


A1

Mobile Security

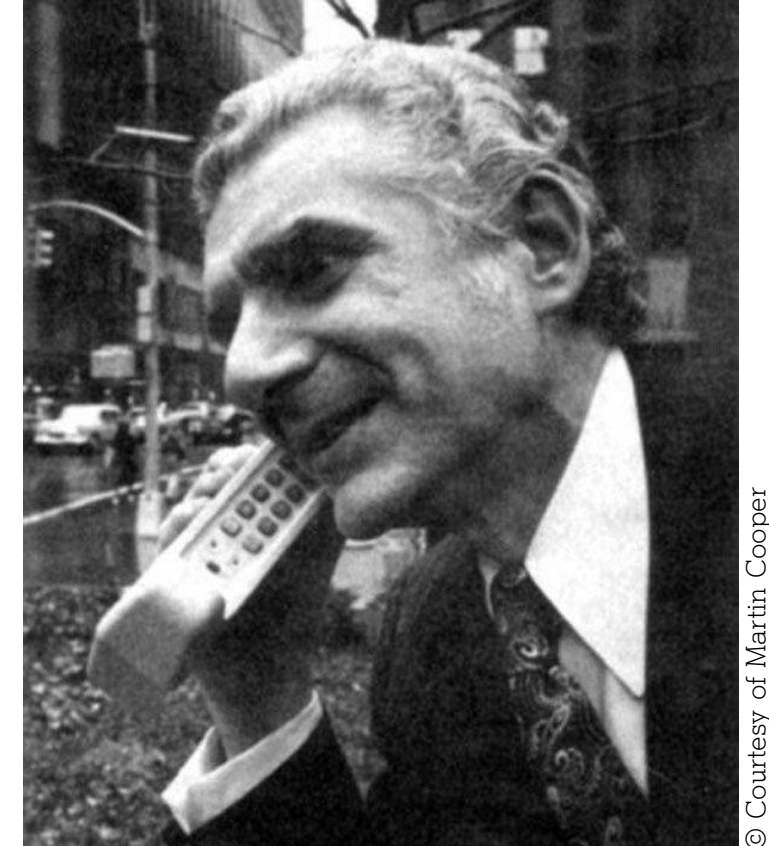
A1 | Georg Löffelmann

29 May 2026

Quotes on Mobile and Security

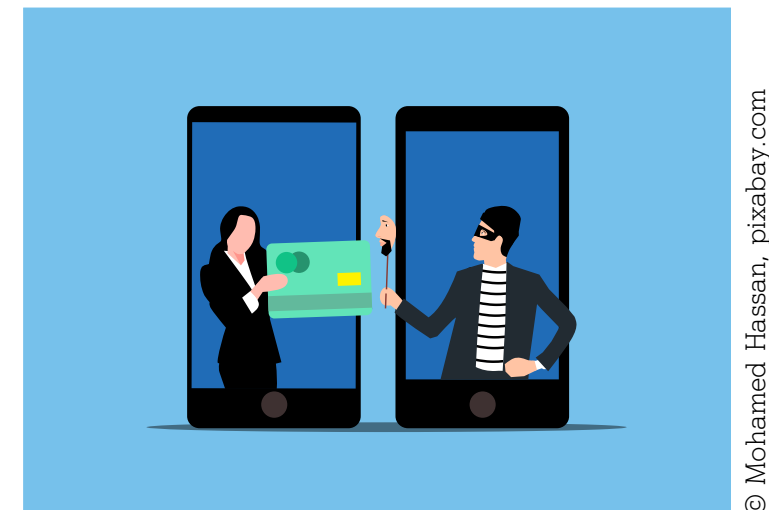
"The biggest innovation of all is social networking, and **cellular technology is the facilitator for social networking.** People are mobile; social networking is people, and the only way people connect with each other is wirelessly." 

Martin Cooper
(Inventor of the first handheld mobile phone)



© Courtesy of Martin Cooper

"Amateurs hack **systems**, professionals hack **people**."



© Mohamed Hassan, pixabay.com

Look Who's Talking

9125569  TECHNISCHE
UNIVERSITÄT
WIEN

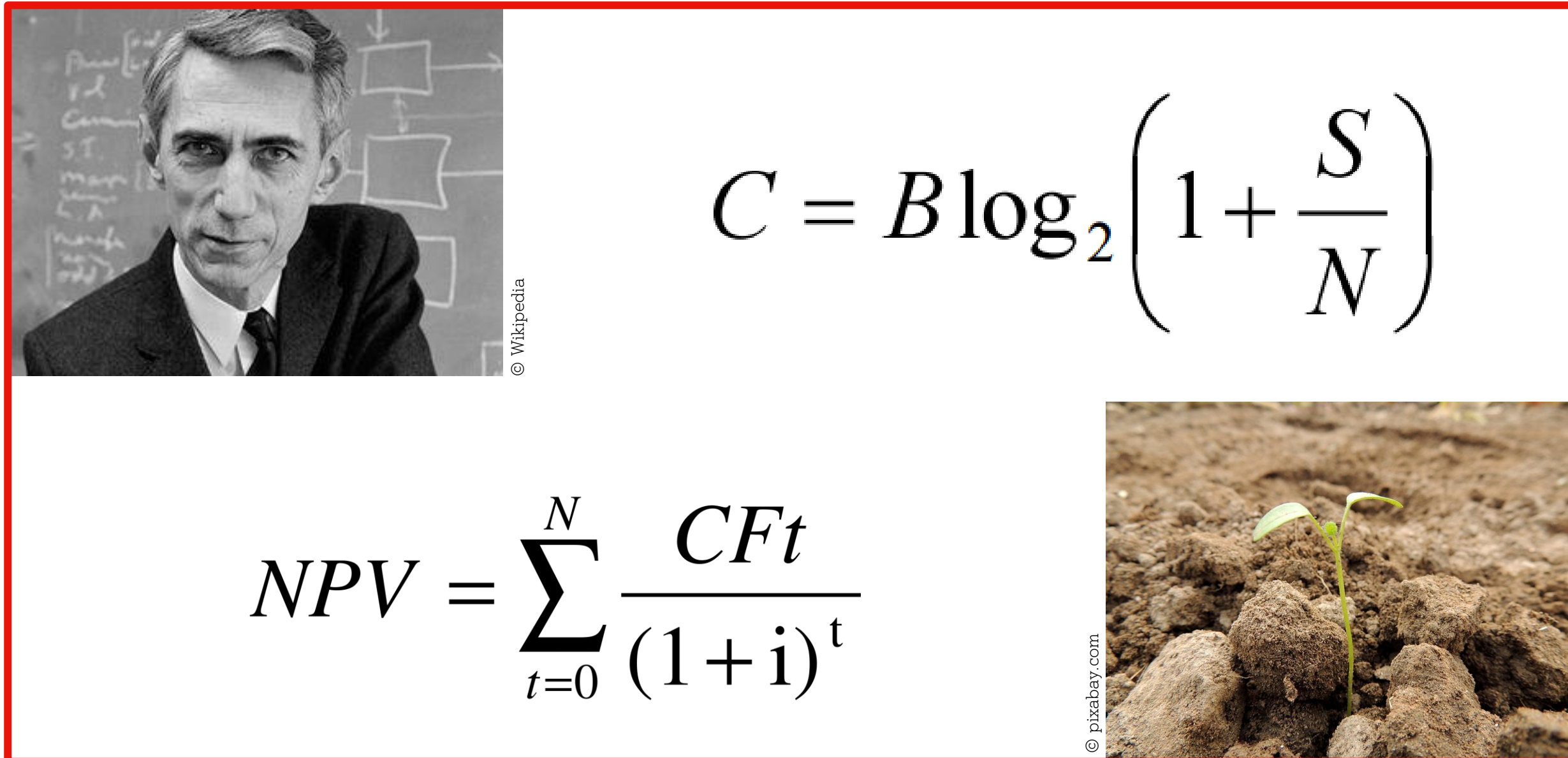
Dipl.-Ing. Georg Löffelmann, Head of Department Mobile, A1 Telekom Austria AG

Siemens Munich	GHz
ABB, Thomcast CSF Baden	kHz
Kapsch	MHz
ÖBH	MHz
A1	MHz → GHz

 <https://www.linkedin.com/in/georgloeffelmann/>



What I do: Mr. Shannon meets Net Present Value



$C = B \log_2 \left(1 + \frac{S}{N} \right)$

$NPV = \sum_{t=0}^N \frac{CF_t}{(1+i)^t}$

© Wikipedia

© pixabay.com

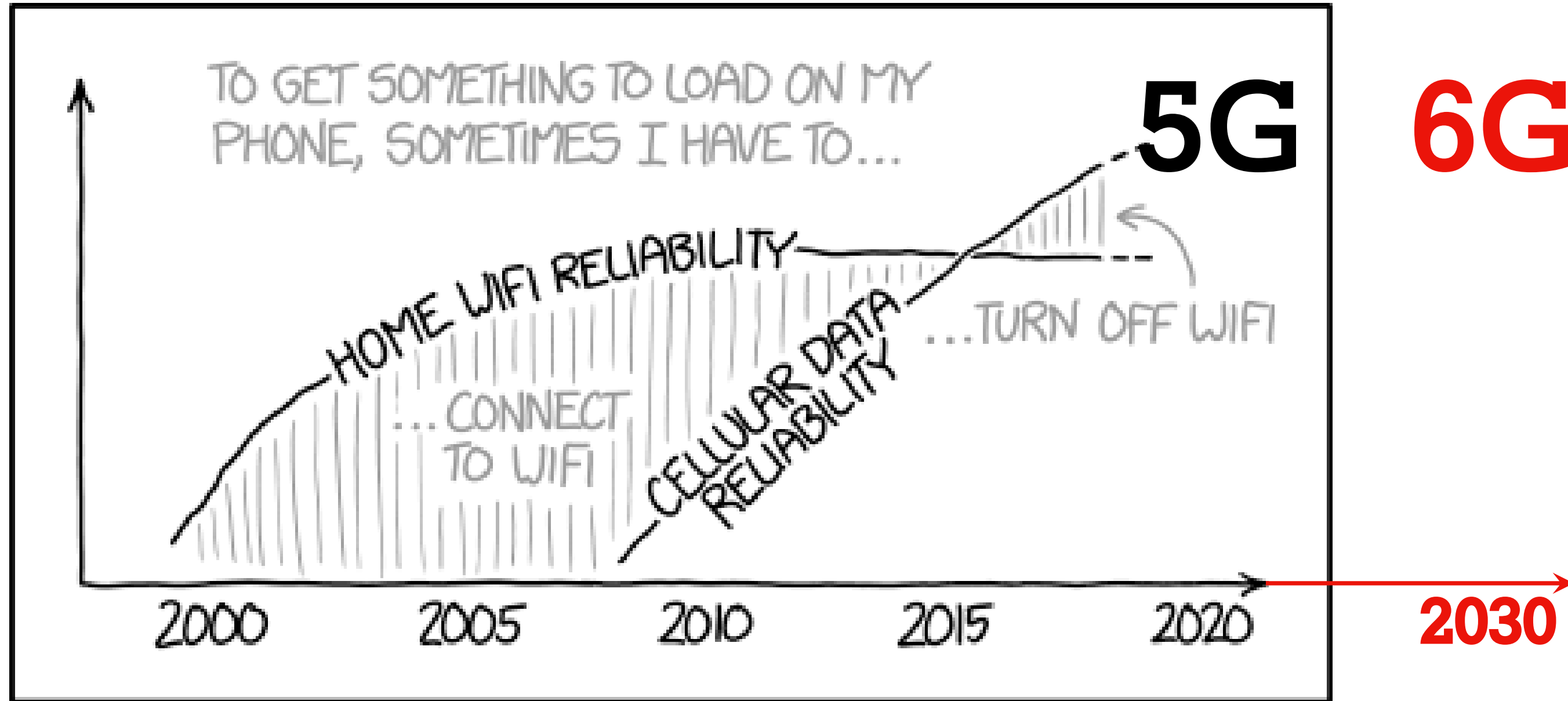
Agenda 29.05.2026

- Megatrends & The Times They Are A-Changin'
- Telecommunications Primer
- Mobile Communications, Frequencies, Immissions, Standards
- Cellular Network Planning, Architecture
- Traffic Development
- Edge Computing
- MNO Spectrum in Austria
- Slow & Fast Fading, Massive MIMO
- 5G Slicing
- 5G Security
- 6G
- Latest News: SMS Blaster

- AMA

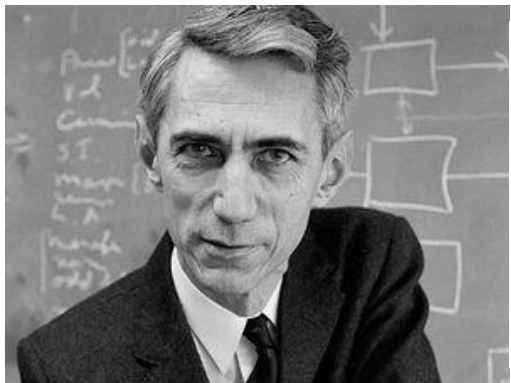
... and who the hell are SUPI, SUCI and SEPP?

The Times They Are A-Changin'



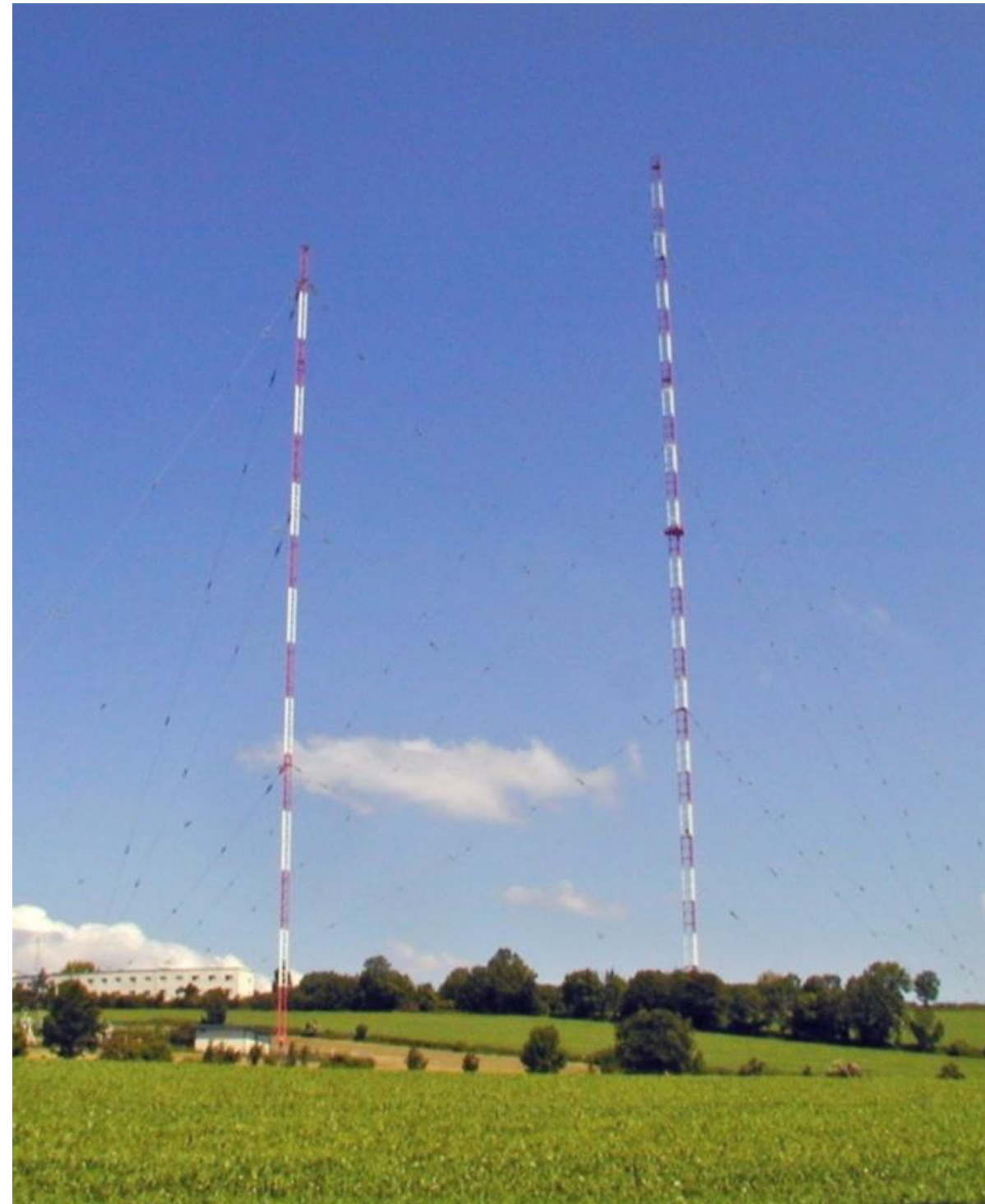
IT SEEMS WEIRD FROM A NETWORKING POINT OF VIEW, BUT SOMETIME IN THE LAST FEW YEARS THIS FLIPPED FOR ME.

Telecommunications Primer - Signal-to-Noise Ratio



$$C = B \log_2 \left(1 + \frac{S}{N} \right)$$

- S ... Signal: e.g. Transmitter power
- N ... Noise: e.g. Interference („Crosstalk“)



Mobile Communications are brought to you by...

James Clerk Maxwell 1831 – 1879 (Classical EM Theory)

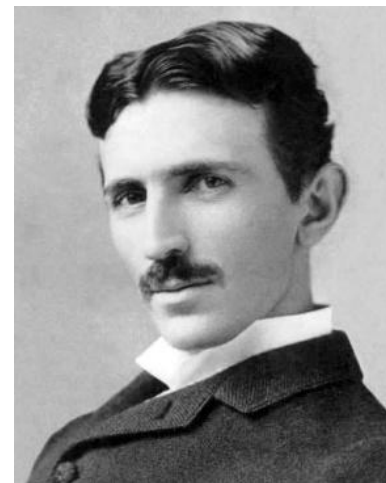
Nikola Tesla 1856 – 1943 (AC, Induction)

Heinrich Hertz 1857 – 1894 (proof of EM waves)

Guglielmo Marconi 1874 – 1934 (long distance radio)

Erwin Schrödinger 1887 – 1961 (Quantum Theory)

Hedy Lamarr 1913 – 2000 (Spread Spectrum)



© Wikipedia

Major Innovation Drivers: Military, Industry

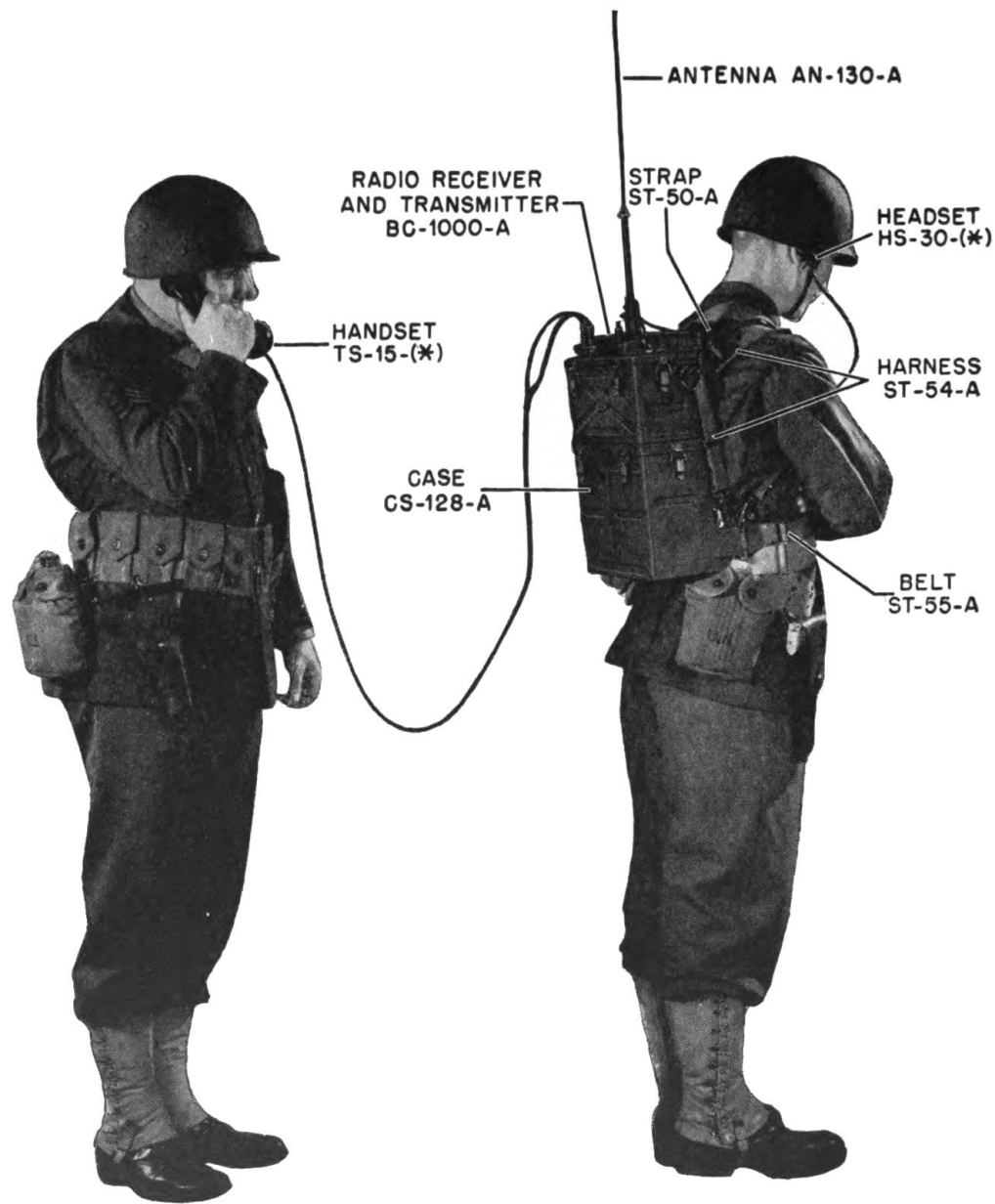


Figure 1. Radio Set SCR-300-A, In Use, Viewed From Right Side.



Woman with Walkie Talkie
Source: DLA/Special Collection

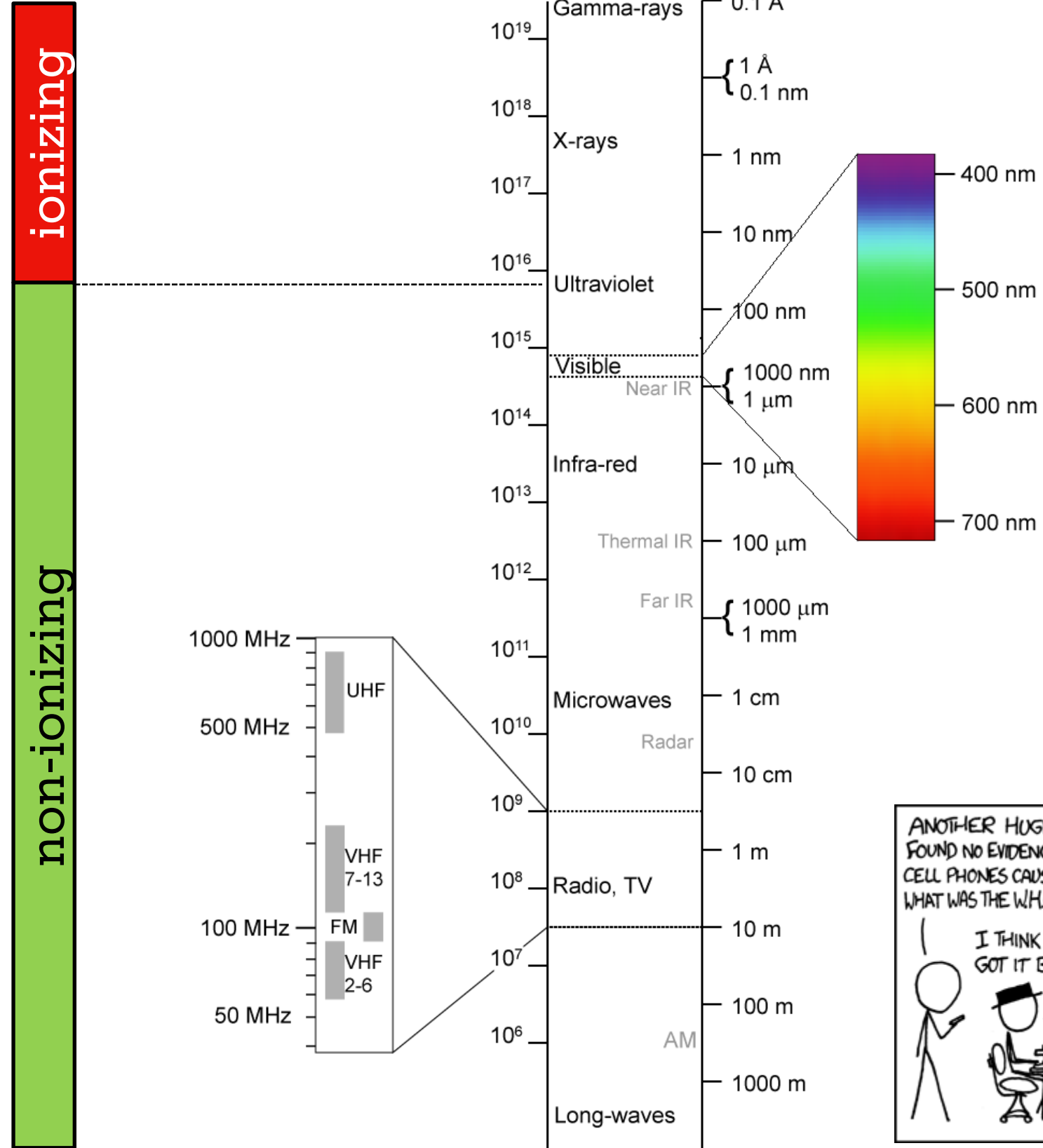


Walkie Talkie from 1939
Source: DLA/Special Collection

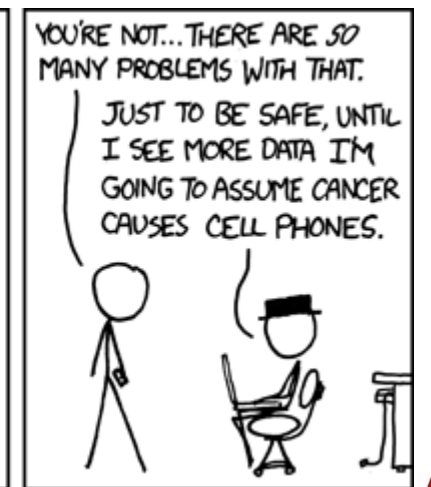
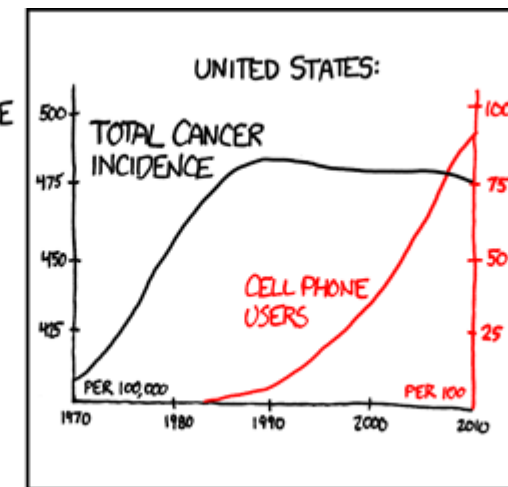
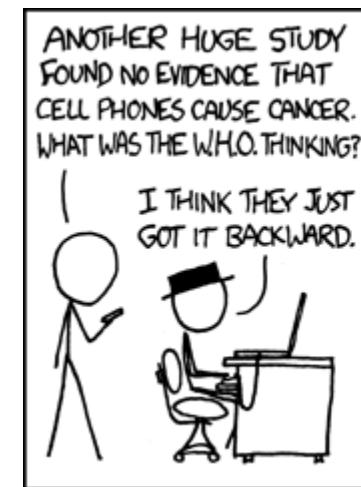
© Wikipedia

Frequencies and EMF

$$E = h \cdot f$$

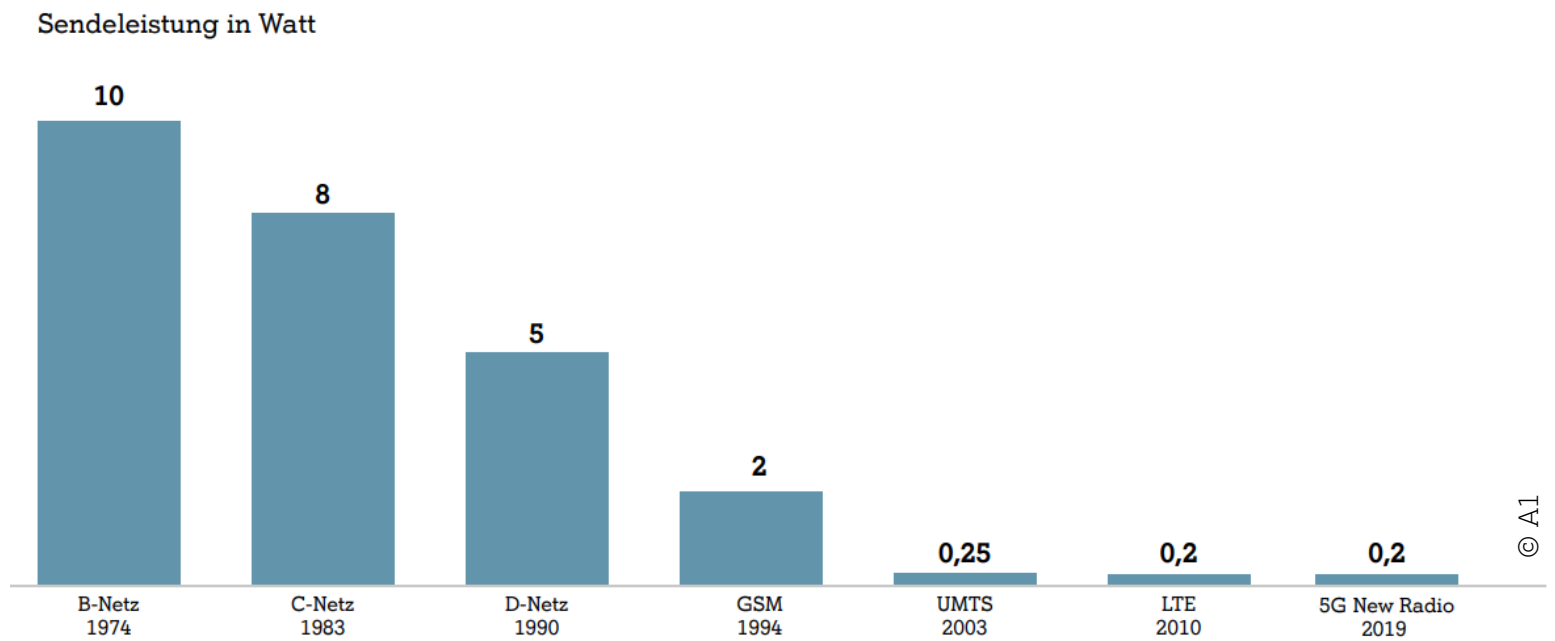
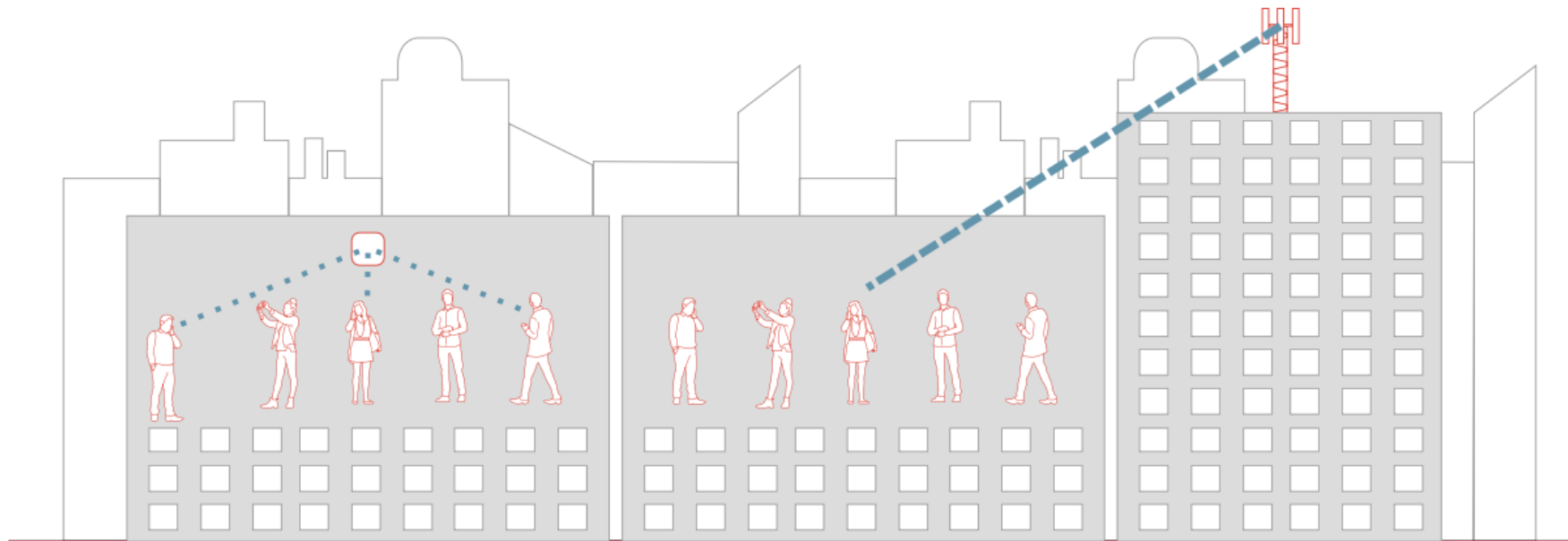
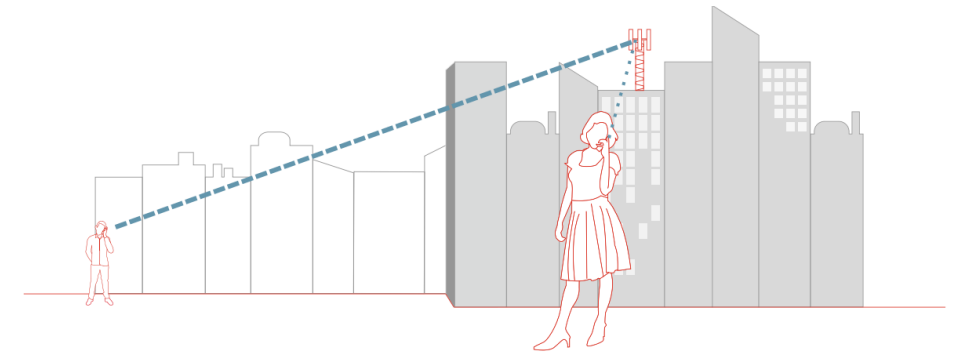
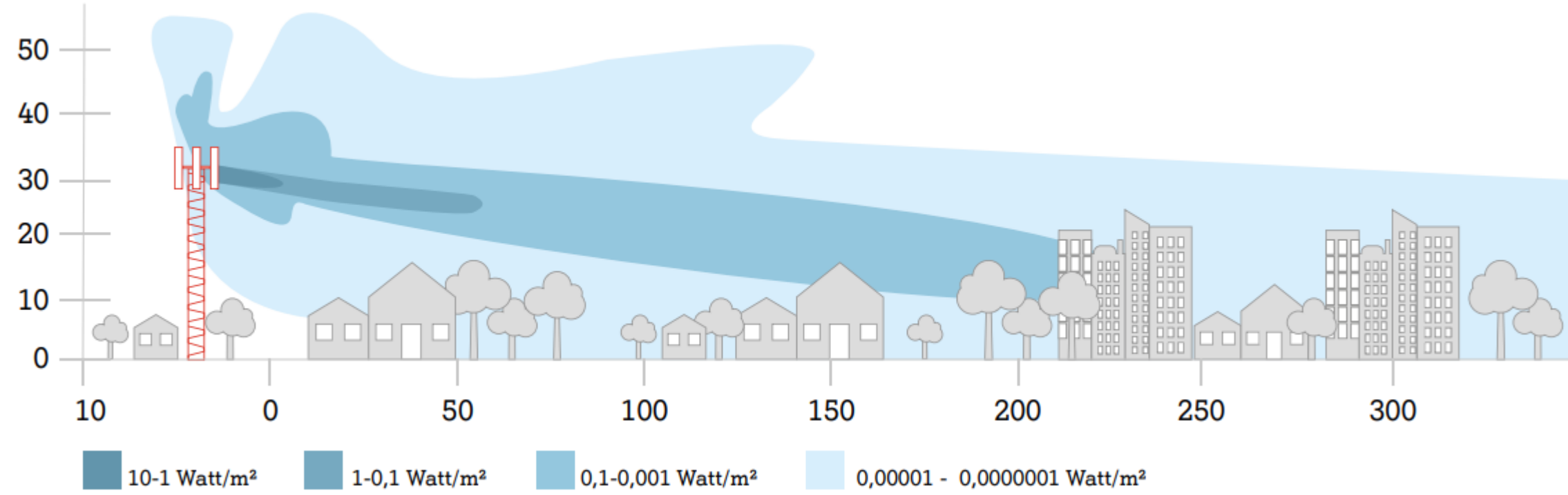


© A1



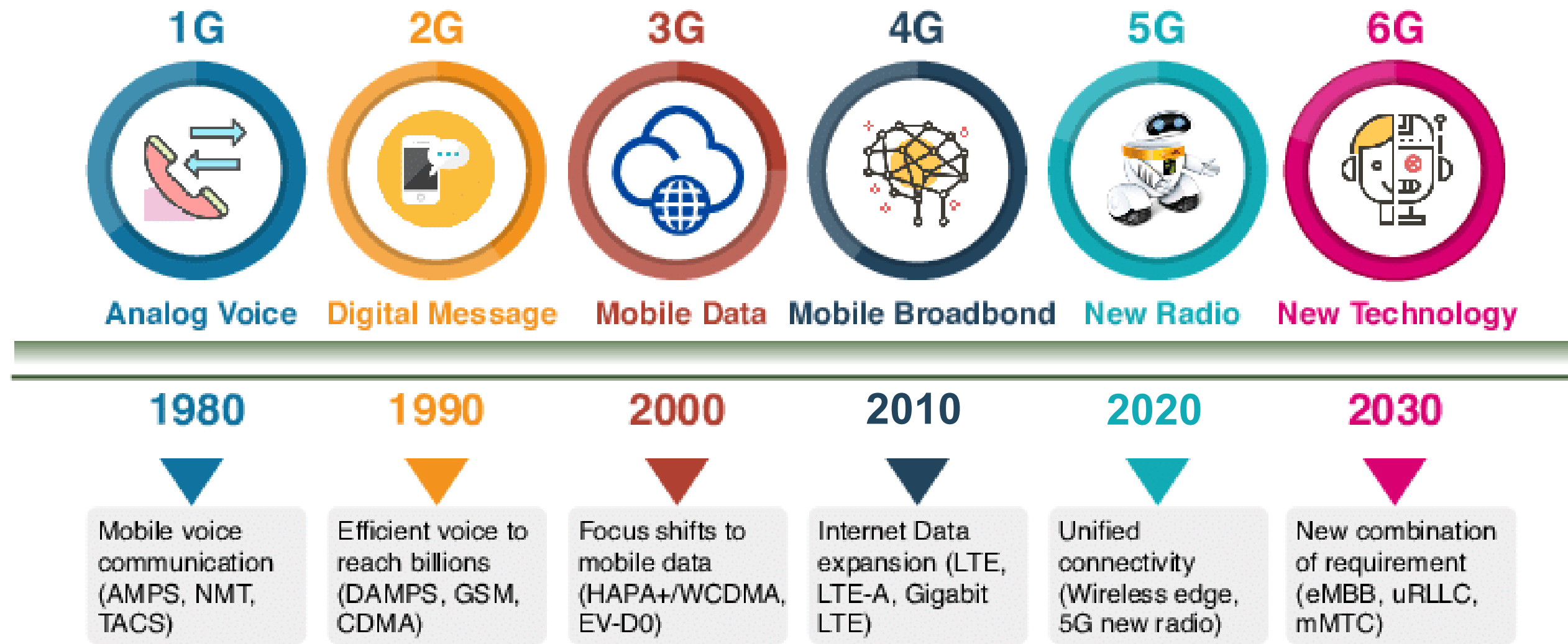
© xkcd, <https://xkcd.com/925/>

Immission



Technology Generations: Industry Standards guarantee interoperability

Spectrum, Technologies, Features

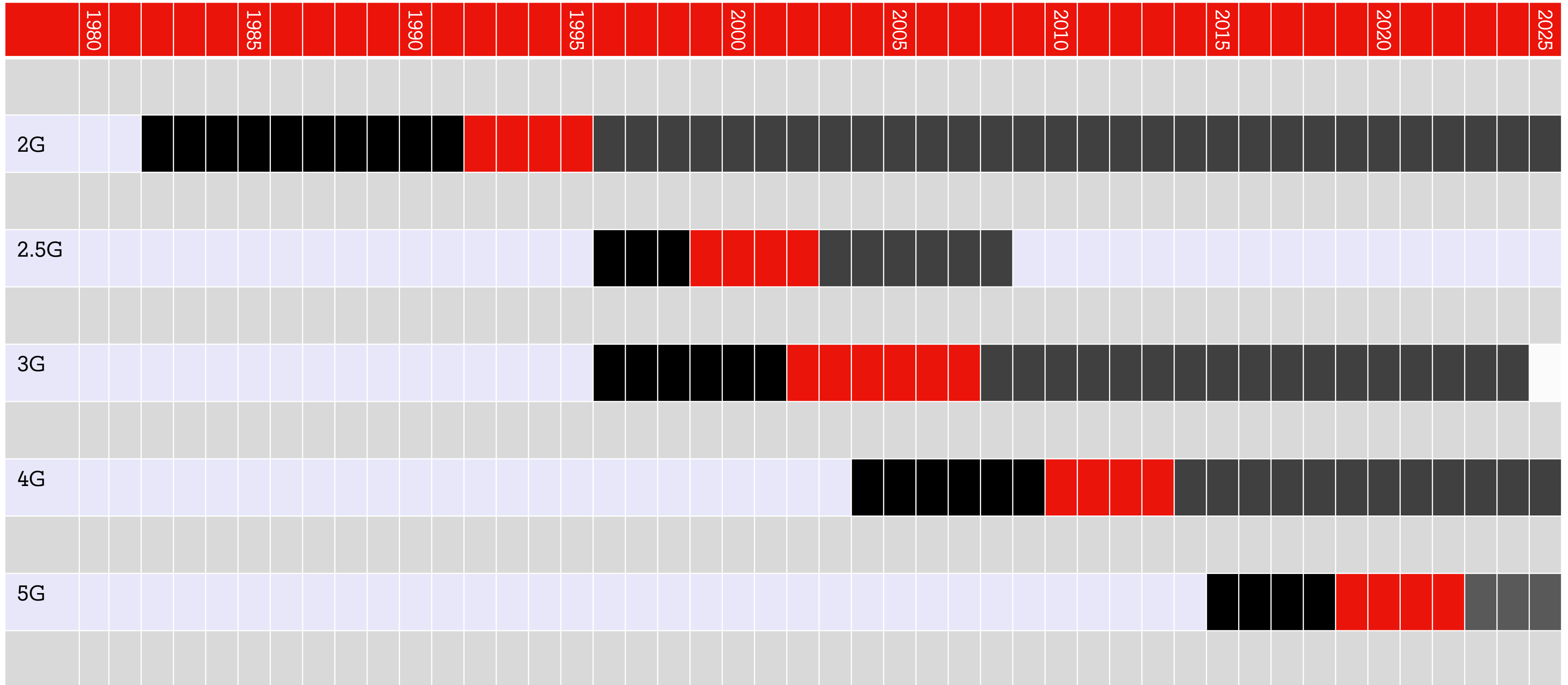


© ResearchGate.net

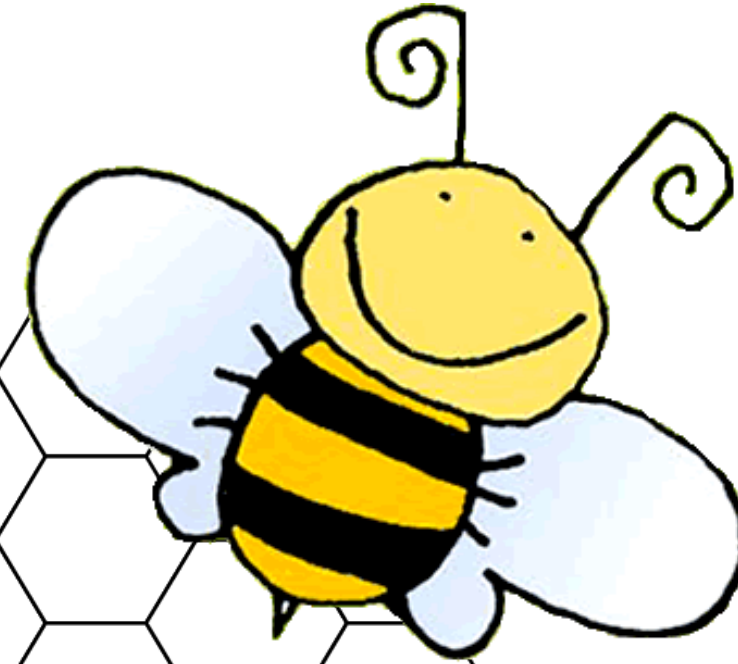
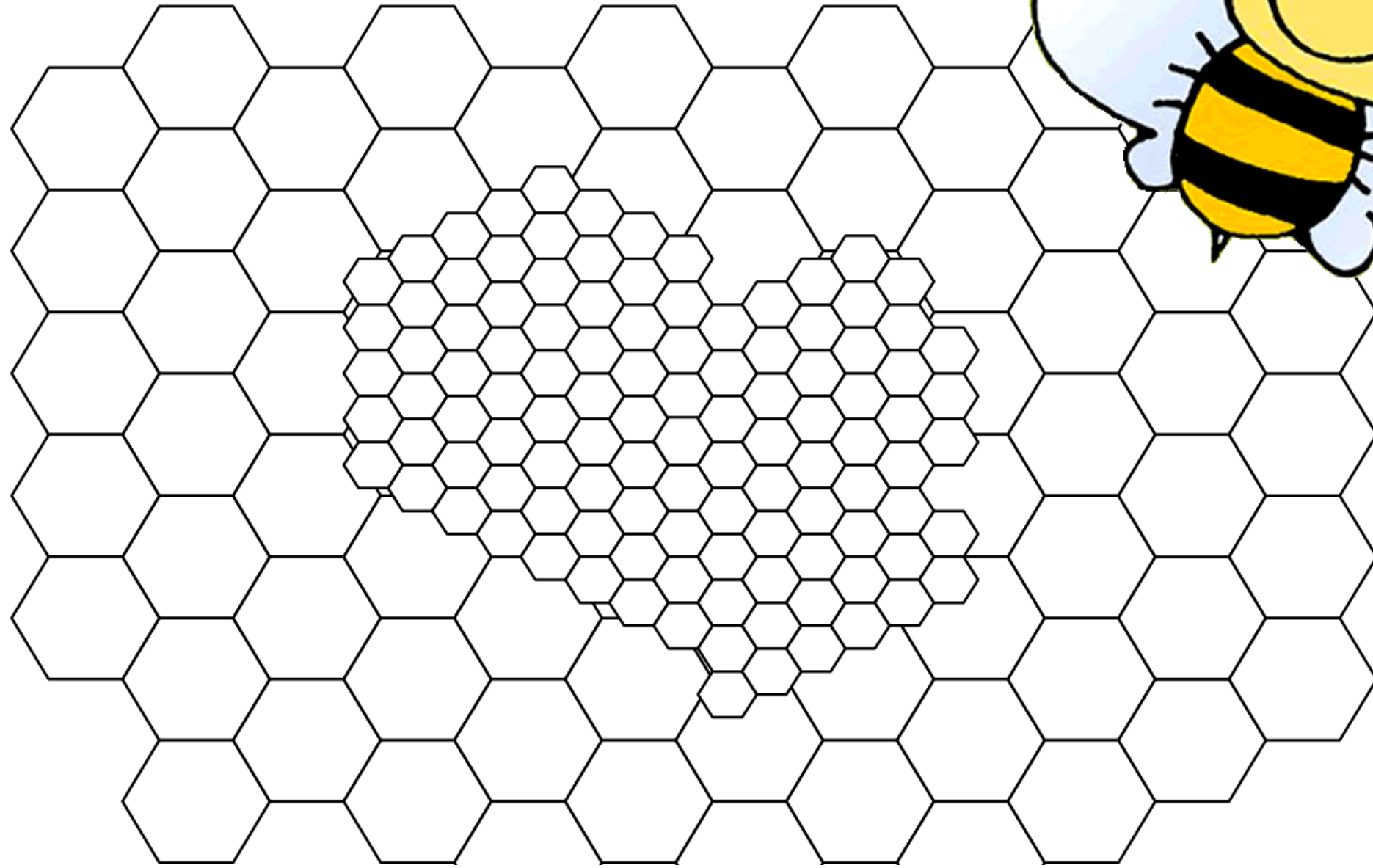
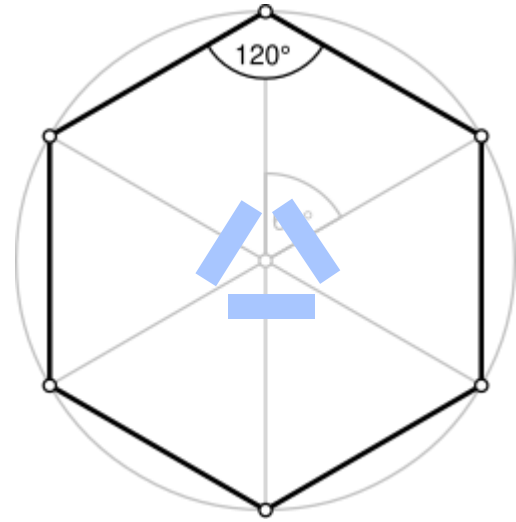
Time To Market

Development
Trials/Uptake
Success

A1 Austria



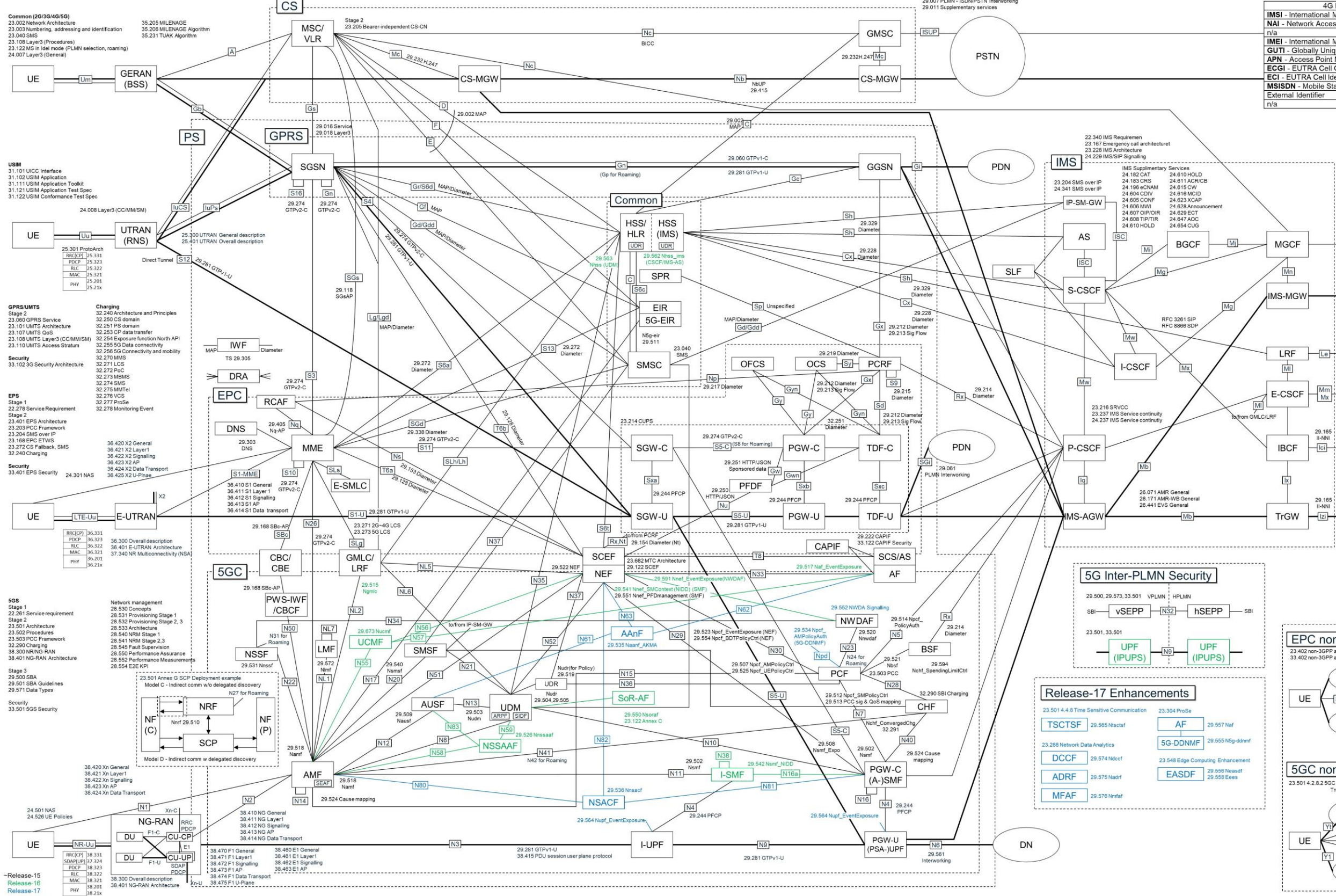
Cellular Network Planning



2G/3G/4G/5G RAN + Core Architecture

3GPP Overall Architecture and Specifications

Copyright © 2021 Muneaki Ogawa (twitter: @nickel0, GitHub: @nickel0)
This diagram is released under the CC BY-NC-SA 4.0 License.



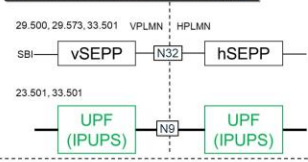
4G and 5G Identifier mapping

4G Identifier	5G Identifier
IMSI - International Mobile Subscriber Identity	SUPI - Subscription Permanent Identifier
NAI - Network Access Identifier	SUPI - Subscription Permanent Identifier
n/a	SUCI - Subscription Concealed Identifier
IMEI - International Mobile Equipment Identity	PEI - Permanent Equipment Identifier
GUTI - Globally Unique Temporary UE Identity	5G-GUTI - 5G Globally Unique Temporary UE Identity
APN - Access Point Name	DNN - Data Network Name
ECGI - E-UTRA Cell Global Identifier	NCGI - NR Cell Global Identifier
ECI - E-UTRA Cell Identity	NCI - NR Cell Identity
MSISDN - Mobile Station ISDN	GPSI - Generic Public Subscription Identifier
External Identifier	GPSI - Generic Public Subscription Identifier
n/a	S-NSSAI - Single-Network Slice Selection Assistance Information

5G Network Function Abbreviations

- Release-15**
- 5G-EIR - 5G Equipment Identity Register
 - AAuF - AKMA (Authentication and Key Management for Applications) Anchor Function
 - AF - Application Function
 - AMF - Access and Mobility Management Function
 - AUSF - Authentication Server Function
 - ARPF - Authentication credential Repository and Processing Function
 - BSF - Binding Support Function
 - CAPIF - Common API Framework for 3GPP northbound APIs
 - CHF - Charging Function
 - I-UPF - Intermediate UPF
 - LMF - Location Management Function
 - LRF - Location Retrieval Function
 - N3IWF - Non-3GPP InterWorking Function
 - NEF - Network Exposure Function
 - NRF - Network Repository Function
 - NSSF - Network Slice Selection Function
 - NWDAF - Network Data Analytics Function
 - PCF - Policy Control Function
 - SCP - Service Communication Proxy
 - SEAF - Security Anchor Function
 - SEPP - Security Edge Protection Proxy
 - SIDF - Subscription Identifier De-concealing Function;
 - SMF - Session Management Function
 - SMF - Short Message Service Function
 - TNAP - Trusted Non-3GPP Access Point
 - TNGF - Trusted Non-3GPP Gateway Function
 - TWIF - Trusted WLAN Interworking Function
 - UDM - Unified Data Management
 - UDR - Unified Data Repository
 - UDSF - Unstructured Data Storage Function
 - UPF - User Plane Function
- Release-16**
- IPUPS - Inter-PLMN UP Security
 - I-SMF - Intermediate SMF
 - NSSAAF - Network Slice-specific and SNPN Authentication and Authorization Function
 - UCMF - UE radio Capability Management Function
 - SoR-AF - Steering of Roaming Application Function
- Release-17**
- 5G DDNMF - 5G Direct Discovery Name Management Function
 - ADRF - Analytics Data Repository Function
 - EASDF - Edge Application Server Discovery Function
 - MFAF - Messaging Framework Adaptor Function
 - DCCF - Data Collection Coordination Function
 - NSACF - Network Slice Admission Control Function
 - TSCTSF - Time Sensitive Communication and Time Synchronization function

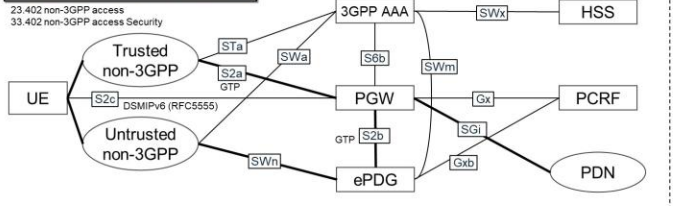
5G Inter-PLMN Security



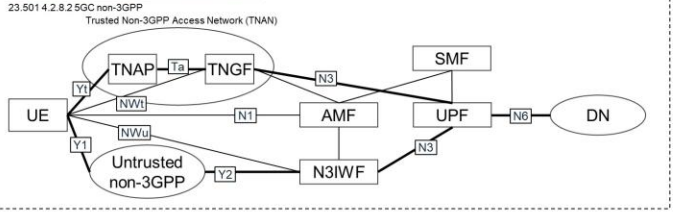
Release-17 Enhancements

- TSCTSF - 23.501 4.8 Time Sensitive Communication
- DCCF - 23.501 5.5.2 Data Collection Coordination Function
- ADRF - 23.501 5.5.3 Analytics Data Repository Function
- MFAF - 23.501 5.5.4 Messaging Framework Adaptor Function
- AF - 23.501 5.5.5 Application Function
- 5G-DDNMF - 23.501 5.5.6 5G Direct Discovery Name Management Function
- EASDF - 23.501 5.5.7 Edge Application Server Discovery Function

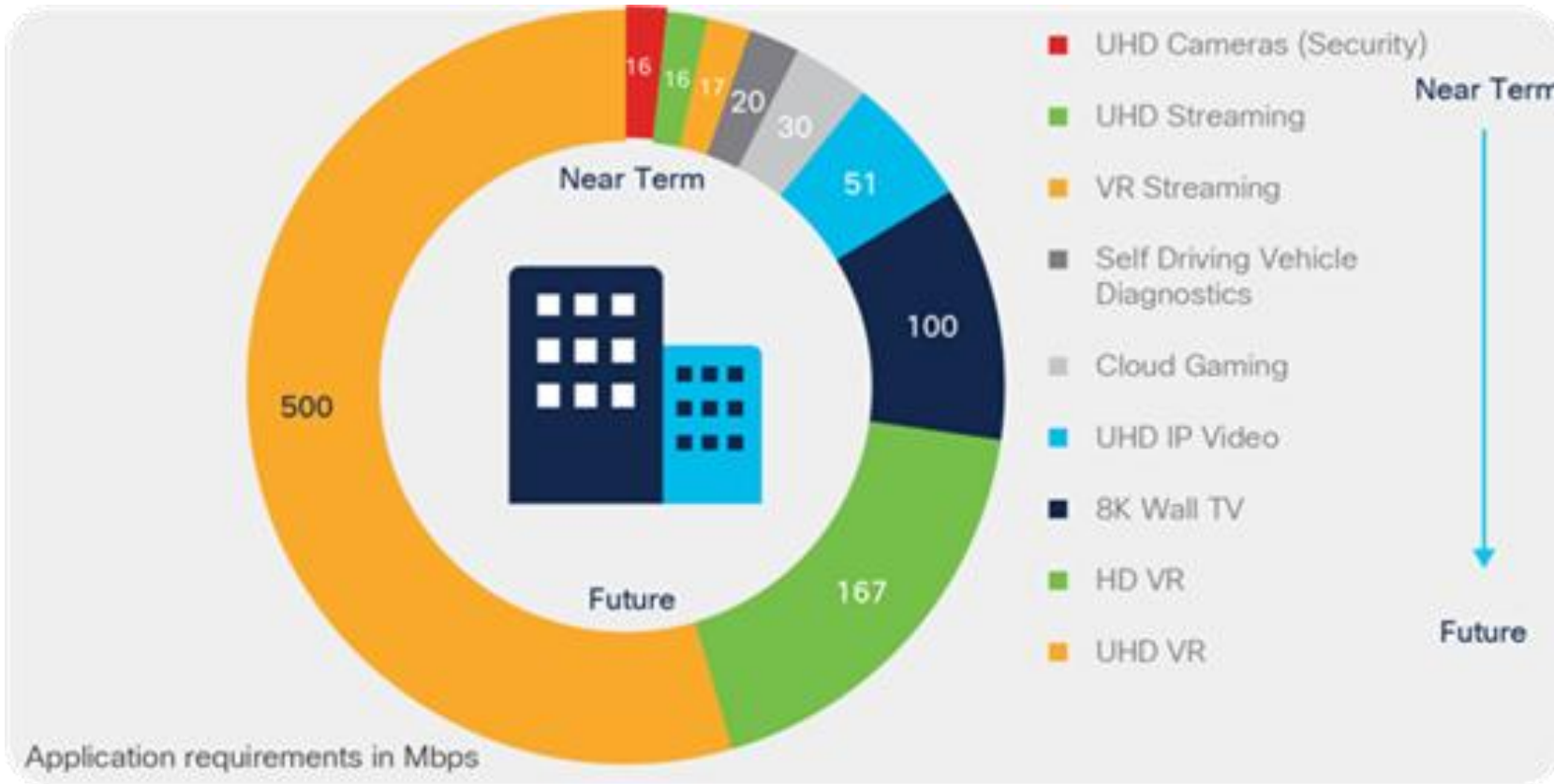
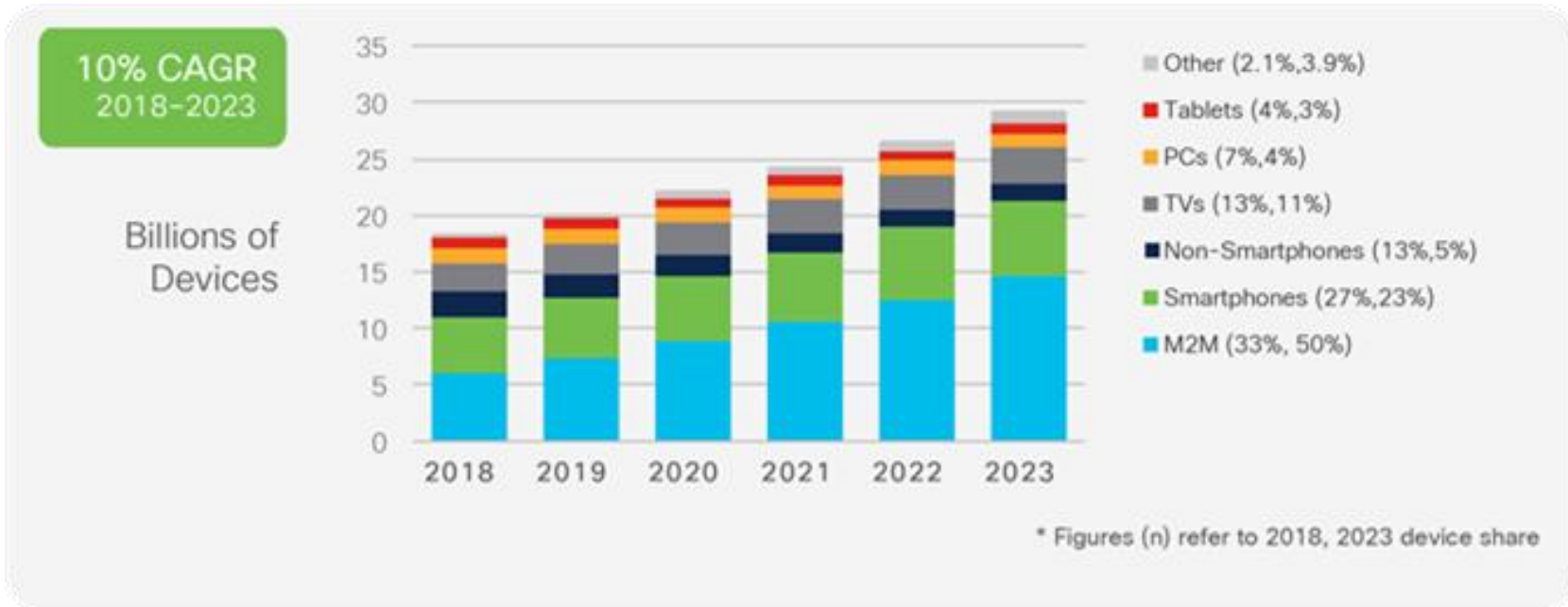
EPC non-3GPP Access



5GC non-3GPP Access



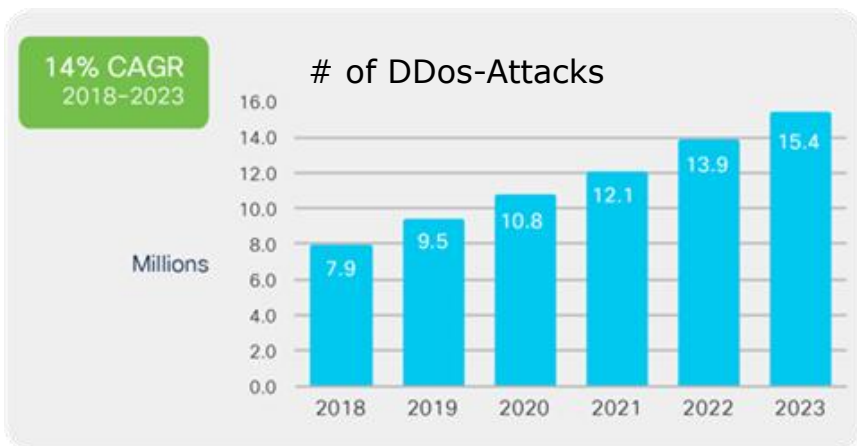
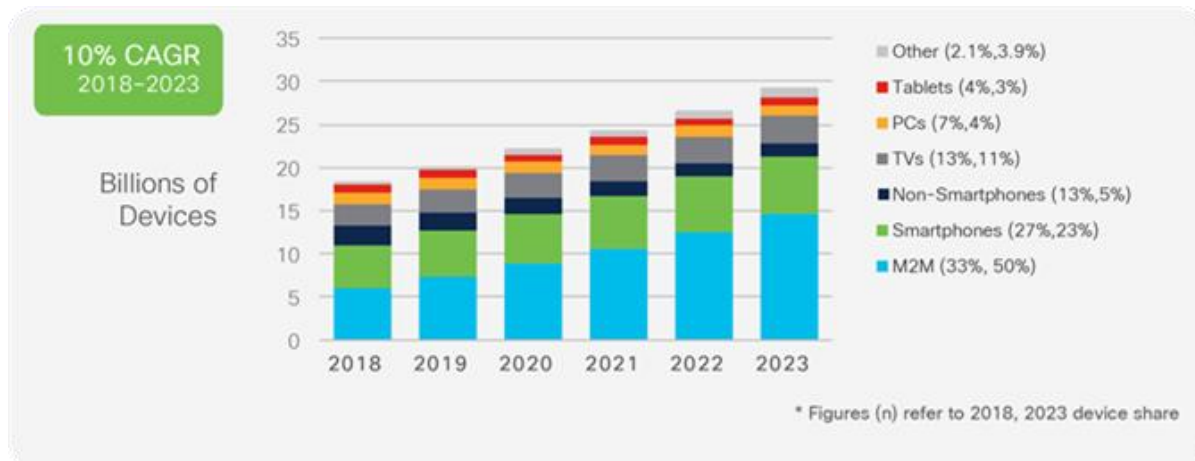
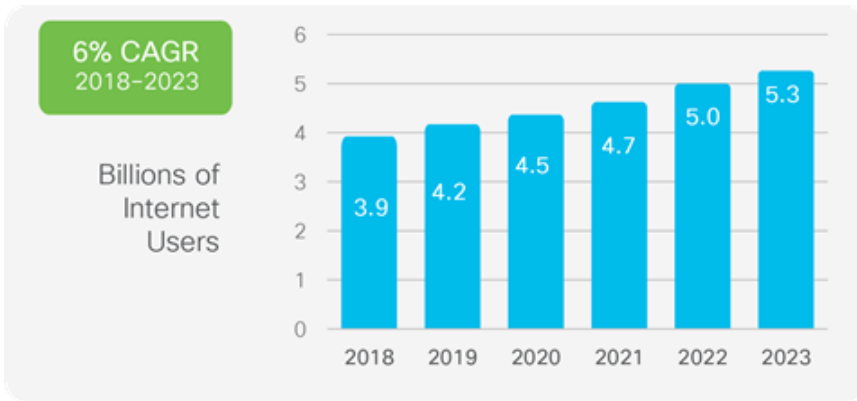
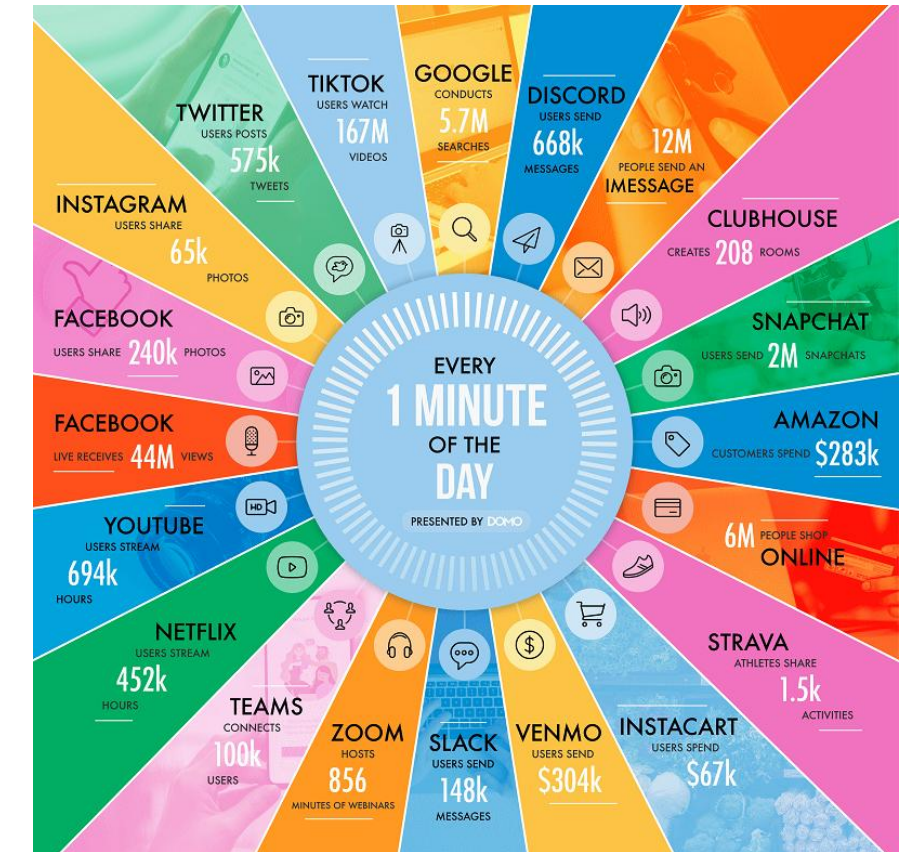
Cisco Annual Internet Report & Internetminute



© DOMO

Traffic Development: The Sky is the Limit

- **Busy-hour** traffic grows stronger than overall traffic
- Traffic shift wired → wireless
- Broadband Datarates double every 5 years
→ Backhaul demand rises



AHB 1959



2+2

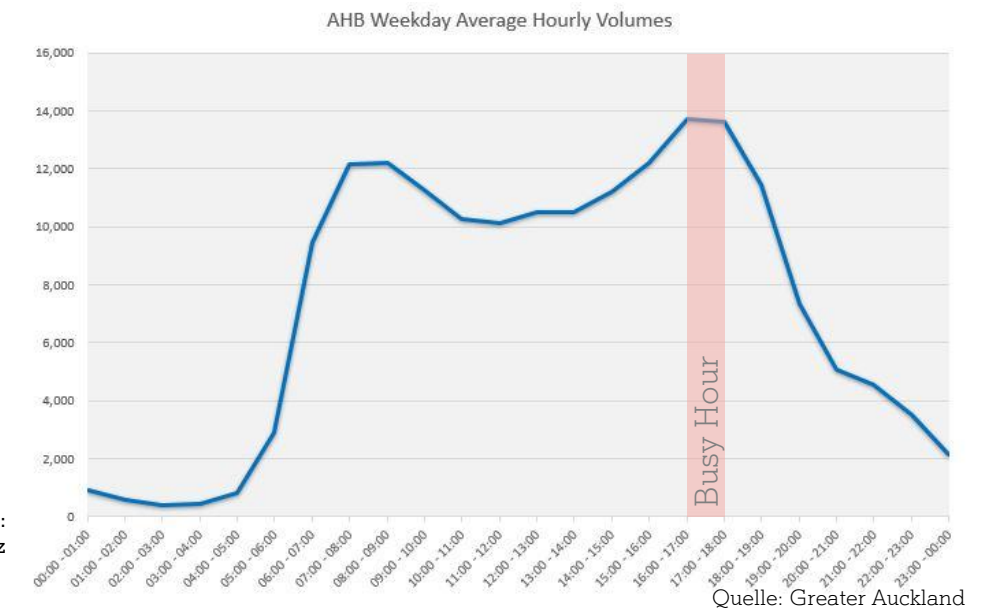
AHB 2009



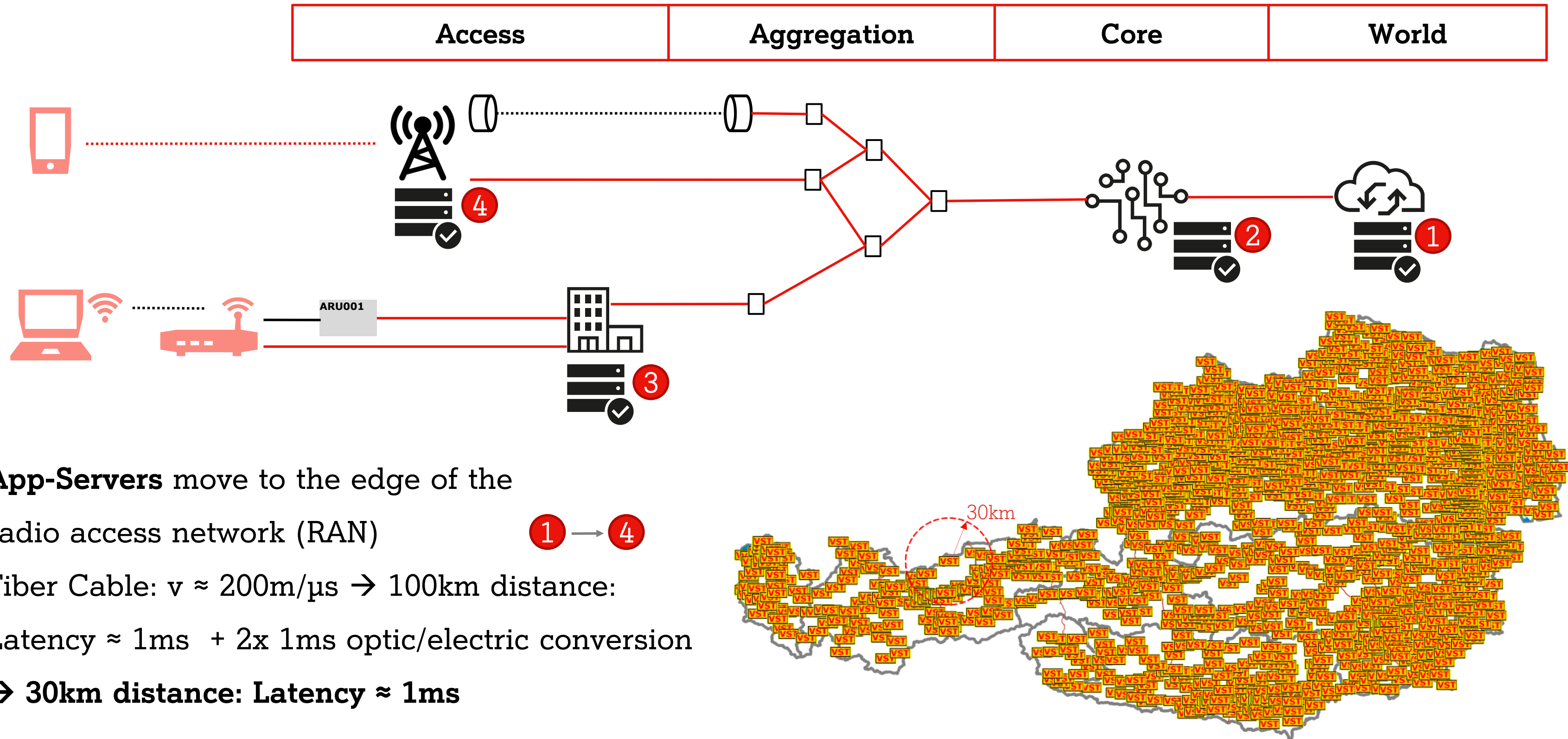
(2+2) + (2+2)

Quelle: nzhistory.govt.nz

Quelle: John Selkirk/stuff.co.nz



Edge Computing



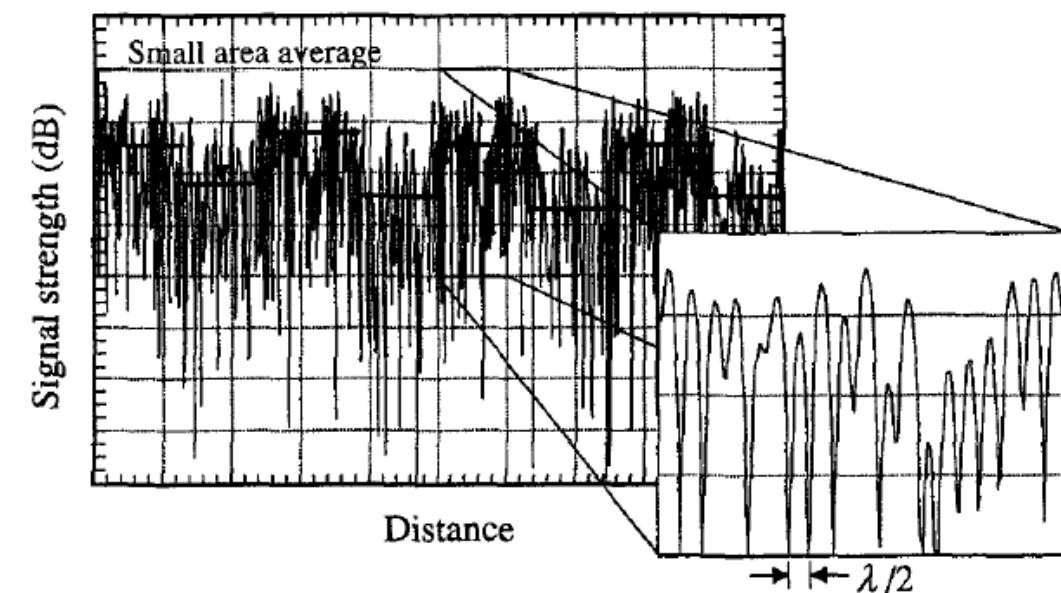
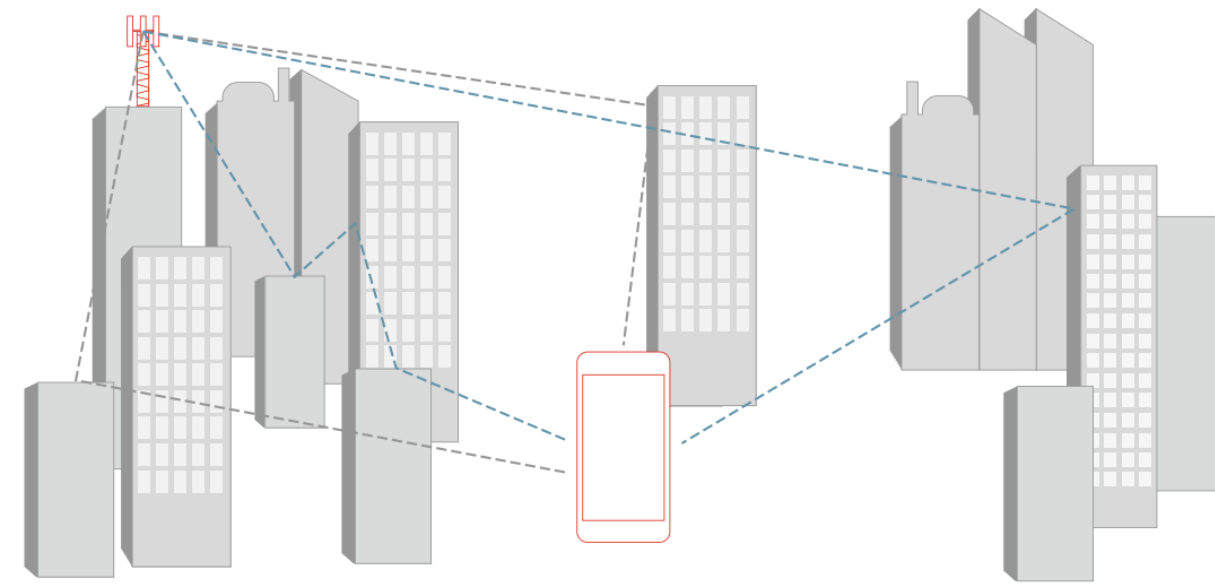
- **App-Servers** move to the edge of the radio access network (RAN) 1 → 4
- Fiber Cable: $v \approx 200\text{m}/\mu\text{s} \rightarrow 100\text{km distance}$:
 Latency $\approx 1\text{ms} + 2 \times 1\text{ms}$ optic/electric conversion
 $\rightarrow 30\text{km distance: Latency} \approx 1\text{ms}$

MNO Spectrum Assets in Austria

Spectrum (MHz)	Band Classification	Duplex	Coverage Layer	Performance Layer	Voice Layer	Data Layer	Fiber Like
700	Low	FDD	●	◐	◑	◐	○
800	Low	FDD	●	◐	●	◐	○
900	Low	FDD	●	◐	●	◐	○
1500	Mid	SDL	◐	◐	○	◐	○
1800	Mid	FDD	◑	◑	◐	◑	○
2100	Mid	FDD	◑	◐	◑	◐	○
2300	Mid	TDD	◐	◐	○	◑	○
2600	Mid	FDD	◐	◐	◐	◐	○
2600	Mid	TDD	◐	◐	○	◐	○
3500	Mid	TDD	◐	●	○	●	◑
26000	High	TDD	○	●	○	●	●

Fast Fading vs Slow Fading

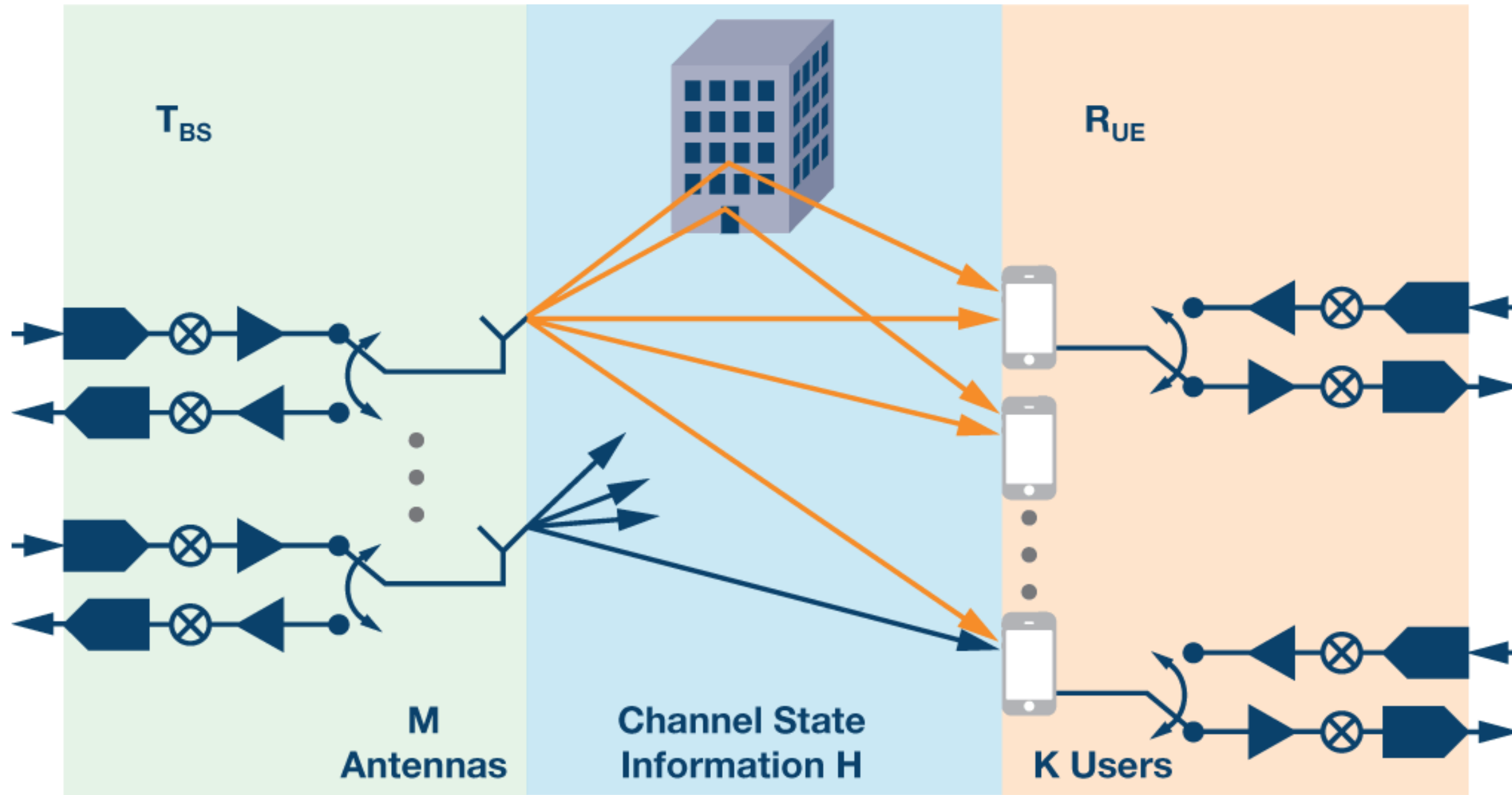
- Fast fading** is also called **multi-path fading**, as a result of multi-path propagation. When multi-path signals arriving at a UE, the constructive and destructive phases create a variation in signal strength.
- Slow fading** is also called **shadowing**. When a UE moves away from a cell the signal strength drops down slowly.



$$\lambda = \frac{c}{f}$$

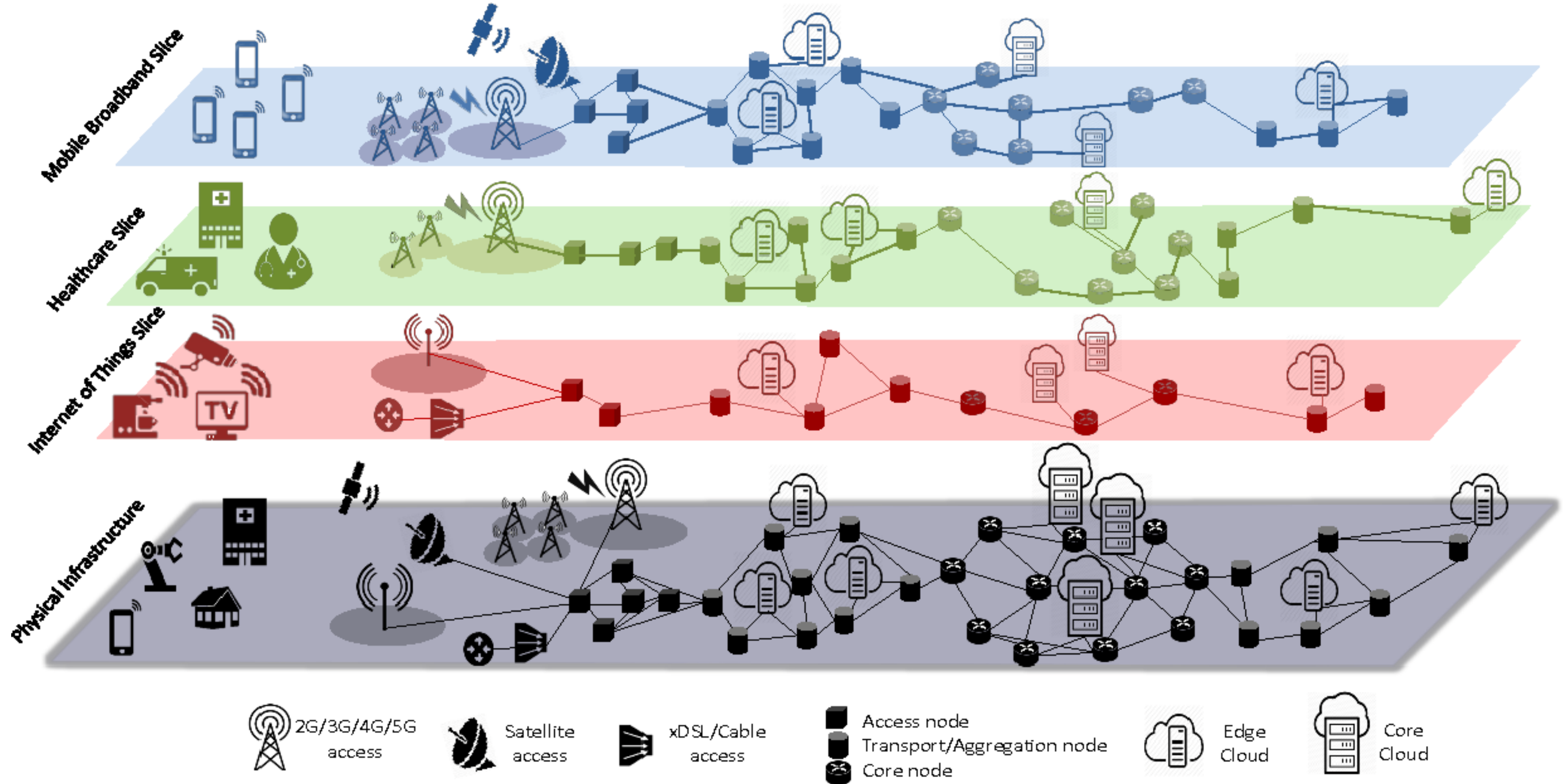
Massive MIMO – Electronic Beamforming

MIMO: Multiple Input Multiple Output



Quelle: mwrf.com

5G Network Slicing – Your own Virtual Network



5G Security – The Paradigm Shift

- **4G Network: Proprietary hardware** (bespoke SoC), security is **perimeter-based** with distinct physical boundaries between core and edge/radio nodes
 - **5G Network: Software-defined and virtualized.** Relies on distributed cloud hosting and Network Function Virtualization (NFV), provides flexibility and scalability/speed.
- **Paradigm Shift: De-coupling** core static **hardware perimeters** to **dynamic software-defined** ecosystem

SUPI & SUCI

- **SUPI: Subscription Permanent Identifier:** never exposed over radio link

- **SUCI: Subscription Concealed Identifier**

→ Using Elliptic Curve Integrated Encryption Scheme (ECIES)-based public-key encryption under MNO control on the SIM/UE, identities are concealed before transmission.

→ Only the Home Public Land Mobile Network (HPLMN) contains the matching private key required to decrypt the SUCI

Authentication Framework

Primary Auth Options:

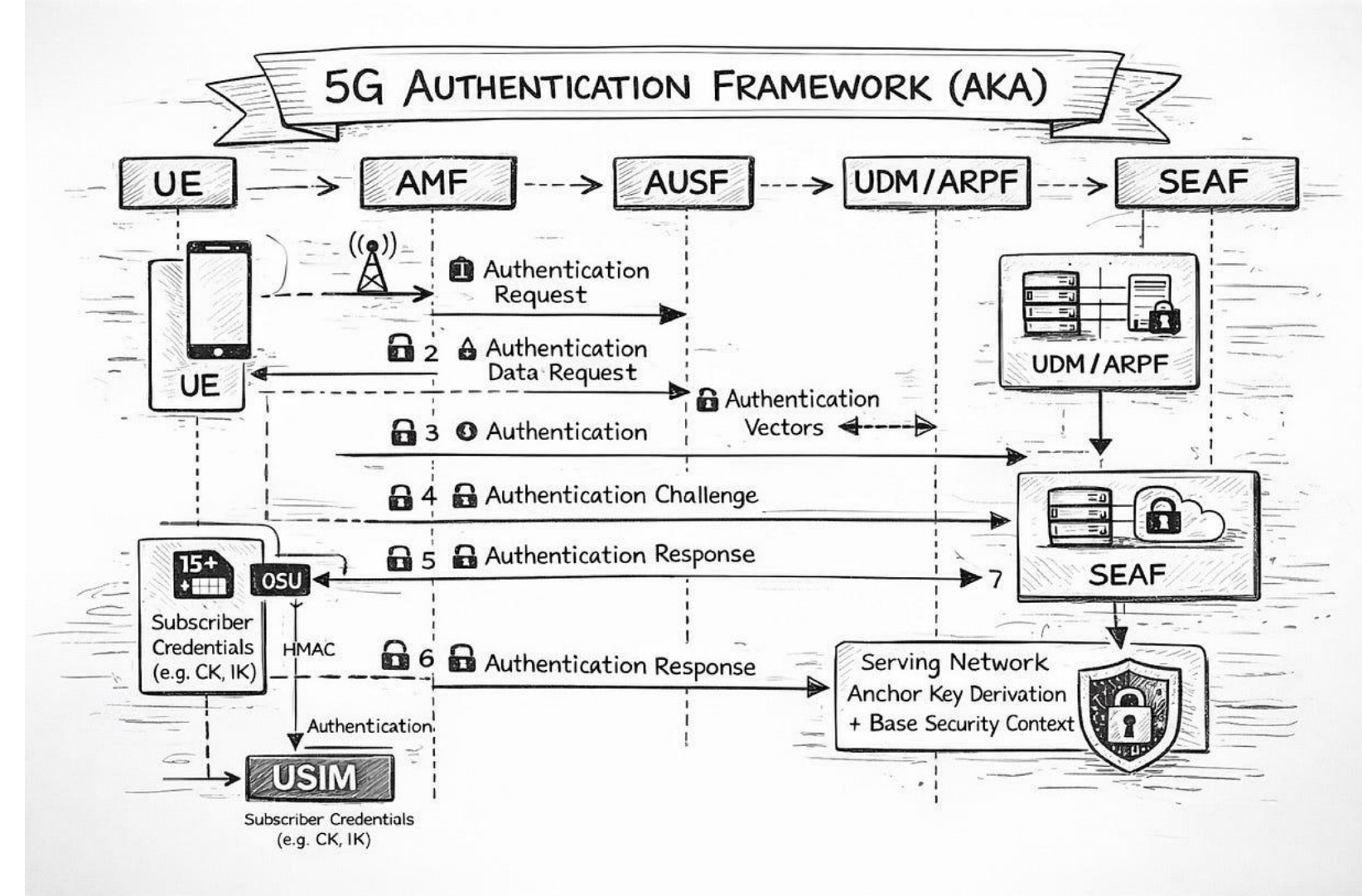
- Standardized options include 5G Authentication and Key Agreement (5G-AKA) and Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement (EAP-AKA). The access layer is fully decoupled, enabling security integration also with Wi-Fi 6 or satellite links.

Home Control Anchor:

- Authentication terminates directly in the HPLMN on Authentication Server Function (AUSF)/ Unified Data Management (UDM). The serving network cannot fake validation. Security Anchor Function (SEAF) decouples mobility from root keys.

Secondary Auth:

- Enables out-of-band enterprise domain EAP authentication, isolating industrial slices from basic carrier access frameworks



5G Key Derivation Tree

HPLMN Root Key (K):

- Cryptographically unexposed master seed stored safely in SIM and Home Network UDM

Security Anchor Key (K_{SEAF}):

- Serving network-level root key, generated in AUSF and handled by SEAF. Tied to specific visited network domain ID

Core Signalling Keys (K_{AMF}, K_{NAS}):

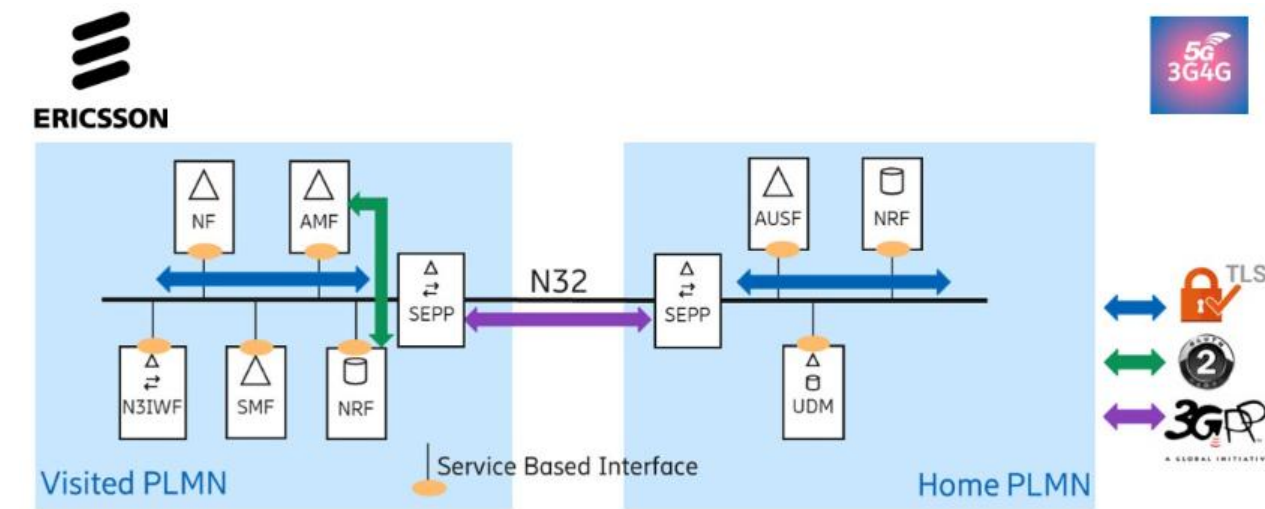
- Derived from K_{SEAF} to secure the Non-Access Stratum (NAS) control plane, splitting into unique identity (K_{NASint}) and ciphering (K_{NASenc}) variations.

Access Stratum Keys (K_{gNB}):

- Keys delivered down to base station. Ensures that a physical compromise of a cell tower HW cannot leak core infrastructure signalling keys

SEPP – Securing Roaming

N32 SEPP Proxy



- Traditional roaming exposed carriers to **malicious signaling over SS7/Diameter** backbones due to implicitly trusted models.
- 5G resolves this by standardizing the **Security Edge Protection Proxy (SEPP)**. Operating at the edge of each PLMN boundary, SEPP handles **mutual authentication** and enforces **application-layer cryptography** protection (N32 PRINS protocol), signing and encrypting inter-operator traffic.
- N32-PRINS **approved cipher suites**:

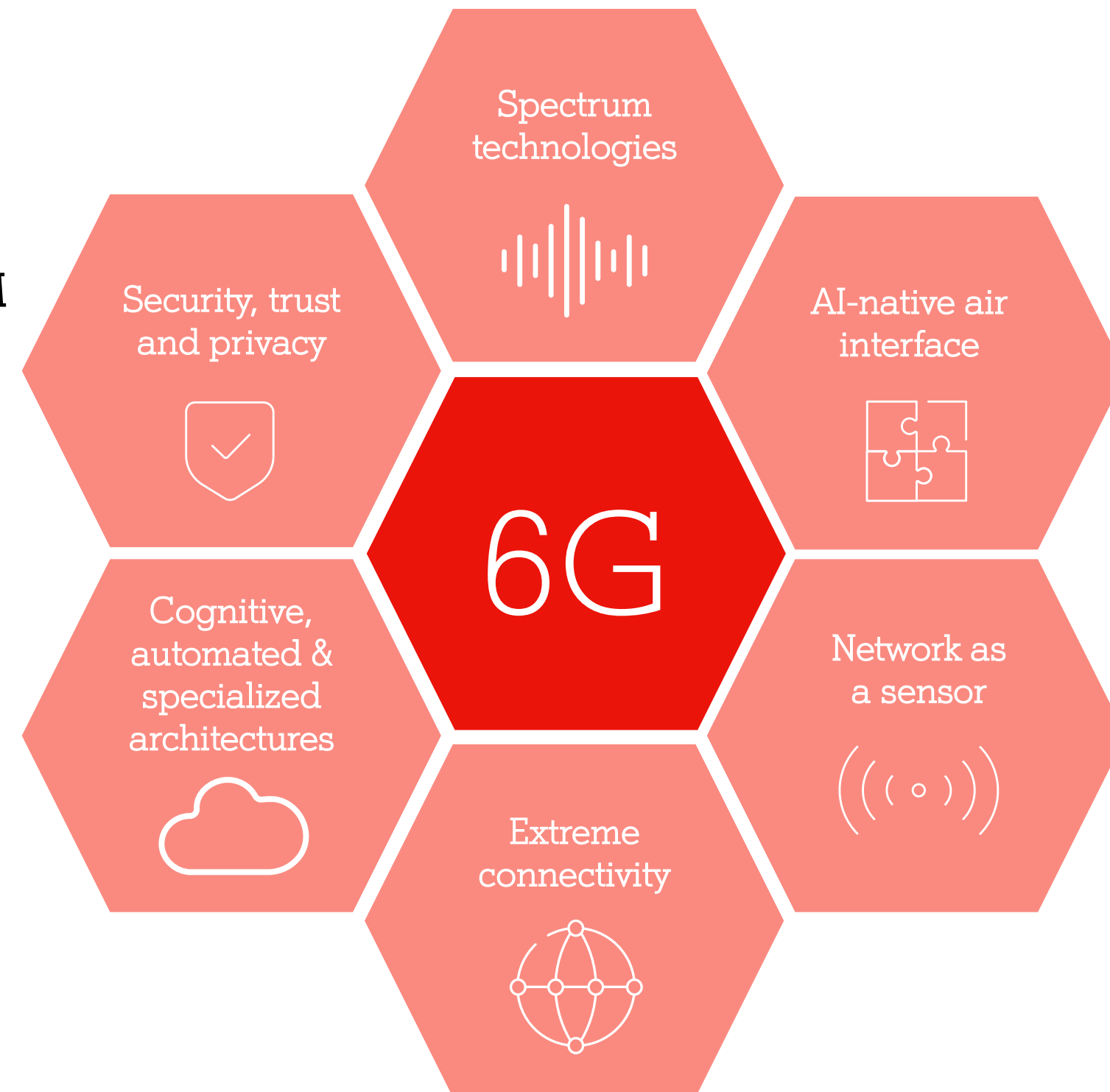
Suite Identifier	Encryption Algorithm	Integrity Method	Deployment Scenario
A128GCM	AES-GCM (128 bit)	AEAD GHASH	Default high-throughput roaming profiles
A256GCM	AES-GCM (256 bit)	AEAD GHASH	Military, government & financial slices
A128CBC-HS256	AES-CBC (128 bit)	HMAC-SHA256	Backward compatibility, IoT environments

6G - Bringing Future to Life

Six key technology areas for the 6G essential infrastructure

PQC Migration:

Post-Quantum Cryptography algorithms inside AUSF/UDM



6G: Networks that

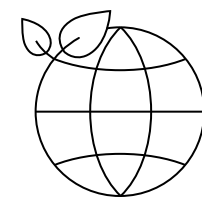
- **Sense**
- **Think**
- **Act**

Key value drivers for 6G



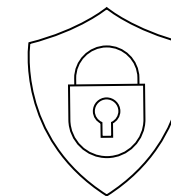
Green by design

▲ 10X capacity increase with 50% power reduction, compared to 5G



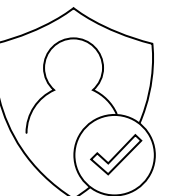
Security and privacy

▲ Increasing security and privacy risks require higher levels of control



Digital inclusion

▲ Aims to address three key factors: accessibility, affordability and consumability





6G Introduction is planned in two steps

6G day-one focus

- Extreme MIMO on existing grid
- Smooth migration and core evolution
- Programmable networks and API native
- Framework for native AI
- Framework for energy efficiency



NextG
mobile
broadband

Fixed
Wireless
Access (FWA)

Immersive
/Cloud
gaming

Extended
Reality

IoT/LPWA
native support

6G evolution and beyond

Potential services that take us:

- From connectedness to **togetherness**: immersive holographic experience, connect the unconnected
- From information to **knowledge**: cognitive and complete context awareness, leveraging ambient IoT, digital twins, sensing
- From efficiency to **purpose**: mission & life-critical services supported by subnetworks

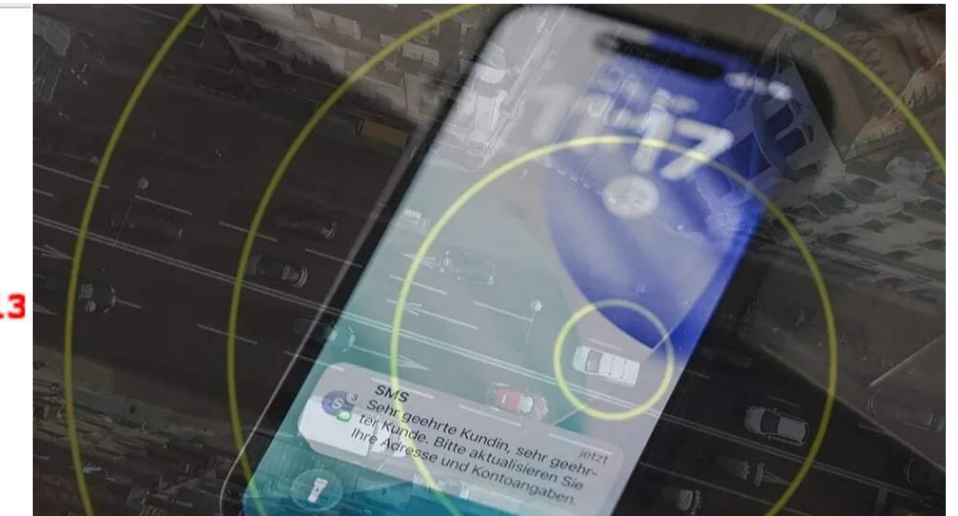
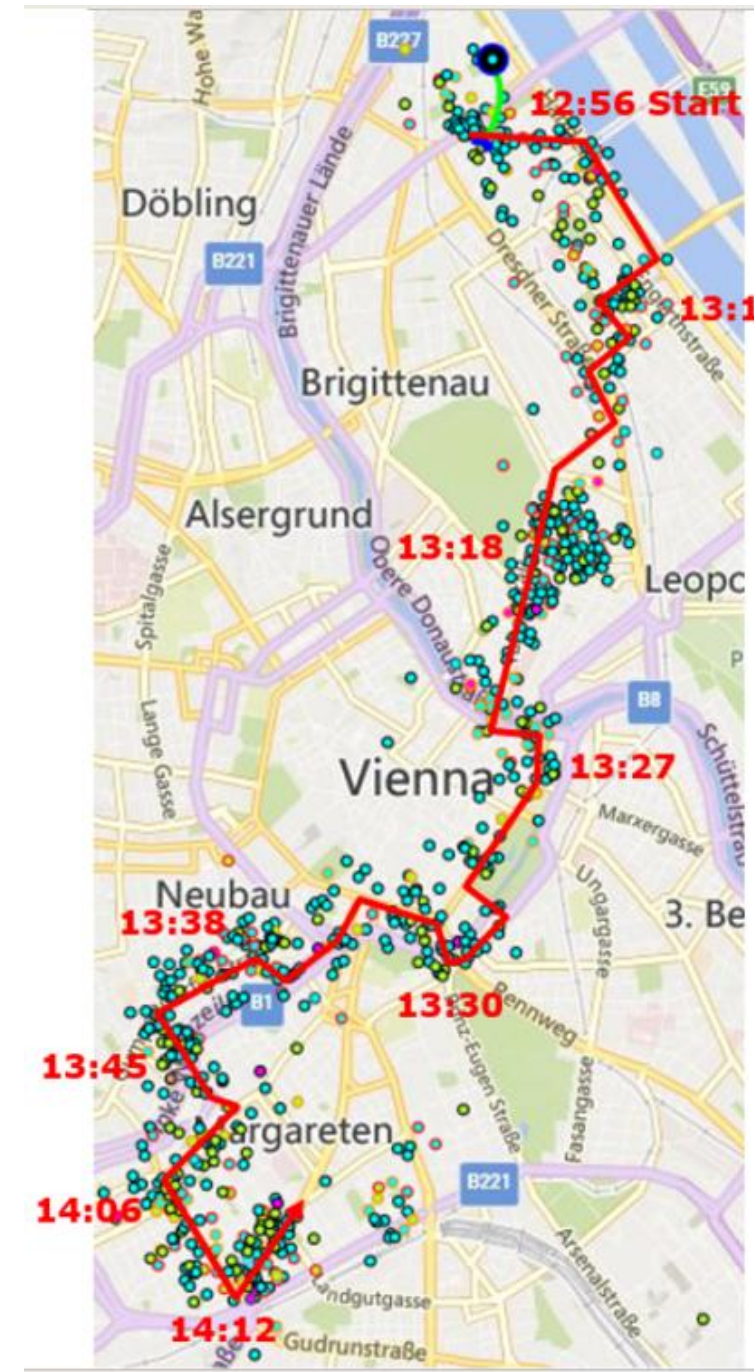


6G to build on 5G success and do so in a more efficient, economical, scalable and sustainable way

Augmenting humanity and the full realization of digital-physical fusion

Latest News: SMS Blaster

- **Situation:** Weeks leading up to the Eurovision Song Contest (ESC) at Wiener Stadthalle
- **Action:** Increase in **fraudulent SMS messages**. **Unusual activity on the mobile network**. Criminals had been using a so-called **SMS blaster** to set up a **fake 2G network across Vienna for days** and were sending out fake text messages
- **Result:** Suspect caught, SMS Blaster off air



In the Media

The screenshot shows the top of the Bild website. On the left is the large red 'Bild' logo. To its right are navigation links: 'Hey...' (with a dropdown arrow), 'BILD-KI', 'INFOS ZU BILDPLUS', 'DEBATTE', 'WETTER', 'BILDPLAY', 'MARKTPLATZ', 'ZEITUNG', 'SUCHE', and 'ANMELDEN'. Below these is a horizontal menu with categories: 'STARTSEITE', 'NEWS', 'POLITIK', 'REGIO', 'UNTERHALTUNG', 'KAUFBERATER', 'SPORT', 'FUSSBALL', 'RATGEBER', 'GESUNDHEIT', 'SEX & LIEBE', and 'AUTO SPIELE'. A 'BREAKING NEWS' banner is visible at the bottom of the screenshot with the text 'JLBUS +++ BUGGENHOUT (BELGIEN): MEHRERE TOTE BEI ZUGUNGLÜCK MIT SCHULBUS +++ BUGGENHOUT (C'.

Mit strahlendem Gerät und Baby im Auto

Chinese (32) verschickte Millionen Phishing-SMS

SMS blaster used in smishing scheme targeting Eurovision fans

Published: 21 May 2026

Niamh Ancell, Journalist



Image by Getty/Picture Alliance

DERSTANDARD

AUF GROSSVERANSTALTUNGEN

32-jähriger SMS-Betrüger in Wien festgenommen

Über "SMS Blaster" konnte der Verdächtige seine Mobiltelefone in seiner Umgebung...

19. Mai 2026, 15:45

106 Postings Später lesen



Kronen Zeitung UNABHÄNGIG

Di, 26.05.2026 25°C Wien

Krone+ Österreich Wien Politik Stars & Society Sport Ges

MIT SOHN AUF RÜCKBANK

So blockierte Chinese Notrufe um den Song Contest

Wien | 20.05.2026 05:30

Millionen Phishing-SMS in Wien versendet – Tatverdächtiger in Haft

19.05.2026 | 13:16 Redaktion Polizeiticker Österreich



Die beschlagnahmte Geräte im Fall großflächiger Phishing-SMS im Großraum Wien. (Bildquelle: LPD Wien) Am Donnerstag, 17. Mai 2026, nahm die Polizei in Wien einen mutmaßlichen Betreiber sogenannter „SMS Blaster“ fest. Der 32-Jährige soll Millionen betrügerische Phishing-SMS versendet haben.

The screenshot shows the top of the 'Heute' website. It features the 'Heute' logo, the temperature 'Wien 28°', and navigation links for 'Leser-Reporter', 'Suchen', and 'Anmelden'. Below the header is a menu with categories: 'Österreich', 'Sport', 'Nachrichten', 'Life', 'Unterhaltung', 'Community', 'Gewinnen', and 'Mehr'. There is also a 'Video Neuste' link.



Hightech-Betrug in Wien Mit "SMS Blaster": Millionen Fake-Nachrichten versendet

Ein 32-Jähriger soll in Wien mit SMS-Blastern Millionen Fake-Nachrichten verschickt haben. Jetzt sitzt er in Haft.

The screenshot shows an article on the MeinBezirk website. The title is 'Mann mit speziellen Betrugs-SMS-Geräten im Auto geschnappt'. The article is dated '19. Mai 2026, 13:56 Uhr' and is written by 'Redaktion Antonio Šećerović'. The article text is partially visible, mentioning the seizure of the devices.

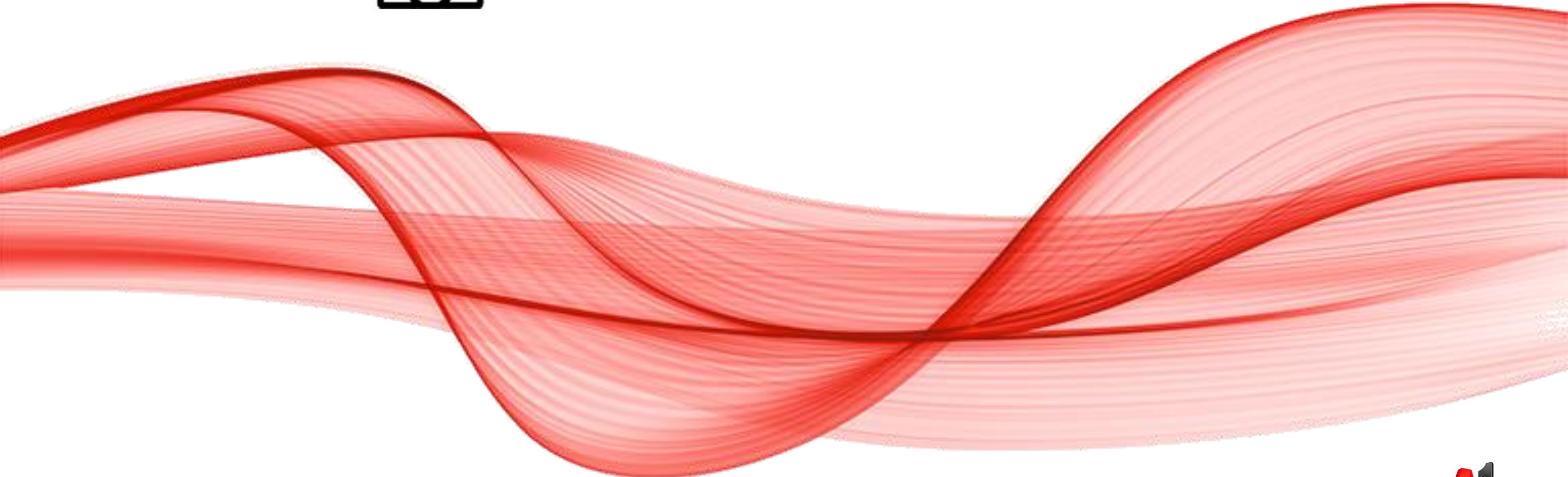


Thank you!

AMA



ASK ME ANYTHING





Stay secure! 