

TLP:WHITE

5G, NEW TELECOMMUNICATIONS STANDARDS

BETWEEN OPPORTUNITIES AND RISKS

SWITHAK



CONFIDENTIALITY

- ▶ No photography
- ▶ No video recording
- ▶ The slides will be available on my blog at the end of the presentation
- ▶ Please respect my privacy



- ▶ Security professional / Incident Responder
- ▶ Threat analyst on my free time
- ▶ Passionate by new security and also old fashioned ones
- ▶ Telecommunications aficionado
- ▶ Other subjects of interest:
 - ▶ Geopolitics
 - ▶ Defense
 - ▶ Intelligence
 - ▶ Legal frameworks



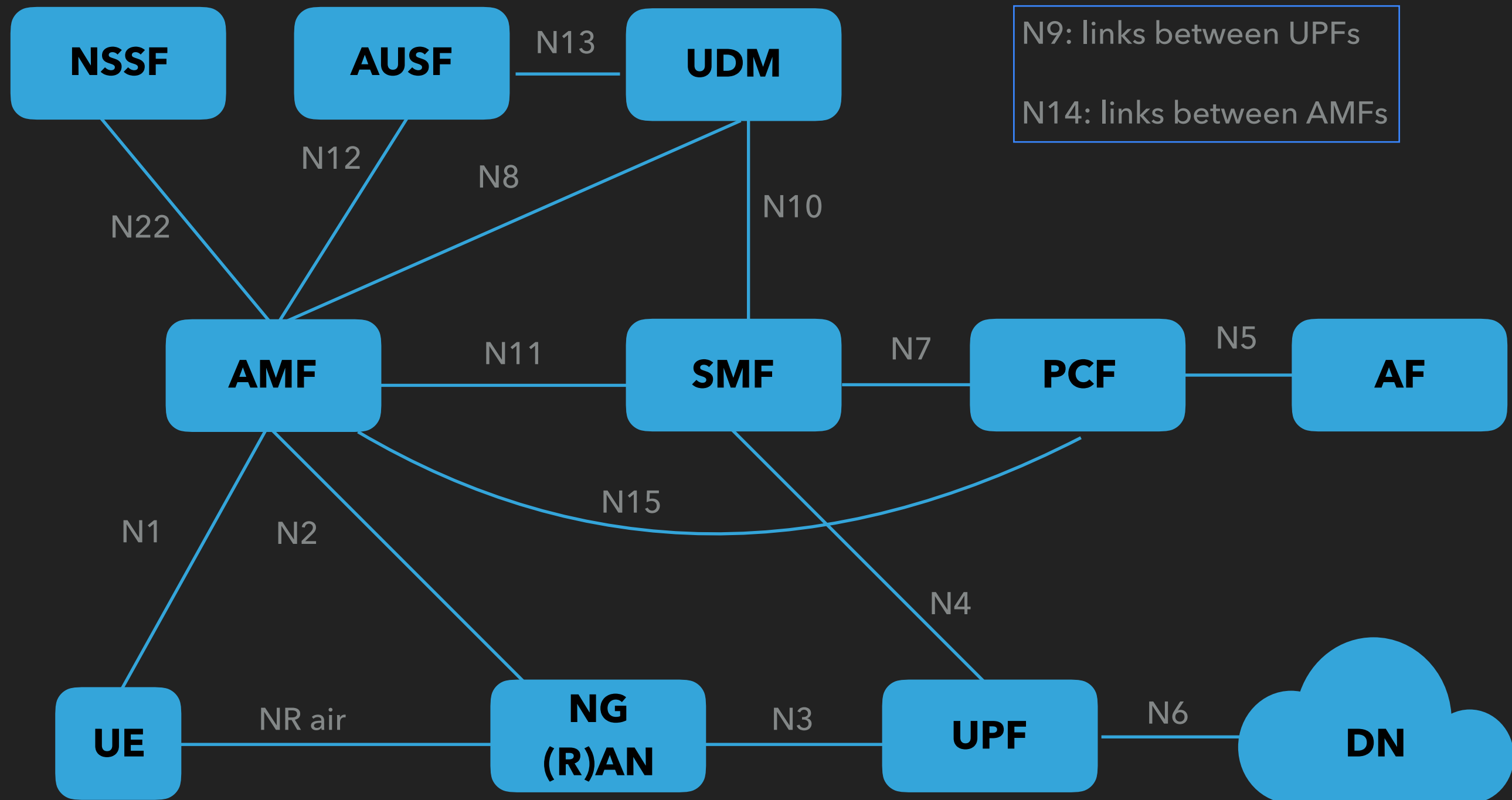
My blog: <https://swithak.github.io/>

My Twitter: [@SwitHak](https://twitter.com/SwitHak)

5G SCHEMES & TERMINOLOGY

5G NETWORK ARCHITECTURE REPRESENTATION

5



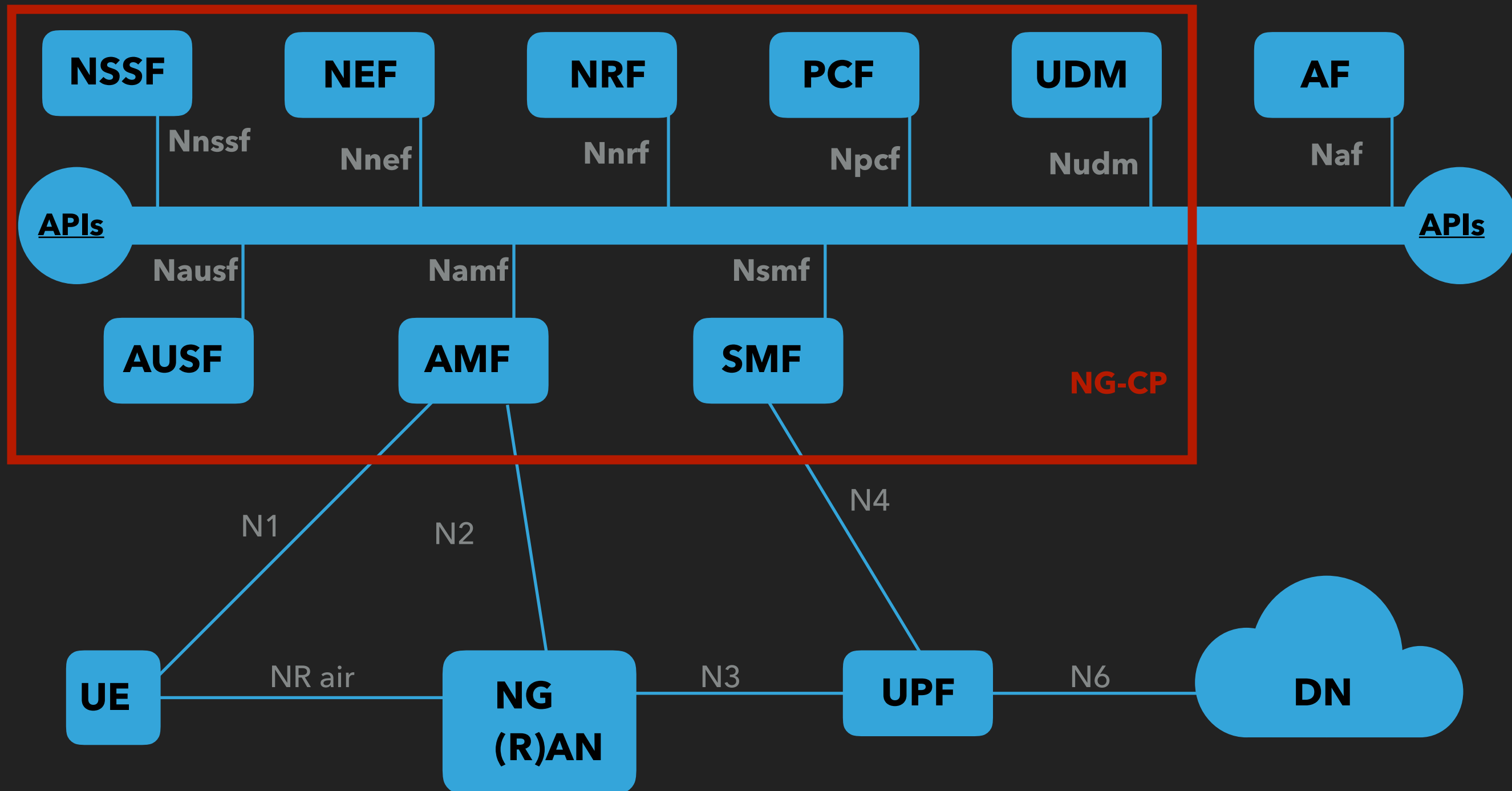
- N1: Reference point between the UE and the AMF.
- N2: Reference point between the (R)AN and the AMF.
- N3: Reference point between the (R)AN and the UPF.
- N4: Reference point between the SMF and the UPF.
- N5: Reference point between the PCF and an AF.
- N6: Reference point between the UPF and a Data Network.
- N7: Reference point between the SMF and the PCF.
- N8: Reference point between the UDM and the AMF.
- N9: Reference point between two UPFs.
- N10: Reference point between the UDM and the SMF.
- N11: Reference point between the AMF and the SMF.
- N12: Reference point between AMF and AUSF.
- N13: Reference point between the UDM and Authentication Server function the AUSF.
- N14: Reference point between two AMFs.
- N15: Reference point between the PCF and the AMF in the case of non-roaming scenario, PCF in the visited network and AMF in the case of roaming scenario.

- N16: Reference point between two SMFs, (in roaming case between SMF in the visited network and the SMF in the home network).
- N16a: Reference point between SMF and I-SMF.
- N17: Reference point between AMF and 5G-EIR.
- N18: Reference point between any NF and UDSF.
- N19: Reference point between two PSA UPFs for 5G LAN-type service.
- N22: Reference point between AMF and NSSF.
- N23: Reference point between PCF and NWDAF.
- N24: Reference point between the PCF in the visited network and the PCF in the home network.
- N27: Reference point between NRF in the visited network and the NRF in the home network.
- N28: Reference point between PCF and CHF.
- N29: Reference point between NEF and SMF.
- N29i: Reference point between I-NEF and SMF in the VPLMN.
- N30: Reference point between PCF and NEF.
- N31: Reference point between the NSSF in the visited network and the NSSF in the home network.
- N32: Reference point between SEPP in the visited network and the SEPP in the home network.

- N33: Reference point between NEF and AF.
- N34: Reference point between NSSF and NWDAF.
- N35: Reference point between UDM and UDR.
- N36: Reference point between PCF and UDR.
- N37: Reference point between NEF and UDR.
- N38: Reference point between I-SMFs.
- N40: Reference point between SMF and the CHF.
- ***N41-N49: The reference points from N40 up to and including N49 are reserved for allocation and definition in TS 23.503 [45].***
- N50: Reference point between AMF and the CBCF.
- N51: Reference point between AMF and NEF.
- N51i: Reference point between I-NEF and the AMF in the VPLMN.
- N52: Reference point between NEF and UDM.
- N53: Reference point between the I-NEF and the NEF.
- N55: Reference point between AMF and the UCMF.
- N56: Reference point between NEF and the UCMF.
- N57: Reference point between AF and the UCMF.
- N58: Reference point between AF and the NEF.

5G SERVICE BASED ARCHITECTURE

9

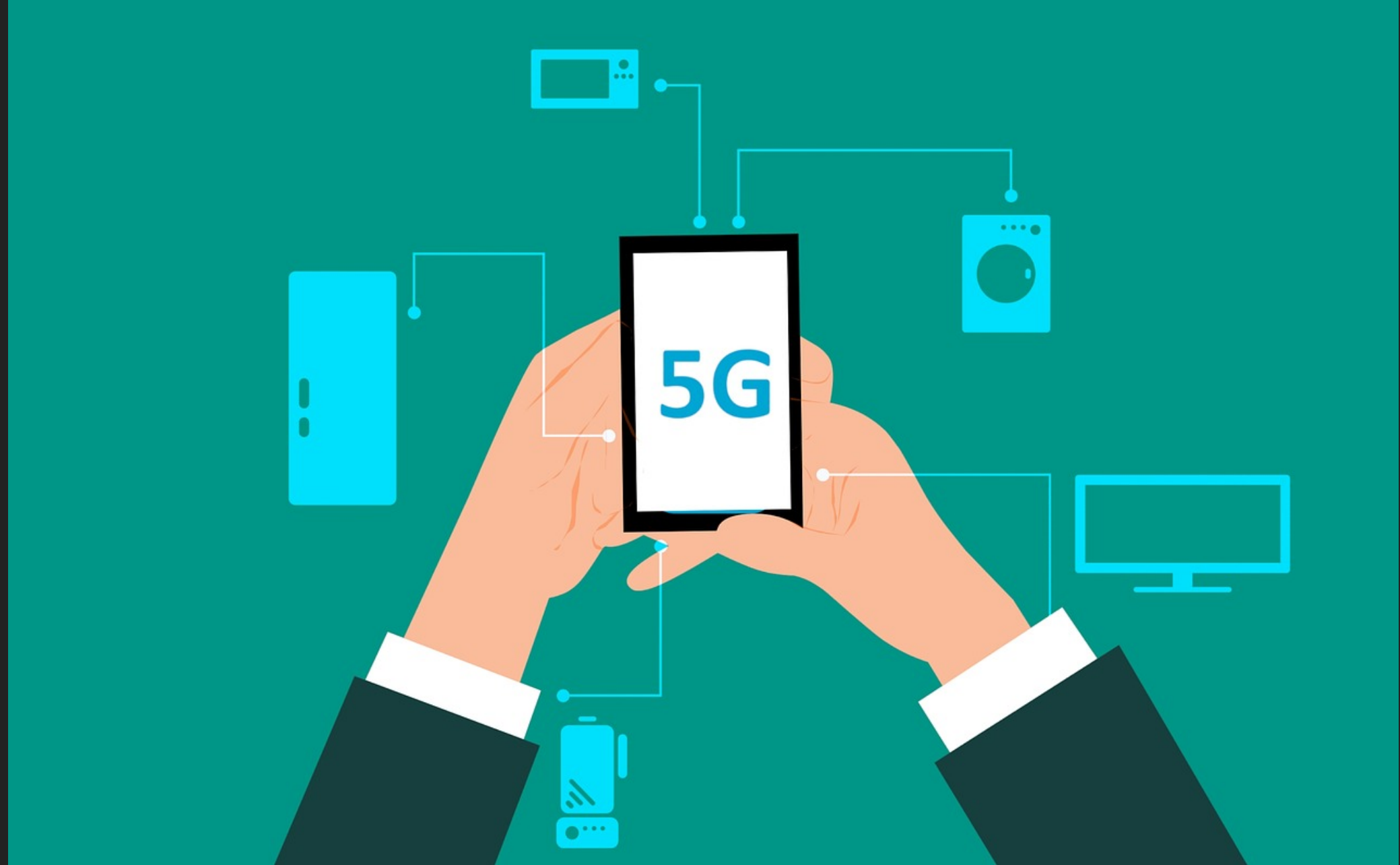


- ▶ Namf: Service-based interface exhibited by AMF.
- ▶ Nsmf: Service-based interface exhibited by SMF.
- ▶ Nnef: Service-based interface exhibited by NEF.
- ▶ Npcf: Service-based interface exhibited by PCF.
- ▶ Nudm: Service-based interface exhibited by UDM.
- ▶ Naf: Service-based interface exhibited by AF.
- ▶ Nnrf: Service-based interface exhibited by NRF.
- ▶ Nnssf: Service-based interface exhibited by NSSF.
- ▶ Nausf: Service-based interface exhibited by AUSF.
- ▶ Nudr: Service-based interface exhibited by UDR.
- ▶ Nudsf: Service-based interface exhibited by UDSF.
- ▶ N5g-eir: Service-based interface exhibited by 5G-EIR.
- ▶ Nnwdaf: Service-based interface exhibited by NWDAF.
- ▶ Ni-nef: Service-based interface exhibited by I-NEF.
- ▶ Nchf: Service-based interface exhibited by CHF.
- ▶ Nucmf: Service-based interface exhibited by UCMF.

- ▶ Authentication Server Function (AUSF)
- ▶ Access and Mobility Management Function (AMF)
- ▶ Data Network (DN), e.g. operator services, Internet access or 3rd party services
- ▶ Unstructured Data Storage Function (UDSF)
- ▶ Network Exposure Function (NEF)
- ▶ Network Repository Function (NRF)
- ▶ Network Slice Selection Function (NSSF)
- ▶ Policy Control Function (PCF)
- ▶ Session Management Function (SMF)
- ▶ Unified Data Management (UDM)
- ▶ Unified Data Repository (UDR)
- ▶ User Plane Function (UPF)
- ▶ UE radio Capability Management Function (UCMF)
- ▶ Application Function (AF)
- ▶ User Equipment (UE)
- ▶ (Radio) Access Network ((R)AN)
- ▶ 5G-Equipment Identity Register (5G-EIR)
- ▶ Network Data Analytics Function (NWDAF)
- ▶ CHarging Function (CHF)
- ▶ Service Communication Proxy (SCP)
- ▶ Security Edge Protection Proxy (SEPP)
- ▶ Non-3GPP InterWorking Function (N3IWF)
- ▶ Trusted Non-3GPP Gateway Function (TNGF)
- ▶ Wireline Access Gateway Function (W-AGF)

- ▶ Latest terminology available: 3GPP TS 23.501 V16.2.0 (2019-09)





**5G ISN'T AN EVOLUTION. IT'S MULTIPLE
TECHNOLOGICAL REVOLUTIONS**



**Millimeter
Waves**



Small Cell



**Massive
MIMO**



Beamforming



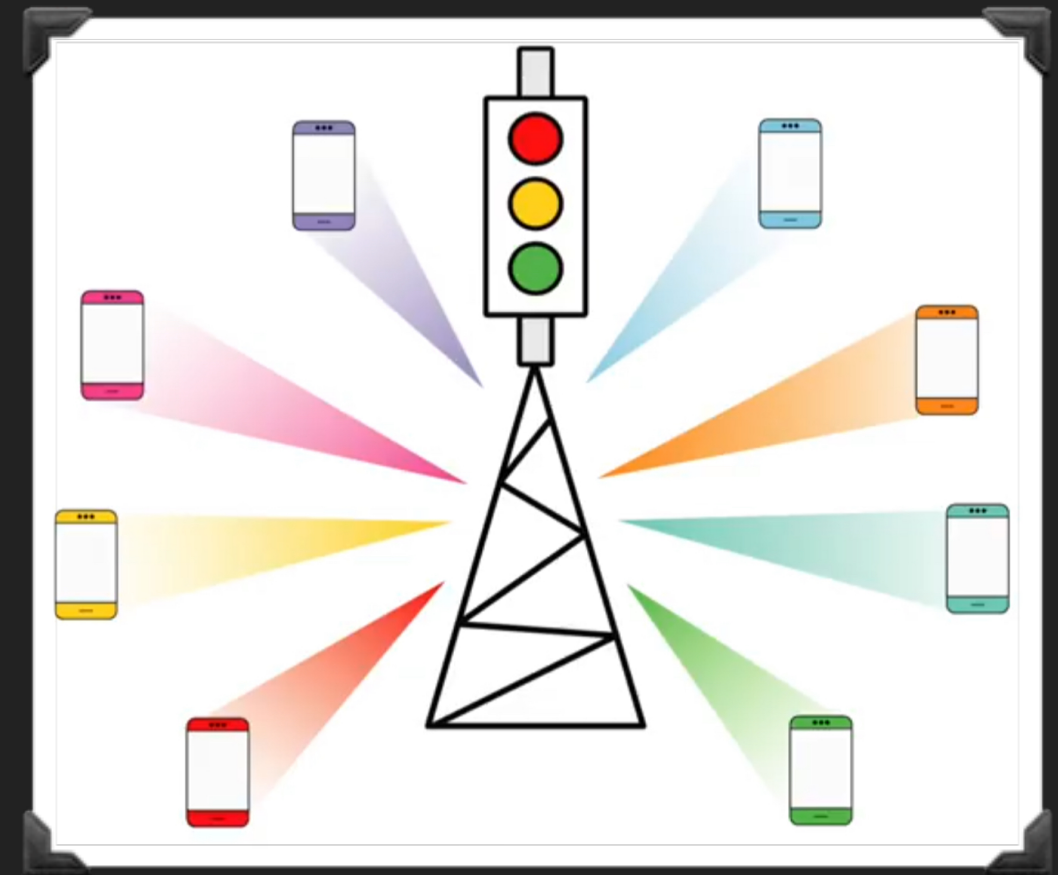
Full Duplex

- ▶ Millimeters waves (mmW):
 - ▶ 6GHz to 300GHz
 - ▶ Less penetration in building or any obstacles
 - ▶ Absorbed by plants and rain
 - ▶ Need more antennas to cover the same area than 4G

- ▶ Small cells:
 - ▶ 1 high powered BTS signals will be repeated by low powered mini-BTS to the UEs
 - ▶ More mini-BTS will allow a better handover coverage
 - ▶ Creates a new sub zone in the Access Network area

- ▶ Massive Multiple Input, Multiple Output (Massive-MIMO)
 - ▶ Increased Network Capacity – Network Capacity is defined as the total data volume that can be served to a user and the maximum number of users that can be served with certain level of expected service.
 - ▶ Improved Coverage – With massive MIMO, users enjoy a more uniform experience across the network, even at the cell's edge – so users can expect high data rate service almost everywhere.
 - ▶ User experience – Ultimately, the above two benefits result in a better overall user experience – users can transfer large data files or download movies, or use data-hungry apps on the go, wherever life takes them.

- ▶ Beam-forming & 3D beam-forming
 - ▶ Beam-forming focuses a wireless signal in a specific direction, rather than broadcasting to a wide area.
 - ▶ 3D Beam-forming creates horizontal and vertical beams toward users.
 - ▶ With algorithms in the BTS to optimize the beams traffic.



- ▶ Full Duplex
 - ▶ 4G
 - ▶ Emits and receive with a delay
 - ▶ 5G enables the possibility on the same frequency to emits and receive in the same time due to fast switches innovation, permitting the reduction of latency.

- ▶ Good news for law enforcement forces & urgencies services, no more congestion problems for critical communications
- ▶ Good news , Quality of Service come too
- ▶ Bad news , we can discriminate the access to bandwidth (sweet dreams for Networks Operators comes to reality)



LAW ENFORCEMENT & LAWFUL INTERCEPTION CAPABILITIES UNDER 5G

- ▶ Identification & localization of users:
 - ▶ IMSI (International Mobile Subscriber Identity) Numbers will be encrypted
 - ▶ IMSI Catchers will be detectable due to false-base new 5G functionality

- ▶ Network slicing:
 - ▶ Network slicing will maximize the flexibility of 5G networks, optimizing both the utilization of the infrastructure and the allocation of resources.
 - ▶ Multiple networks operators sharing the same equipment
 - ▶ Not all of them will be public home networks operators, some will be private and other can be abroad ones (Public, Private & Third Party)
 - ▶ Third party? Yes!
 - ▶ Maybe new regulations will be needed to address the problem

- ▶ Multi-access Edge Computing (MEC):
 - ▶ MEC will allow mobile phone networks to store and process contents in the vicinity of "cellular network participants" in order to achieve faster response times (LATENCY).
 - ▶ Communication content and identifiers no longer have to be directed through CORE NETWORK
 - ▶ will impede the LI capabilities

- ▶ End-To-End encryption (E2E encryption):
 - ▶ Not a mandatory thing (currently), just in the specs
 - ▶ Protocols are included into the draft 16
 - ▶ There's a strong discussion around this subject

- ▶ Network Functions Virtualization (NFV)
 - ▶ Lots of virtualization in 5G architecture
 - ▶ Even for the Lawful Interception functions
 - ▶ Means new possibilities of targeting the LI functions and recover the POI list (Persons of Interest)

- ▶ Law enforcement underrepresented / underestimated the discussion about 5G standards
 - ▶ Late considerations of 5G standards
 - ▶ Underrepresented in 3GPP
 - ▶ But they can count on regulatory powers

5G WARS

**5G WARS, U.S., HUAWEI & ZTE, NOKIA &
ERICSSON ...**




CONTENDERS FOR THE 5G BATTLE

29



- ▶ U.S. threatened its allies to cut off intelligence feeds if they choose Huawei 5G equipments
- ▶ U.S. lobbying against Huawei is a new war
- ▶ U.S. is really concerned with Huawei as they were with ZTE earlier

- ▶ Chinese companies considered by U.S. and others to be an extension of Chinese Intelligence services
- ▶ Sovereignty is vulnerable due to legal framework in China
 - ▶ Article 7 of the *National Intelligence Law of the People's Republic* : Any organization or citizen shall support, assist and cooperate with the state intelligence work in accordance with the law, and keep the secrets of the national intelligence work known to the public. The State protects individuals and organizations that support, assist and cooperate with national intelligence work.
- ▶ Chinese Intelligence is already really good in telecommunications intercepts
 - ▶ Interceptions attacks
 - ▶ Monitoring ethnic groups...
 - ▶ Lots of cases, we can make a full day of conference on the subject

- ▶ Two companies weakened companies
- ▶ 5G market is their future
- ▶ European Union 
- ▶ But...
 - ▶ Lots of Chinese engineers whose have family members in China 
 - ▶ Nokia 5G investments are almost all loans from EU banks 
- ▶ An Ericsson & Nokia government preference can happen in a nearly future

FRANCE



- ▶ Legal framework redefined recently by the “LOI n° 2019-810 du 1er août 2019 visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles”

National 5G Roadmap

- **January 2018** Creation of the “5G pilot” window
- **July 2018** Publication of a 5G roadmap for France and of Arcep’s Work Programme
- **October 2018** Public consultation on spectrum allocations
- **January 2019** Call for 26 GHz band trial platforms
- **1^{er} H 2019** Arcep’s dialogue with local authority associations, verticals, operators
- **May 2019** Government targets set
- **Summer 2019** Public consultation on the call for applications for 3.4 – 3.8 GHz band licences in Metropolitan France
- **Autumn 2019** Launch of the frequency allocation procedure
- **2020** Frequencies allocated, first rollouts and commercial launches

- ▶ Iliad (Free) signed an exclusive agreement with Nokia
 - ▶ https://www.iliad.fr/presse/2019/CP_020919_Eng.pdf
- ▶ Orange is likely to use European suppliers
 - ▶ lots of partnerships with Ericsson recently
 - ▶ Testing have been done with Huawei too
- ▶ Bouygues Telecom is likely to choose Huawei
 - ▶ Already have Huawei technology in 4G networks
- ▶ SFR is very likely to choose Huawei or Nokia
 - ▶ Already have Huawei technology in 4G networks
 - ▶ <https://www.sfrbusiness.fr/room/internet-et-reseaux/tout-savoir-reseau-5g.html>



5G SECURITY (OLD & NEW THREATS)

THREATS TO 5G SECURITY

- ▶ Data interception
- ▶ User impersonation
- ▶ Denial of Service
- ▶ Asset compromise
- ▶ Misconfigurations
- ▶ Virtualization vulnerabilities
- ▶ API exposures
- ▶ Bad implementations (voluntarily)
- ▶ Theft of resources

USER EQUIPMENT (UE) THREATS

▶ Mobile to Infrastructure

- ▶ Botnet coordinated attack against 5G infrastructure to affect the 5G services confidentiality, integrity & availability.

▶ Mobile to Mobile

- ▶ Attacker UE's attack others UE to install malware

▶ Internet to Mobile

- ▶ Malicious attacks against UE from Internet (malicious app, targeted attacks, ...)

▶ Mobile to Internet

- ▶ Using UE 5G connectivity to DDoS website

RADIO ACCESS NETWORK (RAN) THREATS

- ▶ **Rogue Base Station (RBS)**
 - ▶ Exists since the firsts GSM networks
 - ▶ Expected to be more difficult to do under 5G with the False Base Detection functionality

CORE NETWORK (CN) THREATS

▶ DoS/DDoS against critical 5G functions:

- ▶ Access and Mobility Management Function (AMF); stopping handling the mobility services (handover)
- ▶ Authentication Server Function (AUSF); stopping the UE authentication services
- ▶ Unified Data Management (UDM); stopping subscription services

▶ Protocol vulnerabilities:

- ▶ HTTP/2
- ▶ TCP/IP SACK
- ▶ URGENT/11
- ▶ ...

SDN / NFV THREATS

- ▶ **Software Defined Networks (SDN)**
 - ▶ Vulnerabilities in the SDN software
- ▶ **Network Function Virtualization (NFV)**
 - ▶ Virtualization threats
 - ▶ Virtual machines segregation
 - ▶ Containers isolation
 - ▶ Insecure access control

NETWORK SLICING THREATS

- ▶ **Inter-Slice isolation**

- ▶ Communications between SliceA & SliceB

- ▶ **Intra-Slice isolation**

- ▶ Communications between SliceFunctionA & SliceFunctionB

- ▶ **Side channel attack**

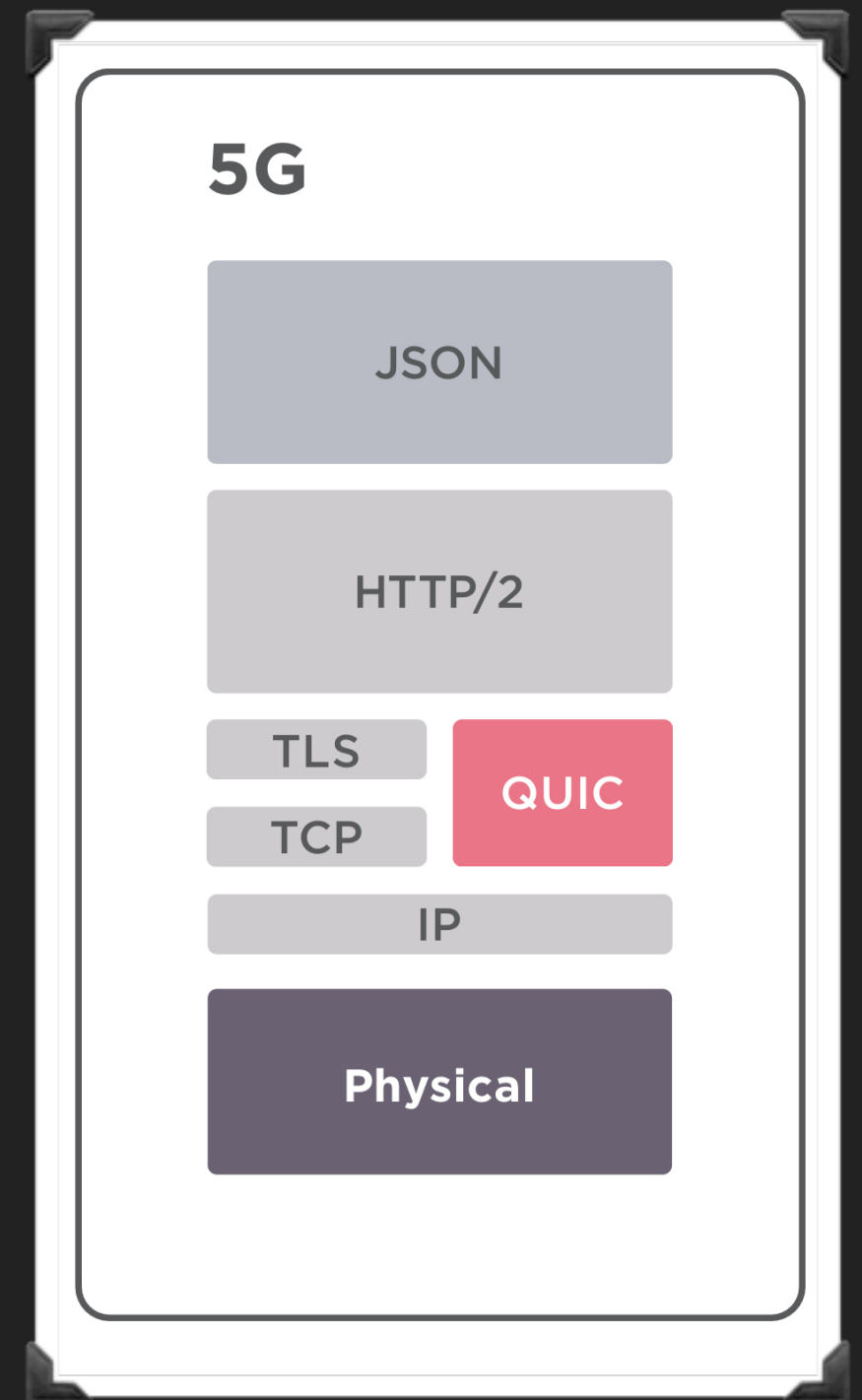
- ▶ leak information (Custom Details Records, ...)

- ▶ **Destruction attack**

- ▶ Gains access to one slices manager, instructed it to destroy all slices

5G PROTOCOLS

- ▶ Signaling / Control: HTTP/2
- ▶ Data / User: GTP-over-IPSec
- ▶ Core Network: TCP/IP
- ▶ RAN: SCTP
- ▶ QUIC: Quick UDP Internet Connections
- ▶ Applications will be in JSON

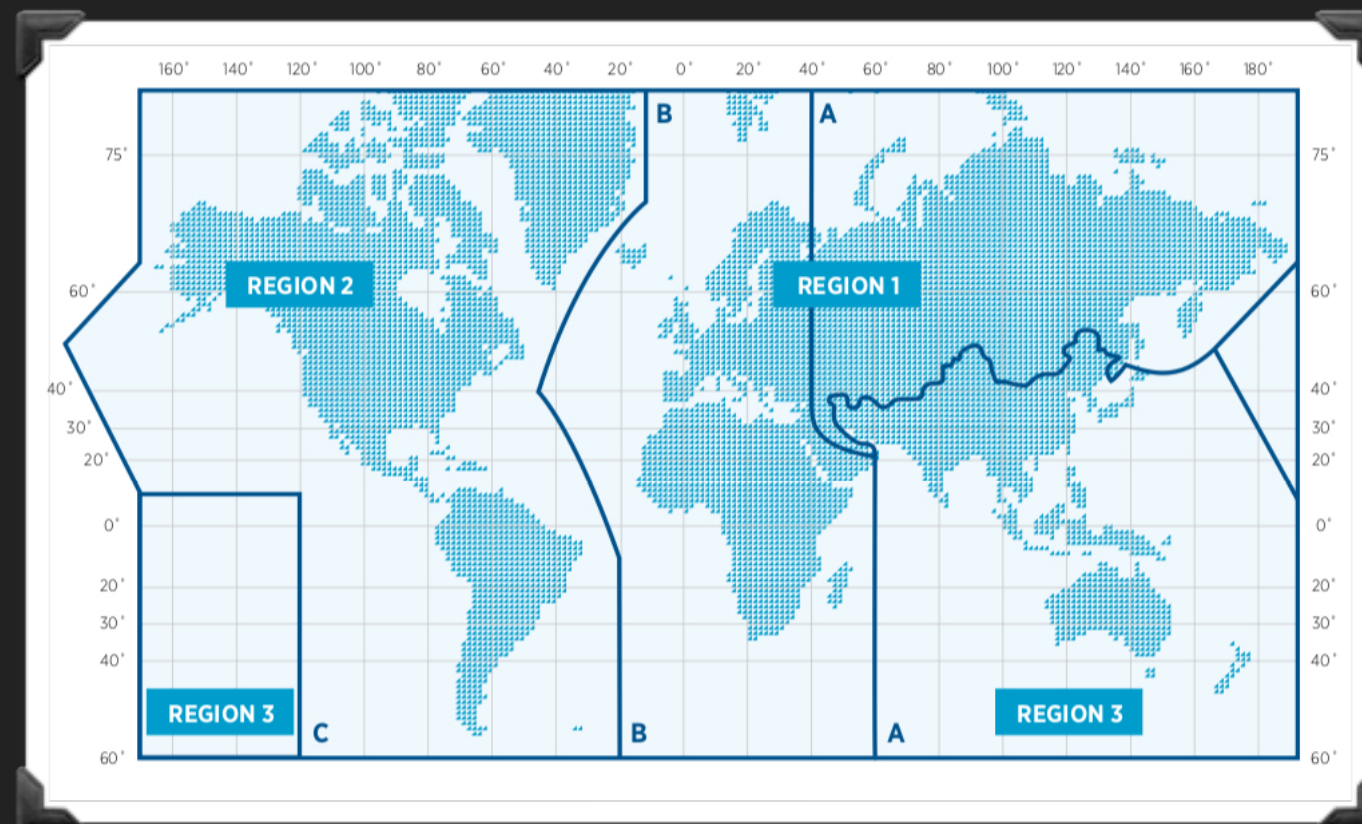


4G TO 5G TRANSITION

- ▶ During the transition, the 5G equipments will not use the 5G core because it will not be available immediately.
- ▶ Instead they are going to use the 4G core, with all the 4G core vulnerabilities

FREQUENCIES ATTRIBUTIONS AND DISPUTES

- ▶ **3.3-3.4 GHz** : A majority of Africa, some countries in Regions 2 and 3
- ▶ **3.4-3.6 GHz** : Region 1, Region 2 and large parts of Region 3
- ▶ **3.6-3.7 GHz** : Some countries in Region 2. Some countries in Region 3 (including Australia, Korea, Japan, New Zealand) have also indicated interest.
- ▶ **3.6-3.8 GHz** : Harmonized for mobile broadband use throughout the European Union by European Decision. GCC countries have also indicated interest.



INTERNATIONAL MOBILE TELECOMMUNICATIONS (IMT) POSSIBLE FREQUENCIES (ITU AGENDA ITEM 1.13)

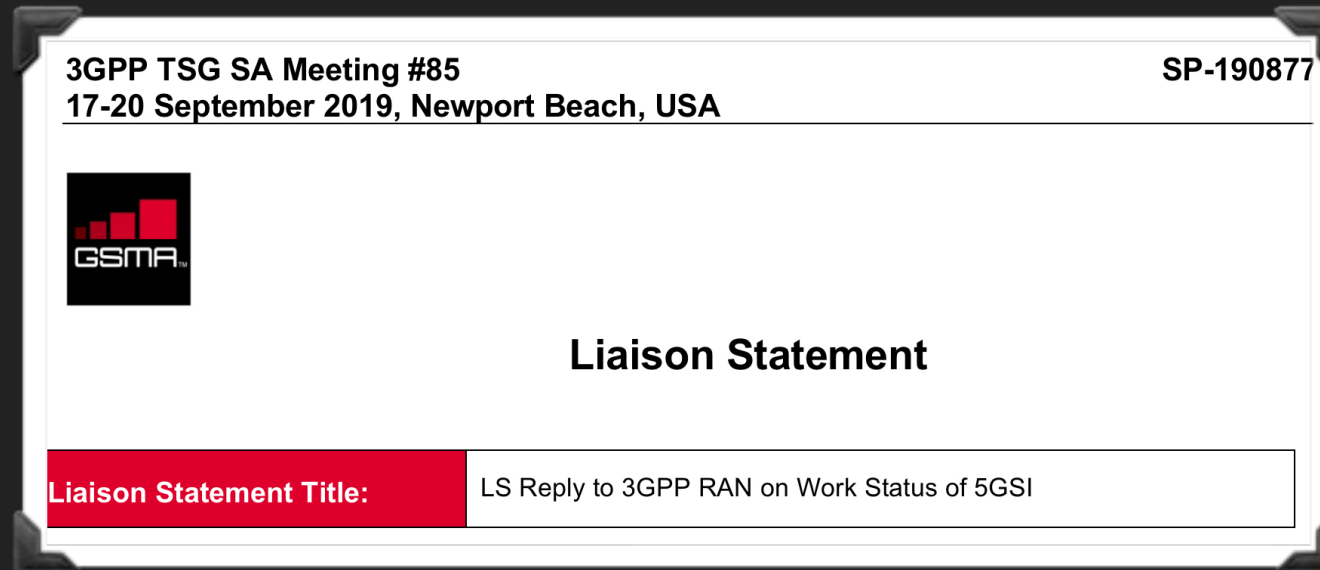
48

- ▶ **24.25-27.5 GHz**
- ▶ 31.8-33.4 GHz
- ▶ **37-43.5 GHz**
- ▶ **45.5-50.2 GHz**
- ▶ **50.4-52.6 GHz**
- ▶ **66-71 GHz**
- ▶ 71-76 GHz
- ▶ 81-86 GHz

Legend:

- **GSMA Strong support**
- **GSMA Medium support**

5G OR FAKEG?



State	UE Indicator
1 (IDLE under or Connected to LTE cell not supporting NSA)	4G
2 (IDLE under or Connected to LTE cell supporting NSA and no detection of NR coverage)	5G
3 (Connected to LTE only under LTE cell supporting NSA and detection of NR coverage)	5G
4 (IDLE under LTE cell supporting NSA and detection of NR coverage)	5G
5 (Connected to LTE + NR under LTE cell supporting NSA)	5G

ANY QUESTION?

**THANKS FOR
YOUR ATTENTION.**

- ▶ 3GPP TS 23.501 V16.2.0 (2019-09)
- ▶ 5G PPP Architecture Working Group View on 5G Architecture, Version 3.0, June 2019
- ▶ 5G; Security architecture and procedures for 5G System (3GPP TS 33.501 version 15.5.0 Release 15)
- ▶ 5G security issues by Positive Technology, 2019
- ▶ KEY DRIVERS AND RESEARCH CHALLENGES FOR 6G UBIQUITOUS WIRELESS INTELLIGENCE, 6G Research Visions 1 September 2019
- ▶ The evolution of Security in 5G by 5G Americas
- ▶ Report of the CPM on technical, operational and regulatory/procedural matters to be considered by the World Radiocommunication Conference 2019, ITU
- ▶ Security of 5G networks: EU Member States complete national risk assessments, Brussels, 19 July 2019
- ▶ Position paper on 5G by Europol
- ▶ Signaling Security in Telecom SS7/Diameter/5G EU level assessment of the current situation by ENISA
- ▶ THE 5G ECOSYSTEM: RISKS & OPPORTUNITIES FOR DoD DEFENSE INNOVATION BOARD April 2019
- ▶ DEFENDING OUR DATA: HUAWEI, 5G AND THE FIVE EYES BY BOB SEELY MP, DR PETER VARNISH OBE & DR JOHN HEMMINGS, HJS
- ▶ Law enforcement and judicial aspects related to 5G, Council of European Union
- ▶ L'Europe et la 5G : le cas Huawei, Institut Montaigne
- ▶ Finite State Supply Chain Assessment: Huawei Technologies Co., Ltd.
- ▶ Executive Order on Securing the Information and Communications Technology and Services Supply Chain, WhiteHouse USA
- ▶ Huawei, 5G and China as a Security Threat by Kadri Kaska, Henrik Beckvard and Tomáš Minárik, CCDCOE
- ▶ HUAWEI CYBER SECURITY EVALUATION CENTRE (HCSEC) OVERSIGHT BOARD, ANNUAL REPORT 2019