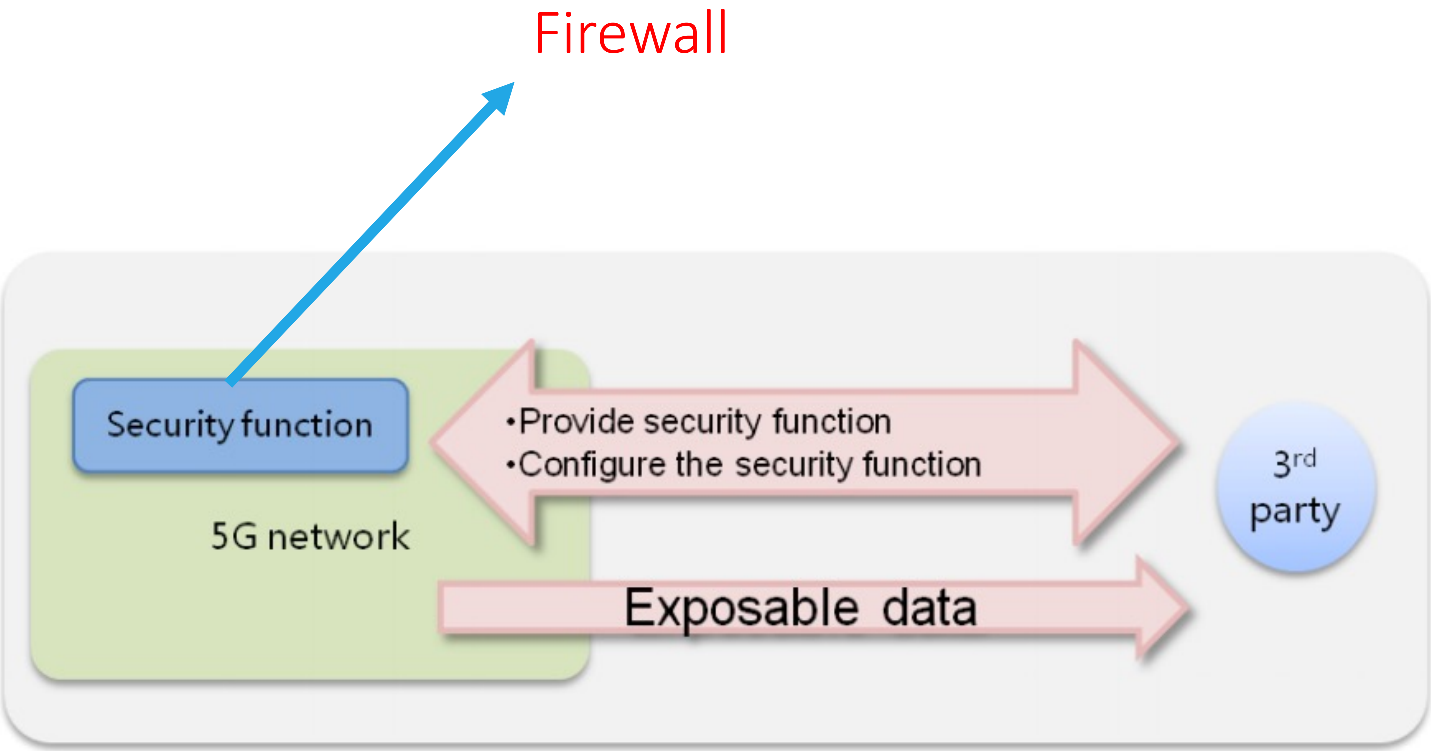
Source: Logolynx

Increased Attack Surface

1. Attack at any component may affect the whole network



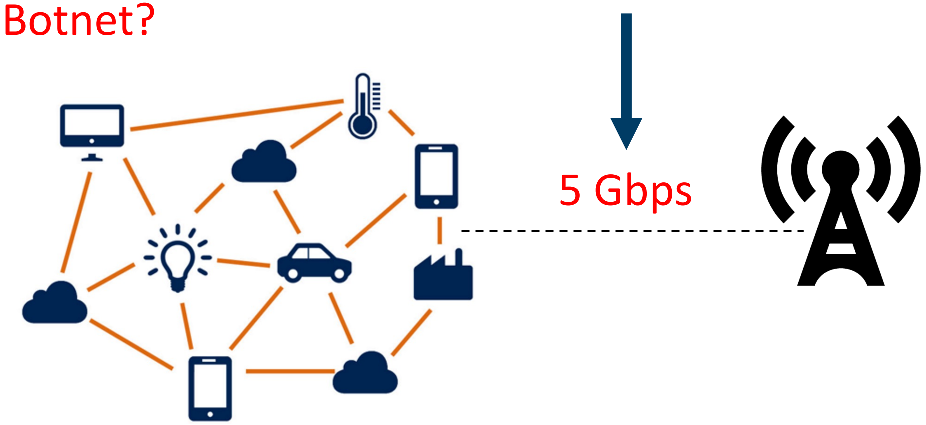
Attack Example



Source: NGMN

Security challenges..

2. Denial of Service / Distributed Denial of Service attack protection



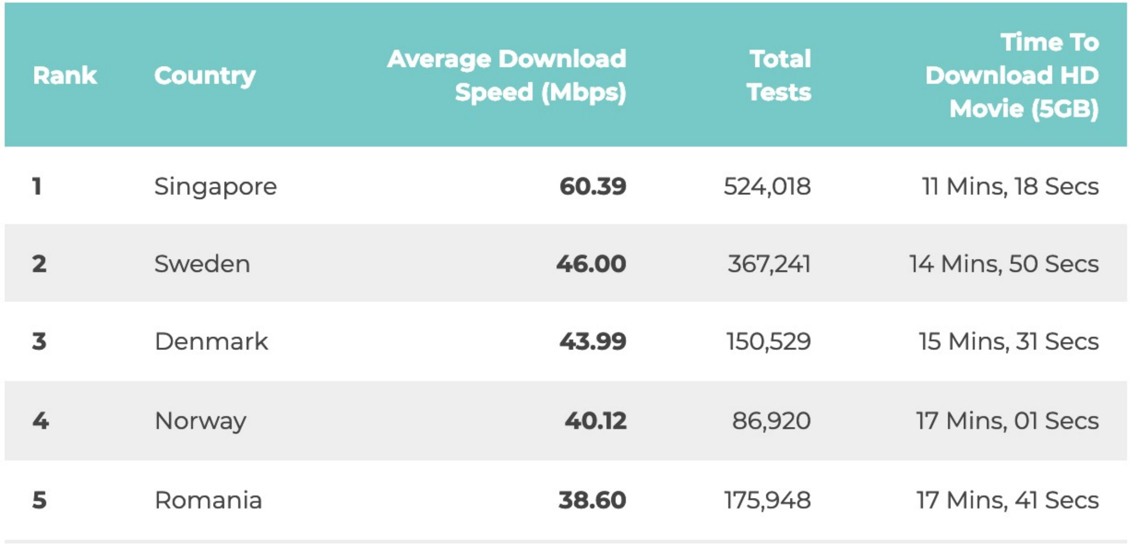
Botnet?

Bandwidth per device

5 Gbps

21 billion by 2020

Average wired broadband speed



Rank	Country	Average Download Speed (Mbps)	Total Tests	Time To Download HD Movie (5GB)
1	Singapore	**60.39**	524,018	11 Mins, 18 Secs
2	Sweden	**46.00**	367,241	14 Mins, 50 Secs
3	Denmark	**43.99**	150,529	15 Mins, 31 Secs
4	Norway	**40.12**	86,920	17 Mins, 01 Secs
5	Romania	**38.60**	175,948	17 Mins, 41 Secs

Source: Fastmetrics

Security challenges..

3. Data privacy issues (vulnerabilities in the 5G standards)

New vulnerabilities in 4G and 5G cellular access network protocols : exposing device capabilities

Altaf Shaik (Technische Universität Berlin, Germany); Ravishankar Borgaonkar (SINTEF Digital, Norway); Shinjo Park and Jean-Pierre Seifert

New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols

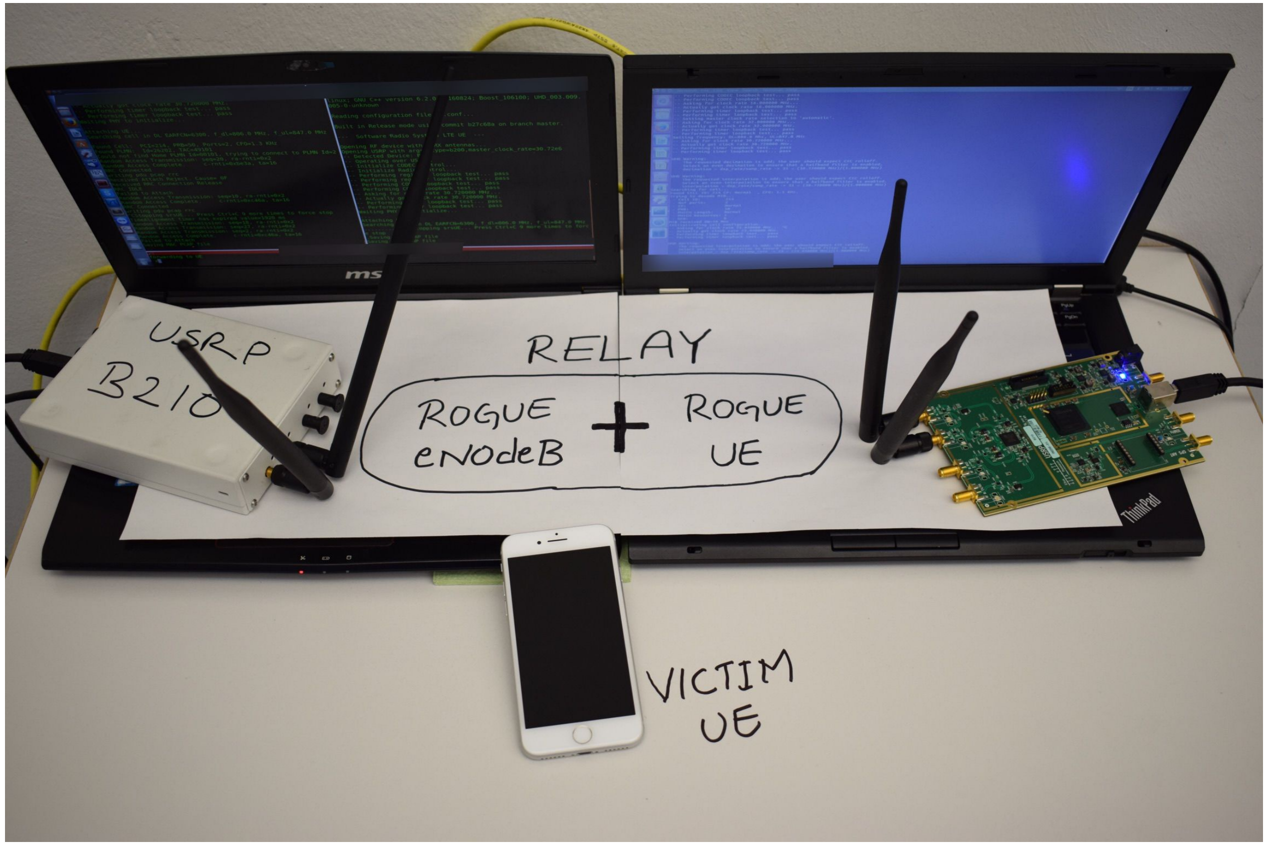
Ravishankar Borgaonkar and Lucca Hirschi and Shinjo Park and Altaf Shaik

A Formal Analysis of 5G Authentication

Component-Based Formal Analysis of 5G-AKA: Channel Assumptions and Session Confusion

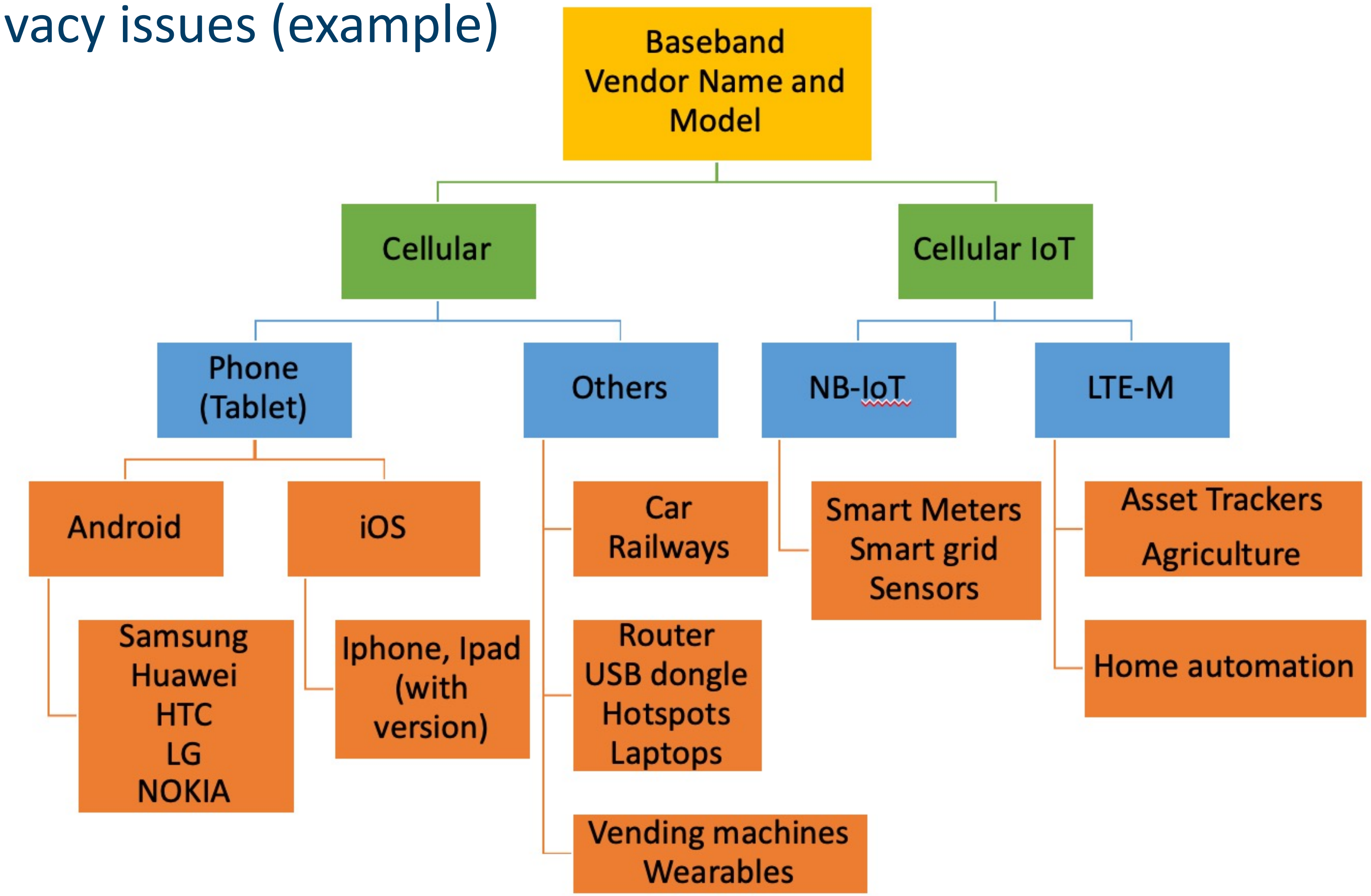
Security challenges..

3. Data privacy issues (practical attack example)



Security challenges..

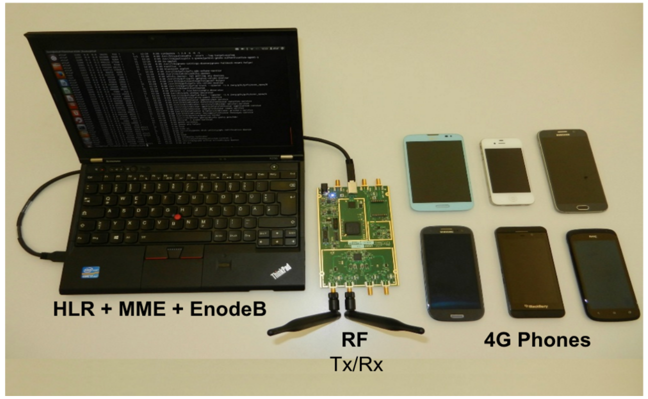
3. Data privacy issues (example)


Baseband Vendor Name and Model
Cellular
Cellular IoT
Phone (Tablet)
Others
NB-IoT
LTE-M
Android
iOS
Car Railways
Smart Meters Smart grid Sensors
Asset Trackers Agriculture
Samsung Huawei HTC LG NOKIA
Iphone, Ipad (with version)
Router USB dongle Hotspots Laptops
Home automation
Vending machines Wearables

Security challenges..

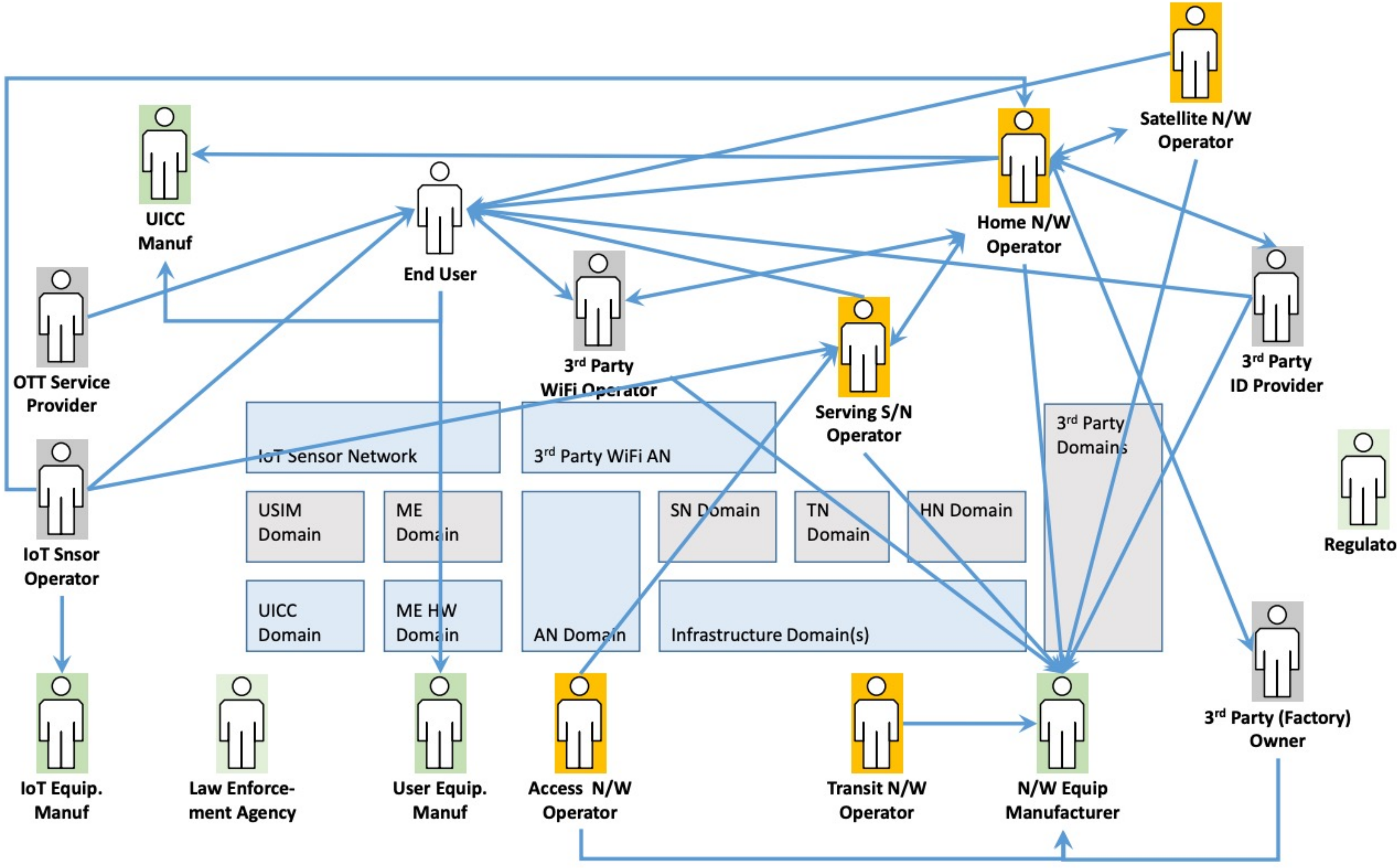
3. IoT / IIoT threats

- Trade-off between low latency and security
- **Availability of low cost attacking tools**
- Standard will be defined this year in phase 2
- Best practices for configuration and deployments?
- Private 5G network based solution?



Security challenges..

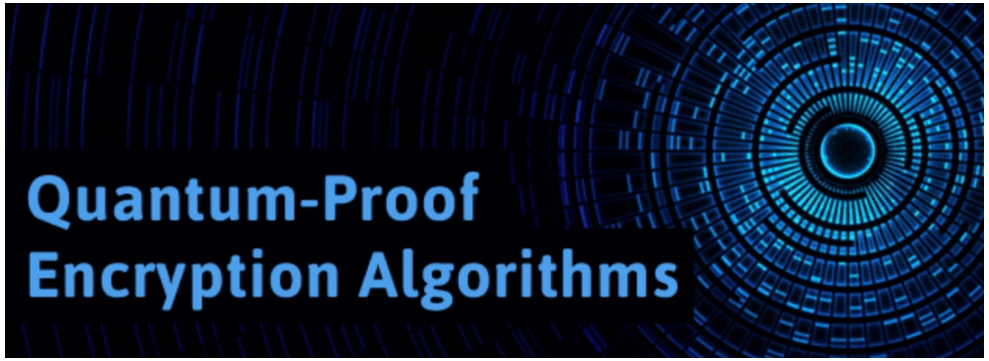
5. Risk analysis & trust modelling approaches

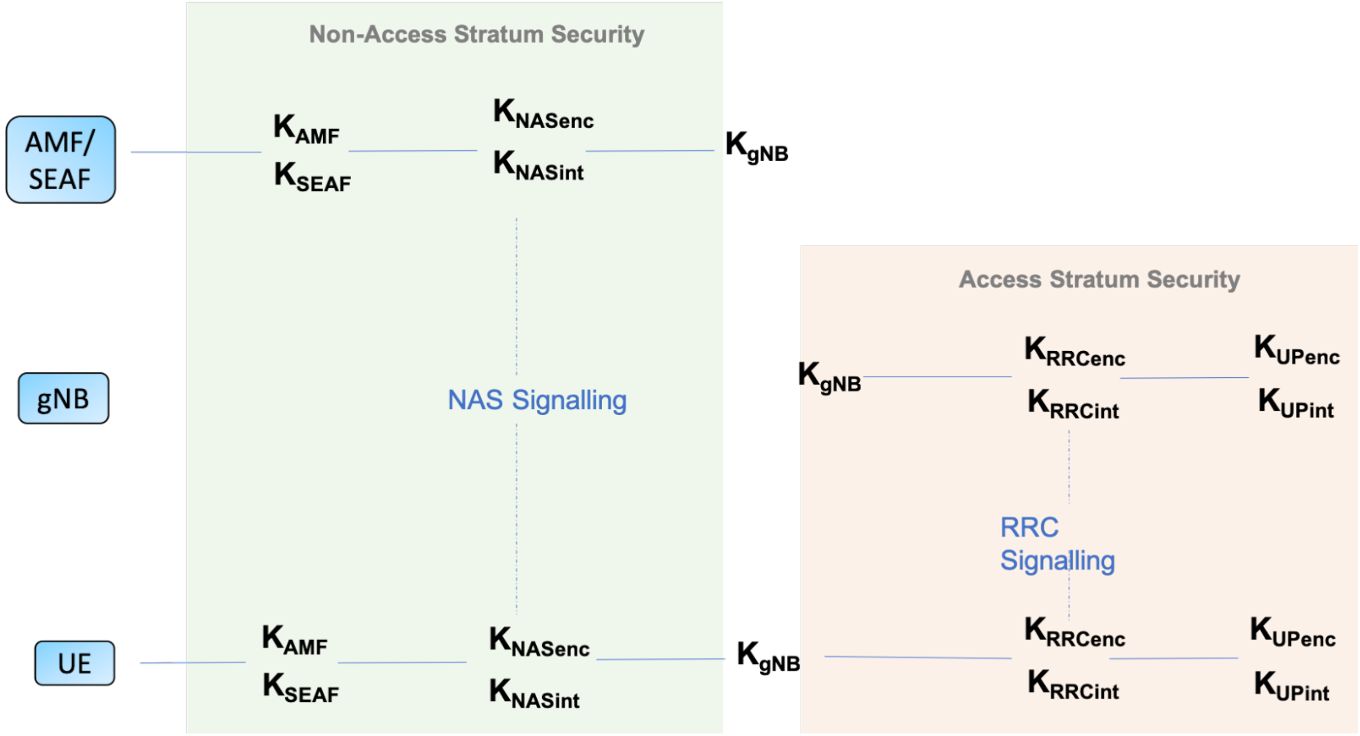


Source: 5G-ENSURE

Security challenges..

6. Cellular encryption algorithms and techniques





Security challenges..

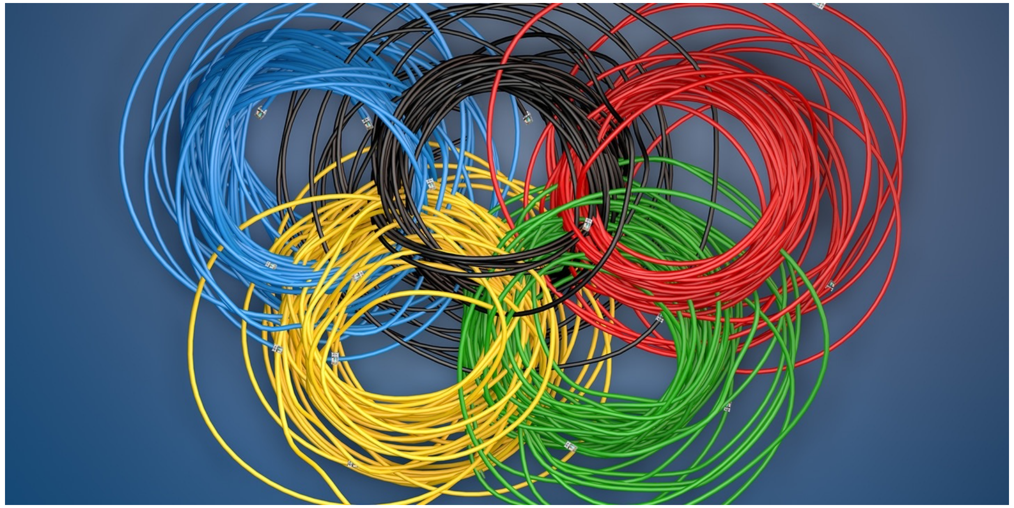
7. Control of infrastructure in the age of cyber-war

“ it is rational to demand high security assurance from 5G technology used for mission-critical communication and, to the farthest degree possible, to eliminate the risk of control over network resources by foreign services. ”

CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

Security challenges..

8. 5G as an emerging signal intelligence platform for collecting and processing telemetry data → surveillance from cyber enemies



CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

Summary and Looking forward

- 5G path towards digital & gigabit society
- Stronger security than 4G but

  new features ==increase in attack surface

  support to the legacy systems == attack inheritance?
- Need of risk assessment and management tools
- **Best security practices while using 5G**
- New security solutions tailored towards protecting the infrastructure telemetry data

SINTEF

Teknologi for et bedre samfunn

Contact at -   ravishankar.Borgaonkar@sinetf.no