RSAConference2020
San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: MBS-W11

Demystifying 5G Security Through Threat Modeling

Zhijun (William) Zhang

Lead Security Architect
The World Bank Group
@zwilliamz

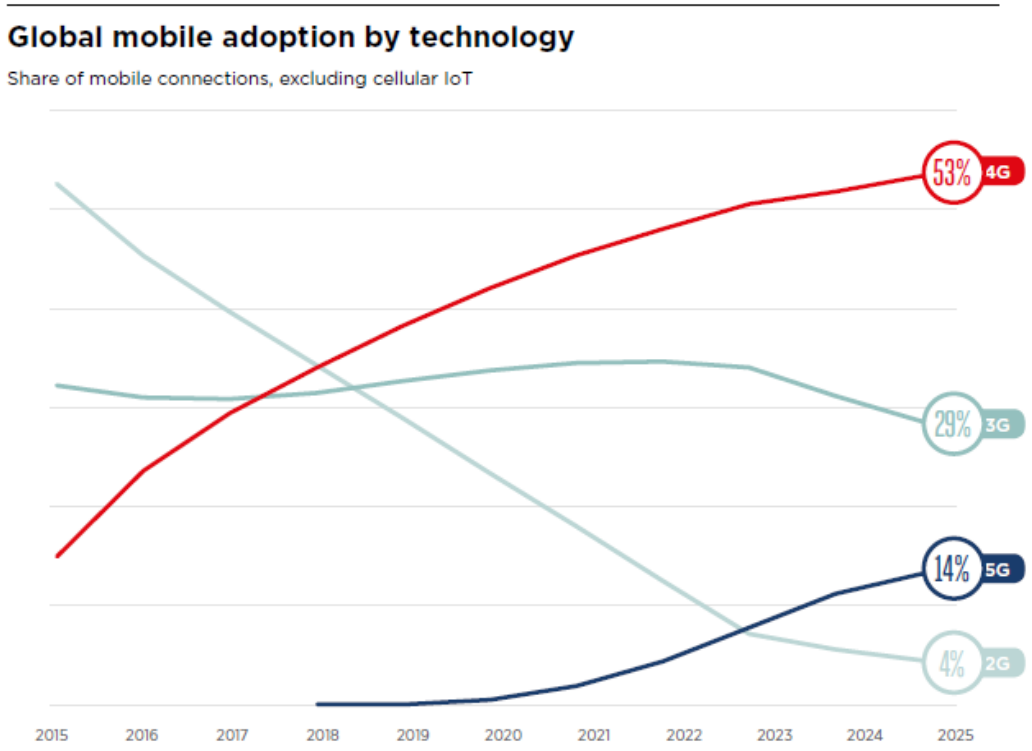
What is 5G ?

- *Officially named as IMT-2020*
  - International Mobile Telecommunications (standards by ITU)

- *Provides far more enhanced capabilities than IMT-2000(3G) and beyond IMT-Advanced(4G)*
  - 4G is called LTE, Long Term Evolution
  - 5G, or IMT-2020, is called NR, New Radio

Generations of Mobile Technologies

Generation (name)	Availability	Characteristics	Speed
1G	1980	Analog, Voice only	14.4kbps
2G	1990	Digital, Data along Voice, MMS, Web browsing	56-115 kbps
3G (IMT-2000)	2000	Video calling Wireless internet	5.8-14.4 mbps
4G (IMT-Advanced)	2012	HD streaming High speed wireless internet	100mbps-1gbps
5G (IMT-2020)	2020	New convergence services	20 gbps



(Source: GSMA 2018)

5G Features - Performance

	Minimum Requirements for 5G (IMT-2020)	Comparison to 4G (IMT-Advanced)
Peak data transmission rate	Downlink peak data rate: 20 Gbps	20 times faster
Latency	1 millisecond, for ultra reliable communications	1/10 the latency of LTE
Connection density	1,000,000 devices per square kilometer	10 times the devices

5G Performance Brings in New Use Cases

High bandwidth, low latency

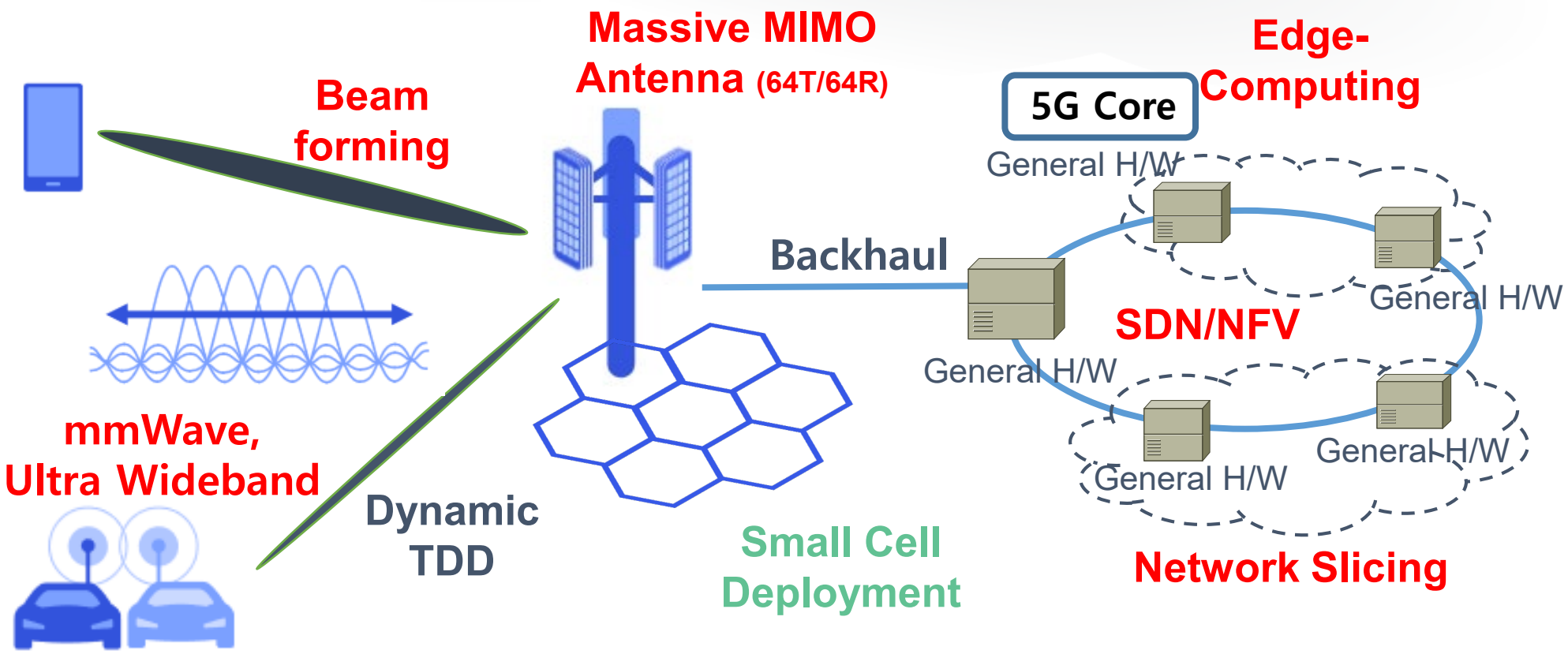
Highly reliable

✓ From “connecting people” to “connecting things”

✓ Real-time broadcasting F1 race with a driver’s view & experience

✓ Mission-critical services like autonomous vehicle & remote surgery

5G Features – Technology Revolution

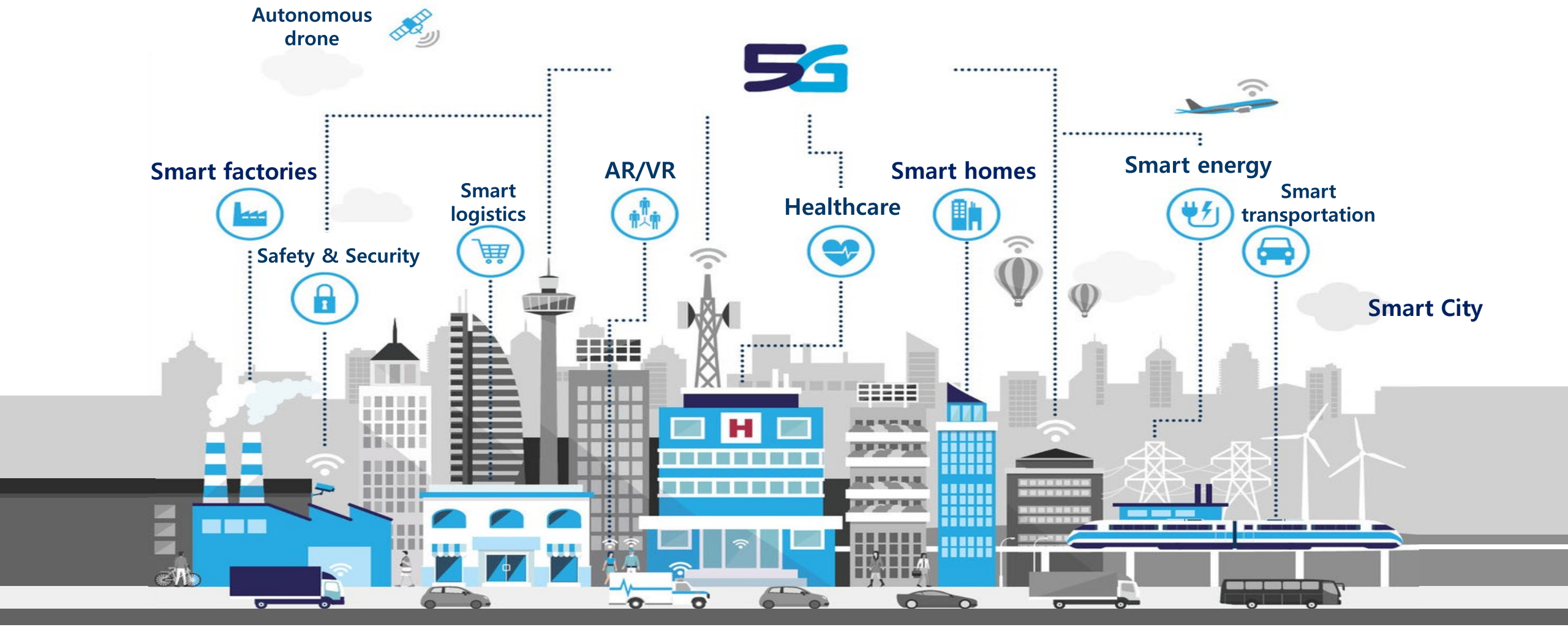


- mmWave (millimeter Wave, e.g. 24.25-27.5GHz, 27.5-29.5GHz)
- MIMO (Multiple Input, Multiple Output), TDD (Time Division Duplexing)
- SDN (Software Defined Network), NFV (Network Functions Virtualization)

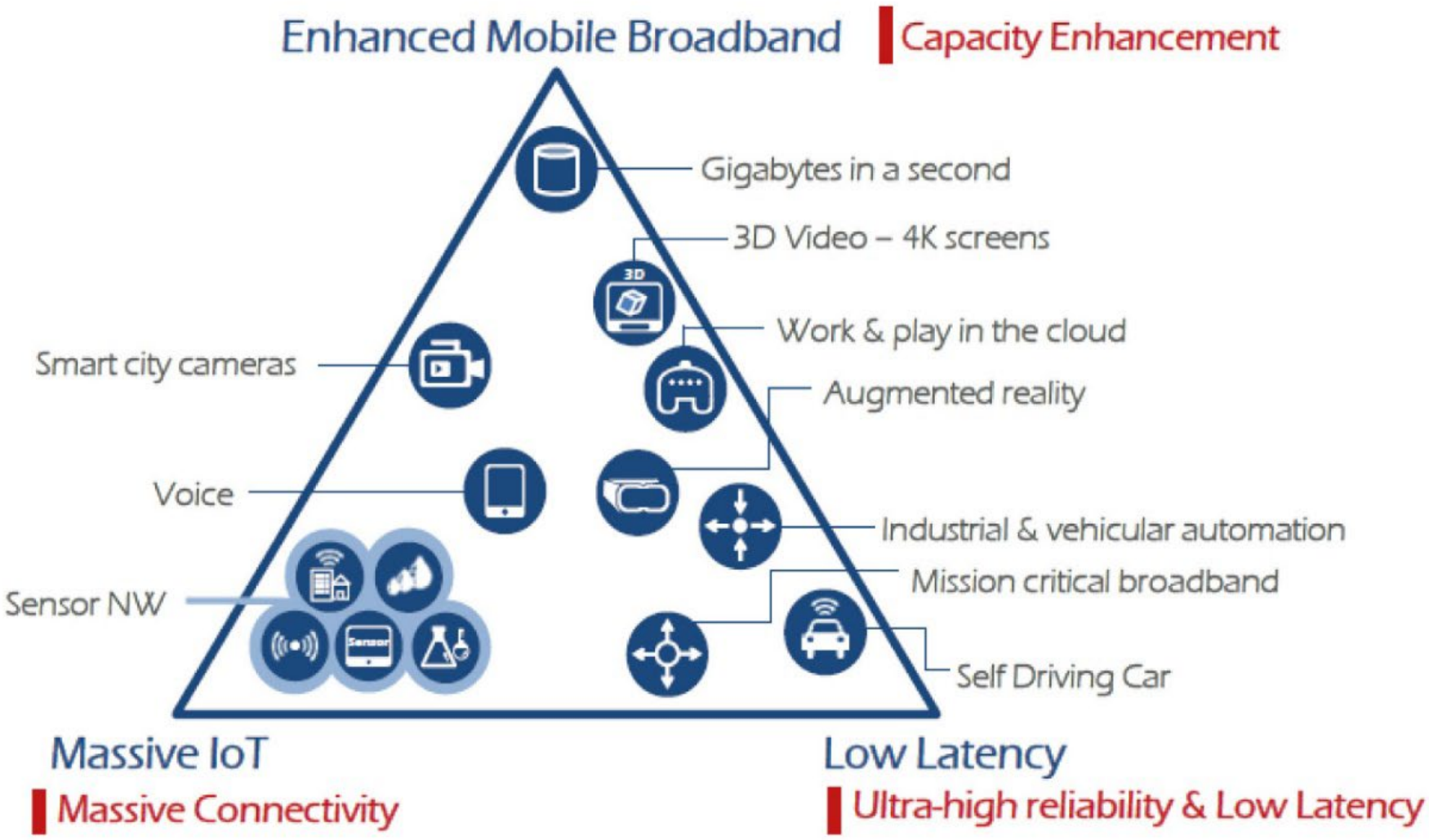
RSAConference2020

5G becomes an invisible infrastructure for all

5G-Enabled Economy



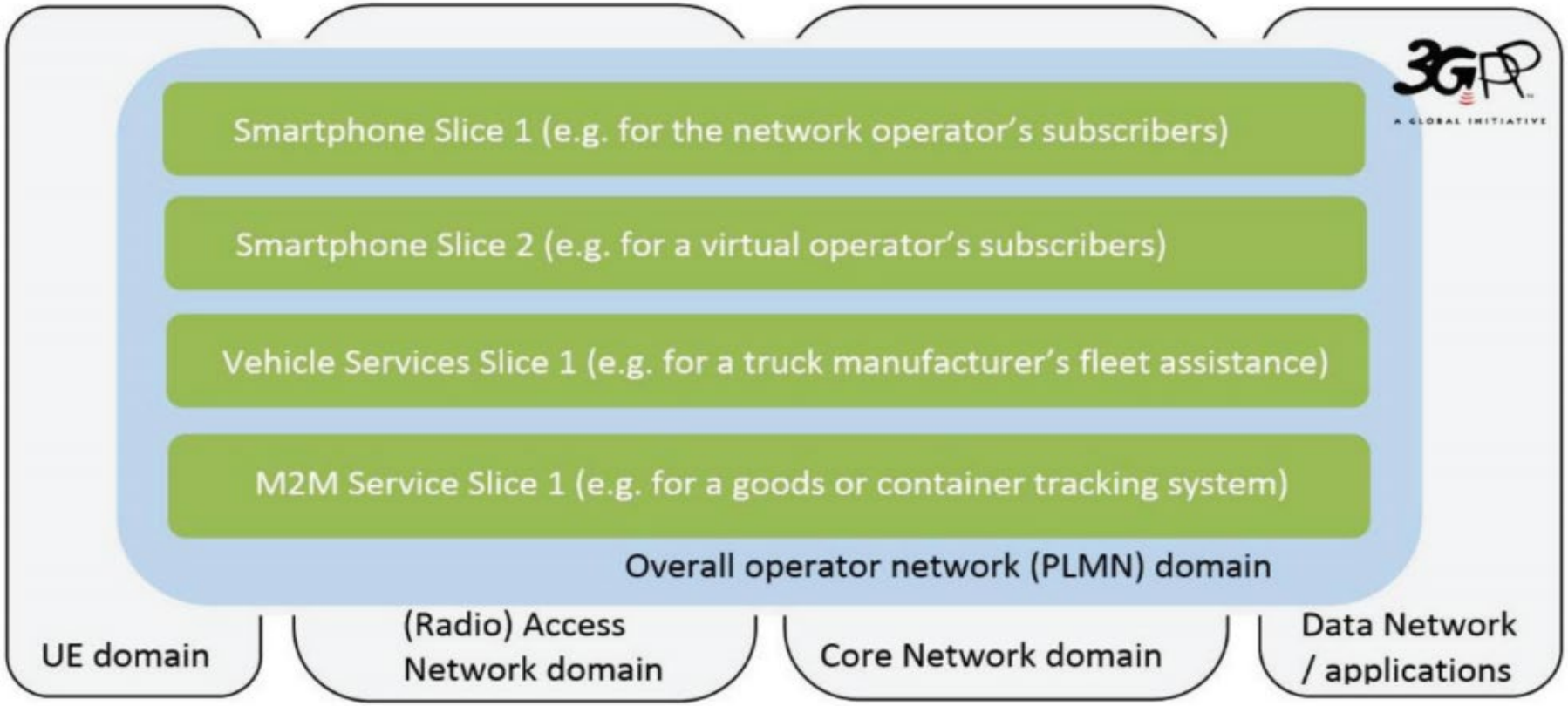
The 5G Vision



(Source: ITU-R IMT 2020)

Supported by Network Slicing and Virtualization

- Concurrent deployment of multiple logical networks on the same physical network infrastructure



RSAConference2020

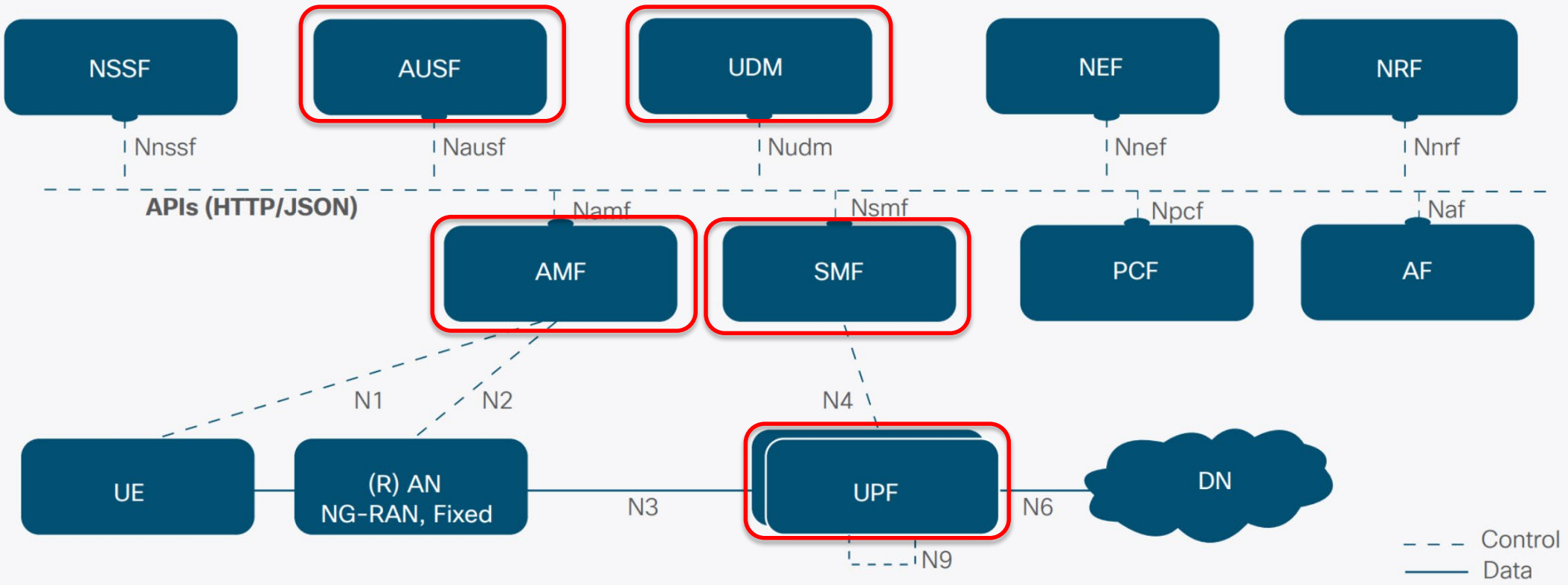
What about security?

5G Security – Radio Access Network

Components that connect mobile devices to the core network

- mmWave radio frequencies
  - Shorter wavelengths and narrower beams, which can provide better security for data transmission
- MIMO (multiple-input, multiple-output) and beamforming
  - More opportunities for masquerading
- Mutual authentication between devices and base stations
- Better protection of subscriber identity

5G Security – Core Network – Service-based Architecture



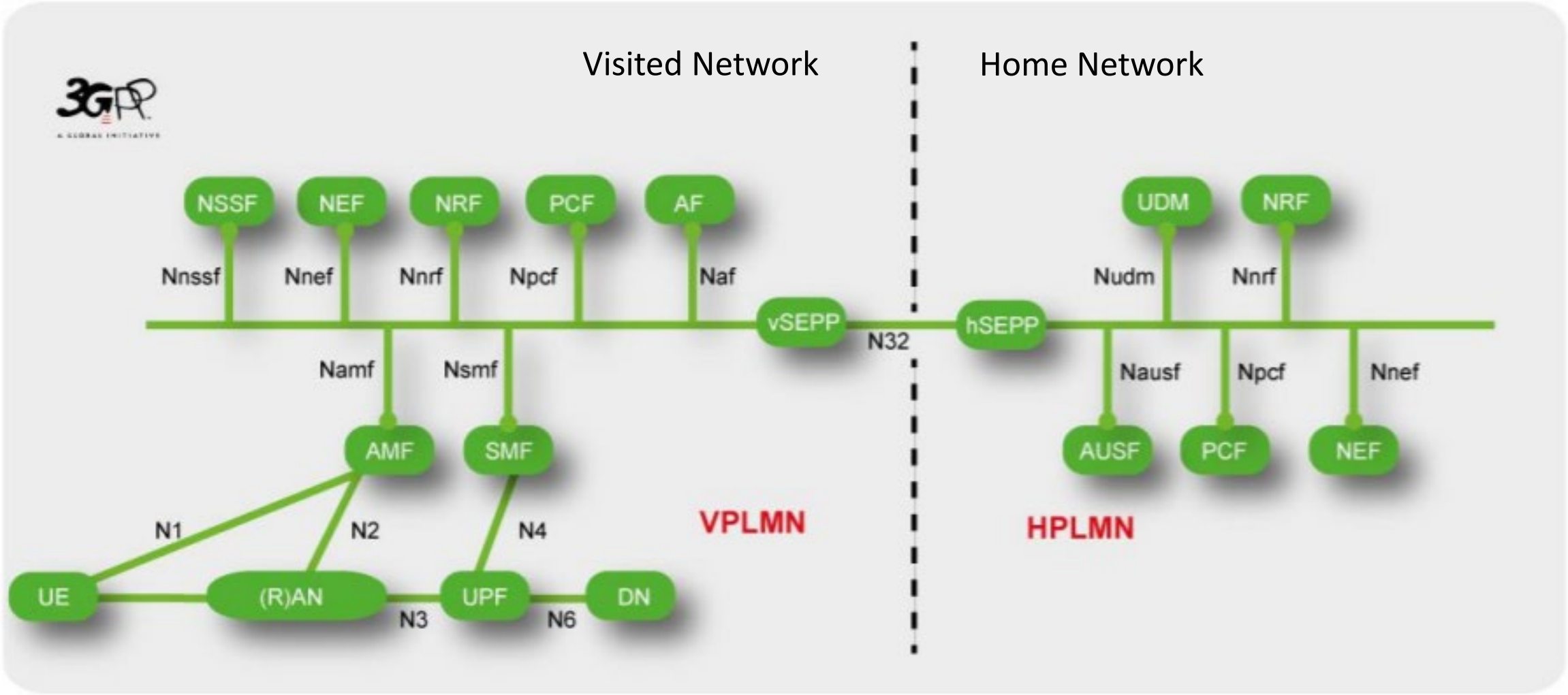
AUSF	Authentication Server Function
AMF	Access and Mobility Management Function
AF	Application Function
DN	Data Networks
SMF	Session Management Function
UDM	User Data Management

NEF	Network Exposure Function
NSSF	Network Slice Selection Function
NRF	Network Repository Function
PCF	Policy Control Function
UPF	User Plane Function
(R)AN	(Radio) Access Network

UE: User Equipment
N*: messages
NG: Next Generation

(Credit: Cisco)

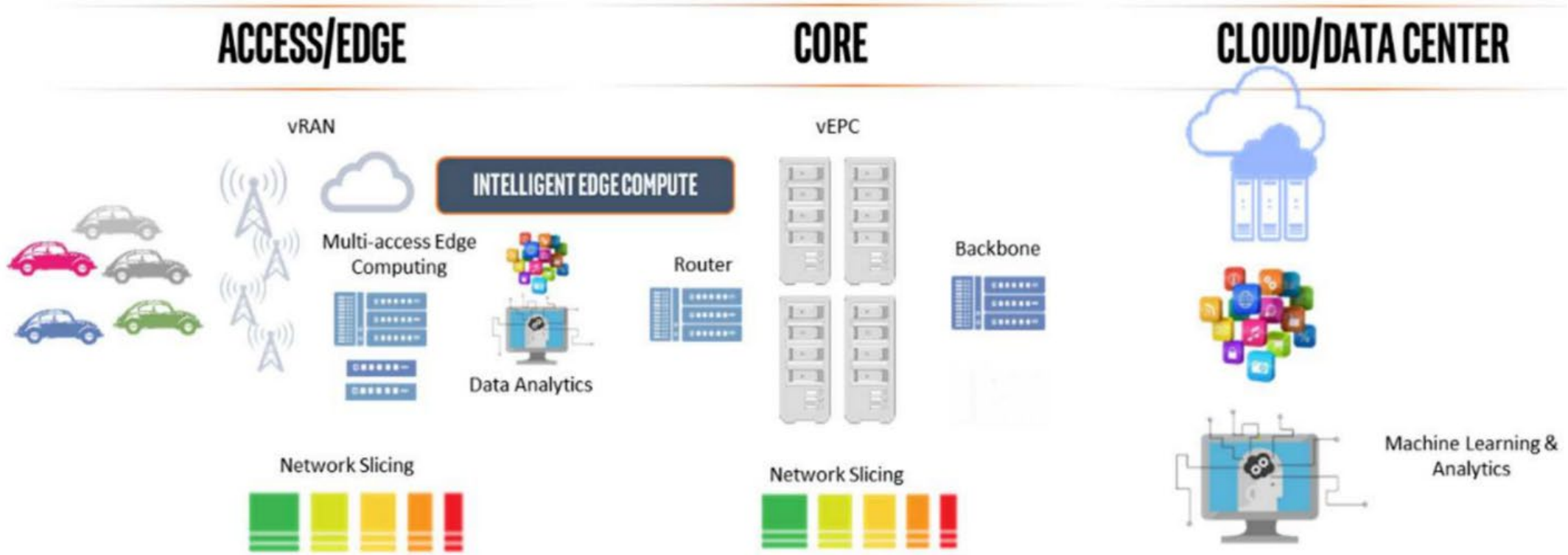
5G Security – Trust Model



SEPP: Security Edge Protection Proxy
PLMN: Public Land Mobile Network

5G Security – Multi-Access Edge Computing (MEC)

- Move application hosting from centralized data centers to the network edge (e.g. cellular base stations)



(Source: 5GAA)

WORLD BANK GROUP
Information and Technology Solutions

vRAN: virtual radio access network
vEPC: virtual evolved packet core

5G Security – Key Elements

1. Subscription Concealed Identifier (SUCI)
2. Updated Authentication and Key Agreement (AKA)
3. Stronger data integrity for radio access network
4. Stronger cryptographic algorithm
5. Stronger security for connectivity to other networks
6. Increased home network control
7. Detection of false base stations based on user equipment data

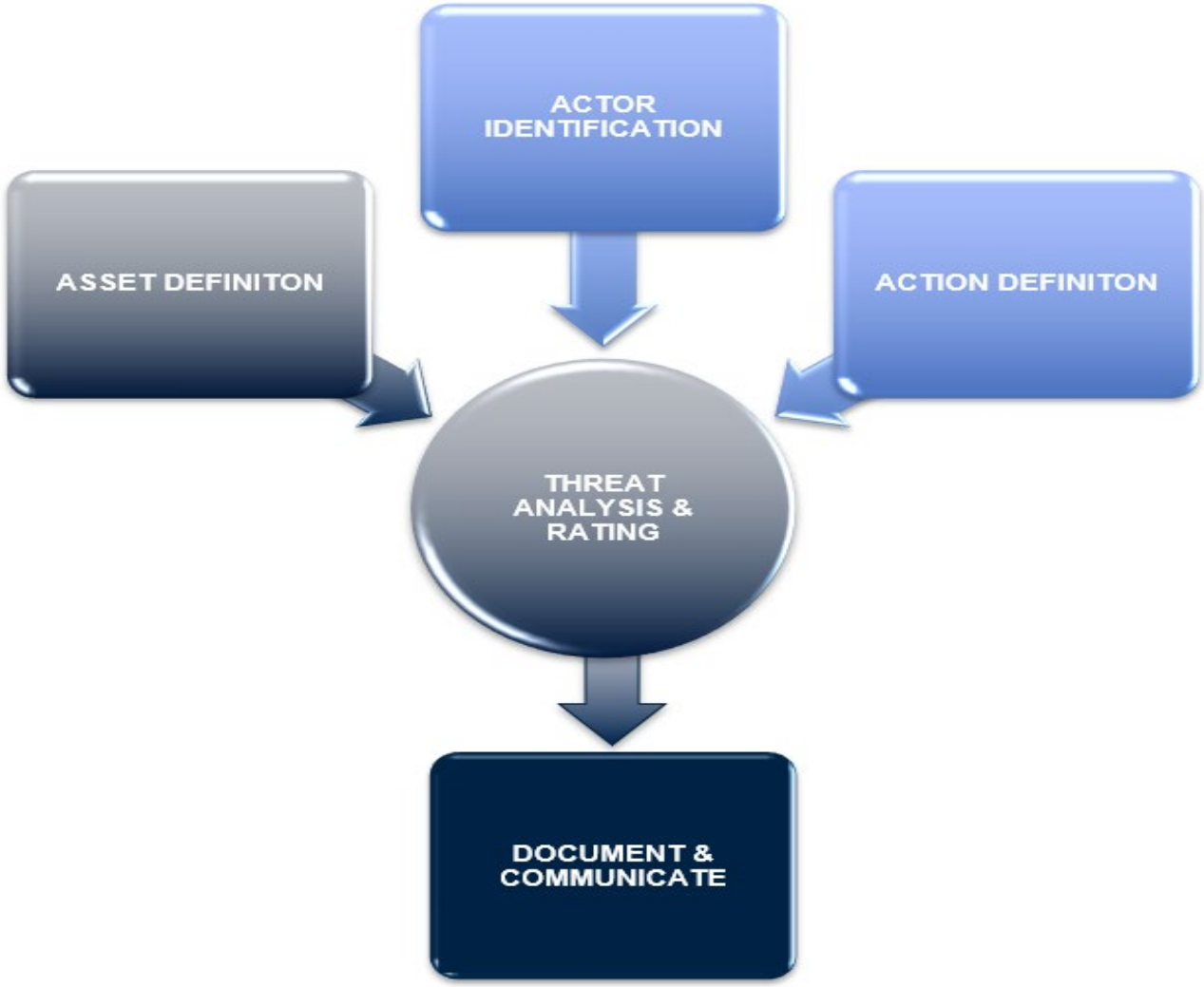
5G Security Challenges

- Increased attack surface
  - More functionality at the edge of the network
  - Distributed architecture, multiple layers, multiple vendors
  - Wide range of devices to connect to the network
  - Heavy reliance on software and cloud providers
- Increased role in the overall economy
  - Support mission-critical applications
- Security features deemed optional

RSAConference2020

An effective way to analyze security risks is via threat modeling

The Threat Modeling Process



Assets

Network side

- Radio access network
- Core network
- Multi-access Edge Computing
- Physical infrastructure
- Virtualization

User side

- User equipment
- User/device identity
- User session
- Application data
  - In storage, on network, in memory
- APIs

Threat Actors

Internal

- Rogue administrator
- Privileged insider
- User – intentional
- User – accidental

External

- State-sponsored actor
- Cyber criminal
- Hacktivist
- Competitor
- Former authorized user

Threat Actions – STRIDE + LM

Threat Type	Property Violated	Definition
Spoofing Identity	Authentication	Impersonating something or someone else
Tampering	Integrity	Modifying data or code
Repudiation	Non-repudiation	Claiming to have not performed an action
Information Disclosure	Confidentiality	Exposing information to unauthorized user
Denial of Service	Availability	Deny or degrade service to users
Elevation of Privilege	Authorization	Gain capabilities without proper authorization
Lateral Movement	Least Privilege	Gain access by crossing control boundary

Threats (Actors Performing Actions)

Same as in 4G

- Fake access network node
- IMSI catching
- Session hijacking
- Signaling fraud between networks
- Abuse of lawful interception
- Abuse of remote access

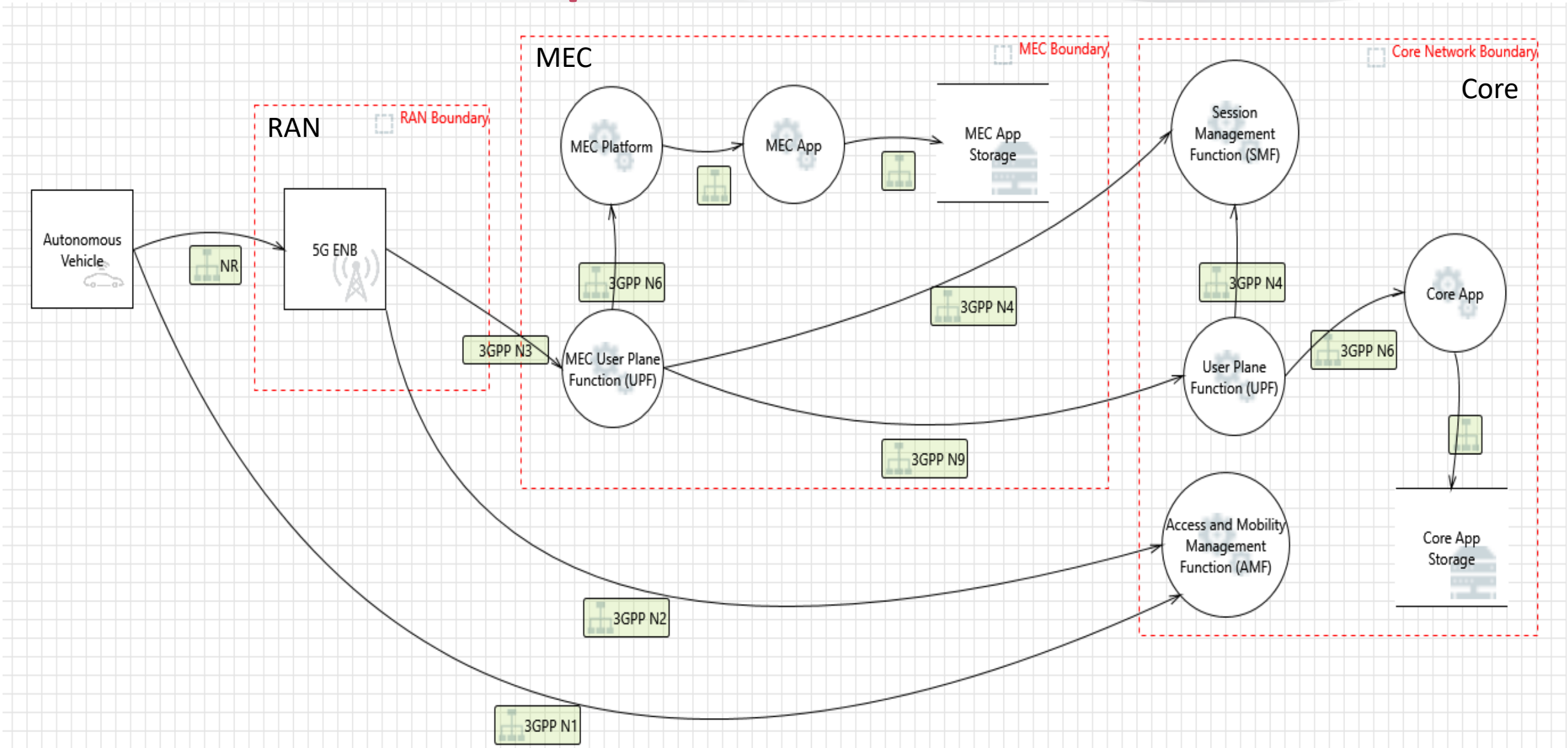
etc.

New or Increased in 5G

- Abuse by rogue cloud service provider
- Memory scraping in SDN
- Network virtualization bypassing
- False or rogue MEC gateway
- (Edge) API exploitation
- Lateral movement in the core network

etc.

Threat Model for a Specific Use Case



Sample Threat Table for the Use Case

Ref. ID	Threat Actor	Threat Action	Property Violated	Description
CC-FN	Cyber Criminals	Fake access network node	Confidentiality, Integrity	Rogue base station that is masqueraded as legitimate, allowing Man in the Middle attacks (MitM).
RA-DE	Internal Rogue Admin at MEC layer	Data exfiltration	Confidentiality	A rogue admin who has access to an MEC node could make copies of sensitive data and send it somewhere else.
EH-API	Hacktivist	Abuse of Open API at MEC layer	Confidentiality, Availability	Hackers exploits vulnerabilities in the MEC APIs that is used for federated services, external content, etc.
RA-MNF	Rogue Admin at core network layer	Registration of malicious network function	Confidentiality	Setup and register an unauthorized network function (NF) or function embedding a Trojan, by an insider or a vendor/service provider.

Sample Risk Assessment and Disposition

Ref. ID	Inherent Risk	Existing Controls	Residual Risk	Further Mitigation Needed?
CC-FN	High	Certificate-based authentication of network nodes	Low	No
RA-DE	Moderate	Third-party attestation, Two-factor authentication	Low	No
EH-API	Substantial	Regular vulnerability scan and remediation	Moderate	Yes
RA-MNF	Substantial	Third-party certification of network functions with digital signature	Low	No

5G Threats – Major Mitigating Controls

- Zero-trust architecture approach
- Segmentation and isolation at network and application layers
- Policy-based security management
- Security controls automation
- Granular user access control
- Strong authentication and end point protection
- Certification and compliance of equipment and (virtual) network

Apply What You Have Learned Today

- Identify 5G relevance for your organization in the next 18 months
- Conduct research on the technologies components in your use cases
- Run each use case through a threat model
- Based on the threat models, influence
  - Internal policy and procedures
  - Procurement process
  - Solution design and implementation
  - Control testing and monitoring

References

- Anand Prasad et al, “3GPP 5G Security.” May 2018.
- 3GPP, “System Architecture for the 5G System (5GS).” Dec. 2017.
- CSRIC WG3, “Report on Best Practices and Recommendations to Mitigate Security Risks to Emerging 5G Wireless Networks v14.0.” Sep. 2018.
- Adam Shostack, “Threat Modeling in 2019.” RSA 2019.
- ENISA, “Threat Landscape for 5G Networks.” Nov. 2019.
- NIS Cooperation Group, “EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks.” Oct. 2019.

RSAConference2020

Thank you!

My email: zzhang3@worldbankgroup.org