

# 5G 보안



2020. 11.  
(2021년 5월까지 사용 권장)

안 종 석  
james@jslab.kr  
**JS Lab**

# 목차

---

1. 5G 개요
2. 5G 보안 개요
3. 5G 네트워크 보안
4. 5G 기기와 사용자 보안
5. 5G 클라우드와 가상네트워크 보안

1. 5G 개요
2. 5G 보안 개요
3. 5G 네트워크 보안
4. 5G 기기와 사용자 보안
5. 5G 클라우드와 가상네트워크 보안

# 1. 5G 개요

## □ 5G는 아래의 세 가지 목표를 비전으로 기술개발 및 표준화 작업

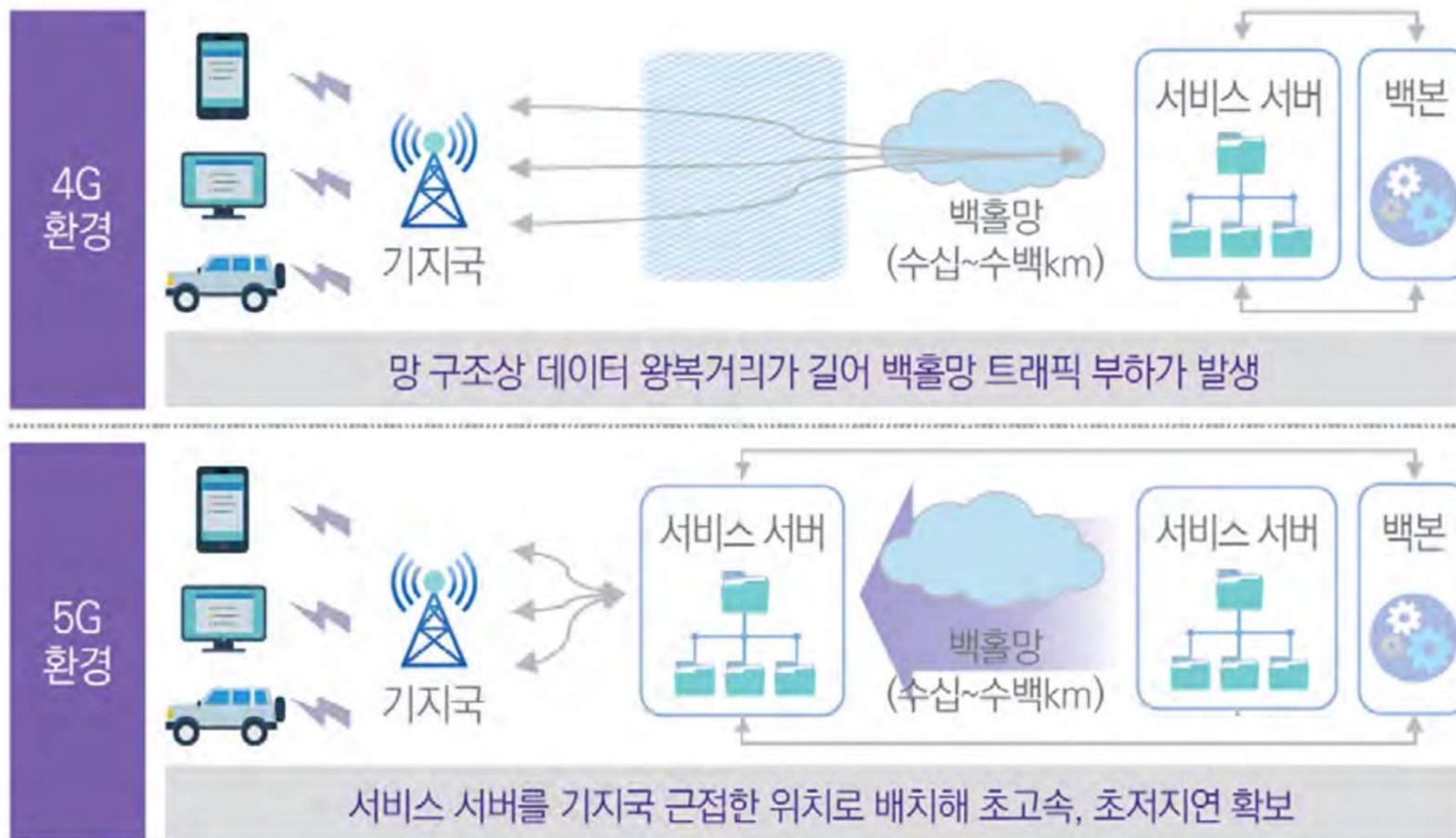
- 최대 전송속도 향상(**eMBB**: Enhanced Mobile Broadband)
- 초저지연 실시간 서비스(**URLLC**: Ultra-reliable and Low Latency Communication)
- 다수 기기 연결(**mMTC**: Massive Machine Type Communication)

초고속 (Hyper Capacity)	초저지연 (Near-Zero Latency)	초연결 (Massive Connectivity)
20Gbps~ (2020년)	1 msec (× 1/30)	1백만개/km <sup>2</sup> (× 1,000)
VR/AR, 홀로그램	Self-Driving Car	실시간 동시 통역
		

(출처: 매직리프, 구글, 와이어드 참고, KT경제경영연구소 재구성)

# 1. 5G 개요

- 5G는 애플리케이션의 분산/전진 배치로 초저지연 서비스 제공

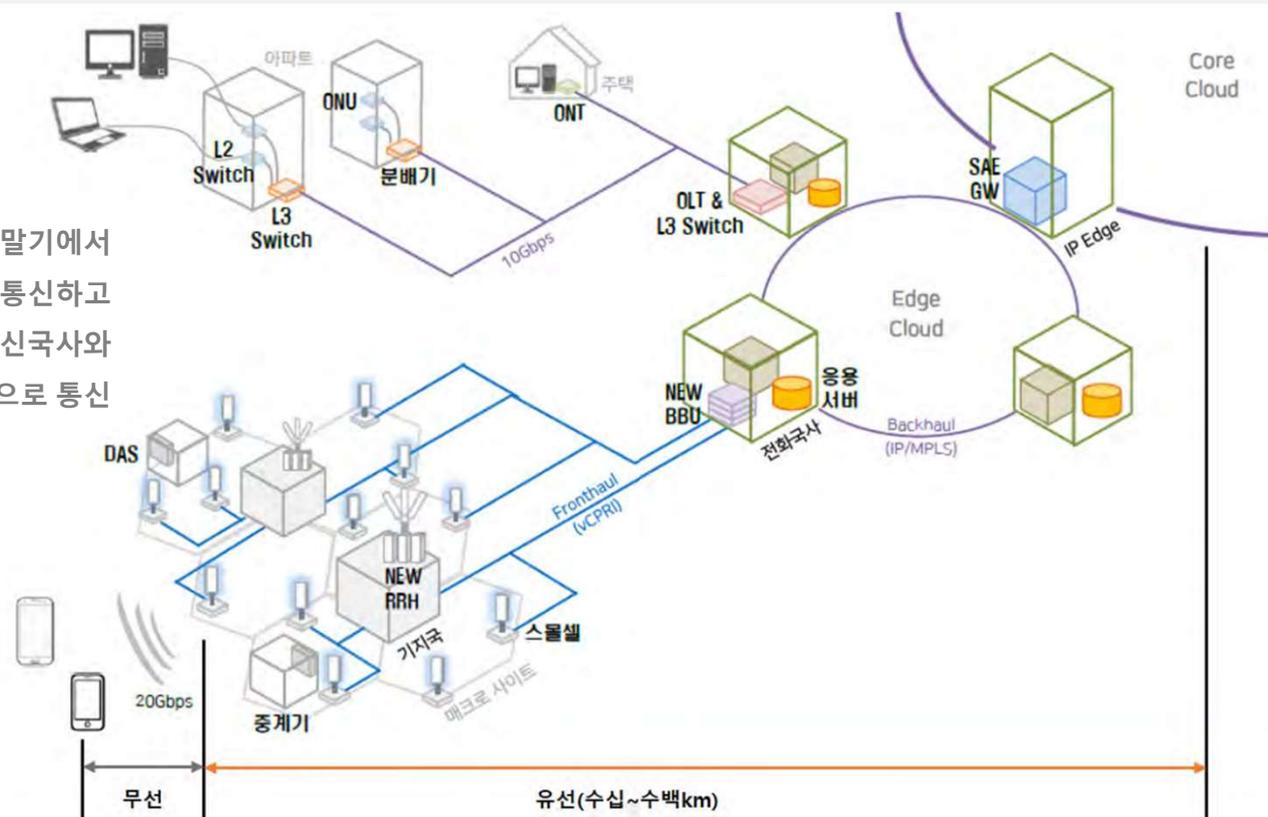


출처: 5G가 촉발하는 산업생태계 변화(삼성KPMG, '19)

# 1. 5G 개요

- 이동통신의 프로세스는 크게 세 가지로 구분이 가능하며, 단말기기지국, 기지국-통신국사, 통신국사-중앙 통신서버로 구분

스마트폰 등 단말기에서  
기지국까지는 무선으로 통신하고  
기지국을 거친 뒤 지역의 통신국사와  
서버까지는 유선으로 통신

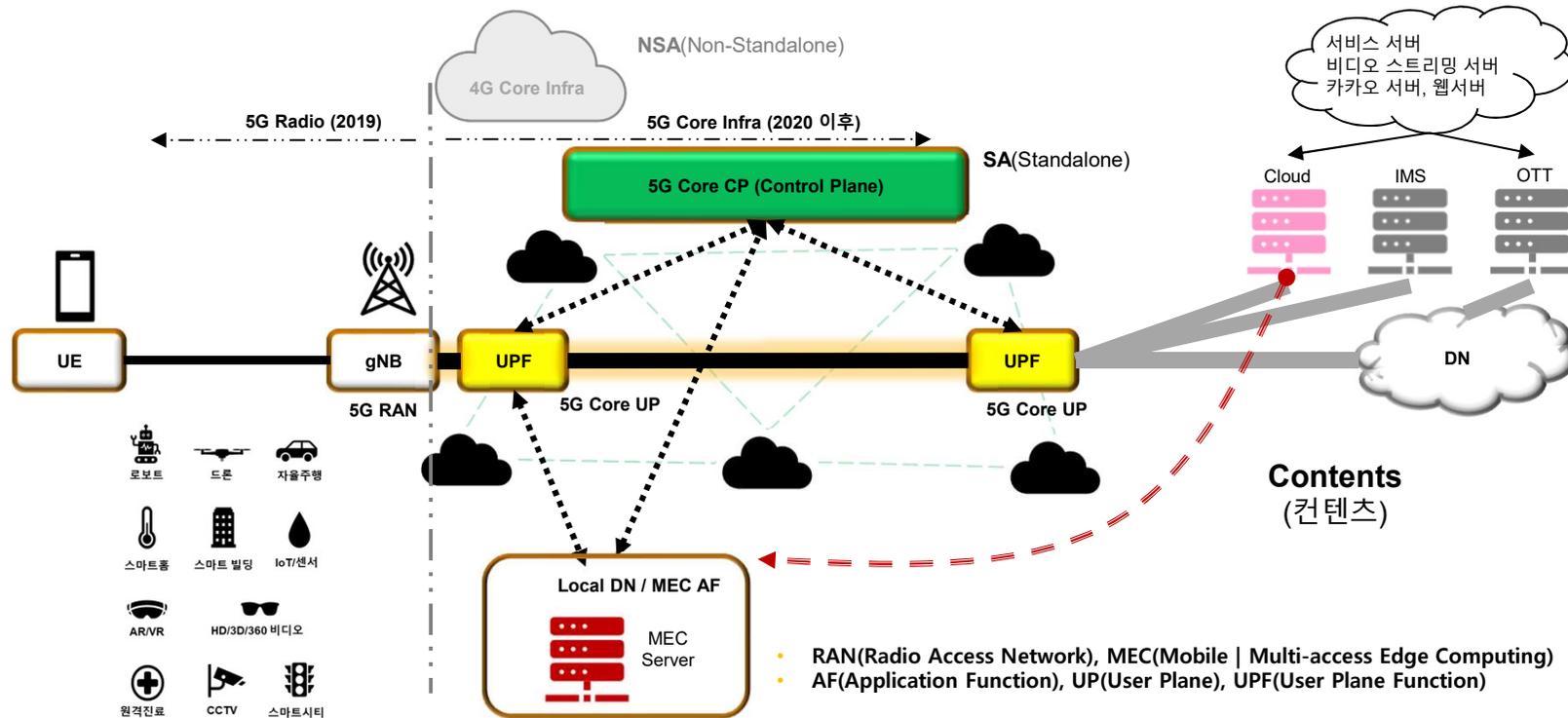


출처: 5G산업 심층 분석(메리츠, '18.8)

# 1. 5G 개요

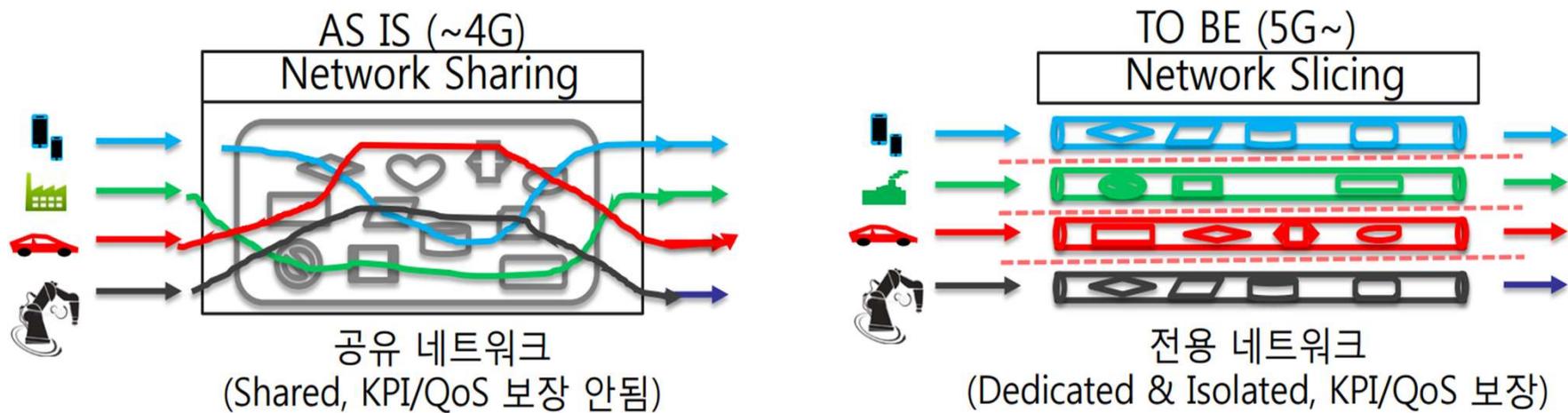
## □ 5G Standalone (SA) 구성

- 에지의 데이터센터 기술 도입: 국사의 데이터센터화 기지국 확대 고려
- 5G는 4G EPC 코어 공유로 서비스 시작: 5G 코어 적용 확대 중
- MEC는 Eco-system 확대 영역: API 제공 및 B2B 등의 모델 확대



# 1. 5G 개요

- 네트워크 슬라이싱으로 전용 네트워크를 위한 QoS(Quality of Service) 보장
- 융합산업 서비스 인프라 서비스 제공

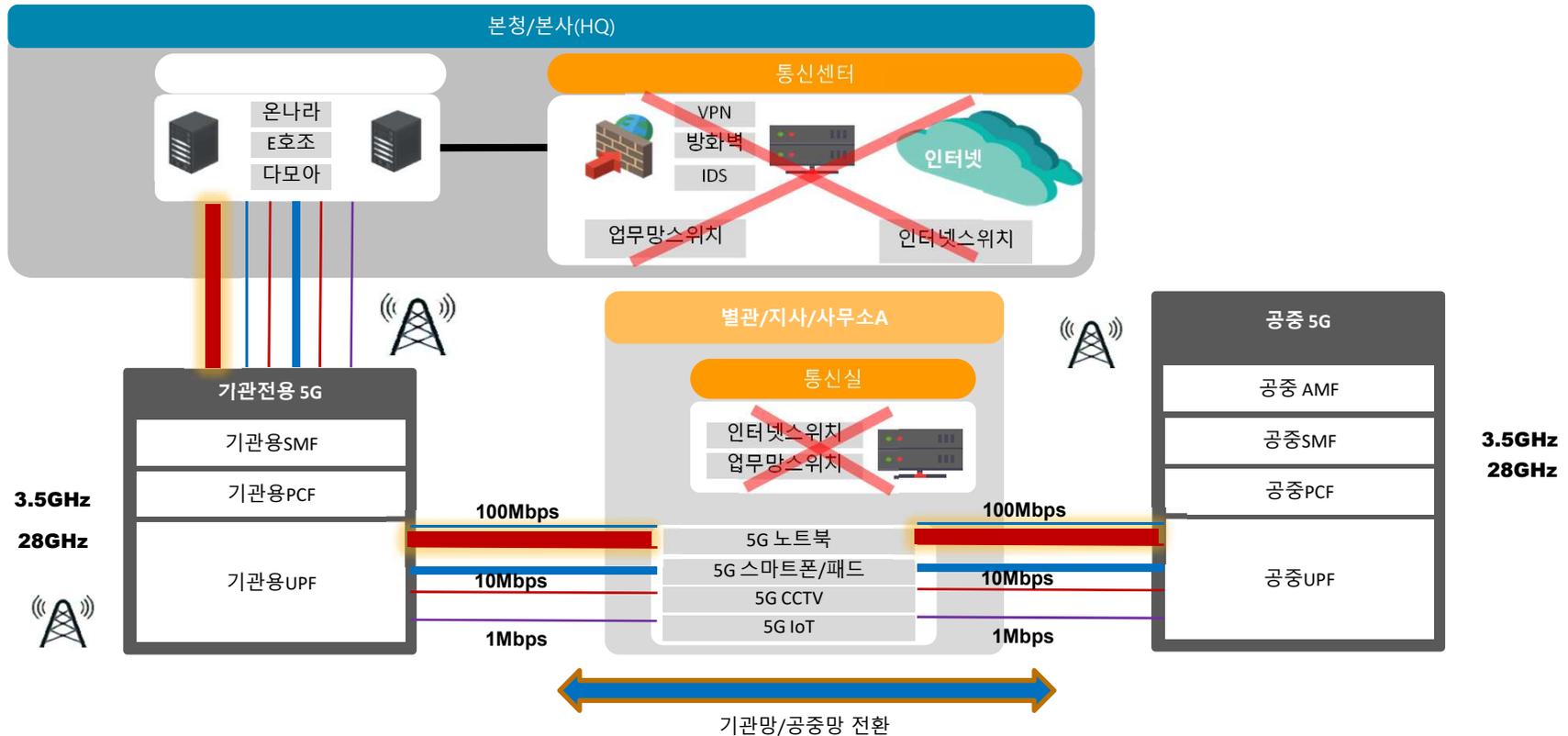


출처: 송평중, 한국전자통신연구원

# 1. 5G 개요

## □ 5G LAN/WAN(모델1/모델2)

- 장거리 전용회선 대신 5G를 이용하여 업무망/인터넷망 대체하고 네트워크 슬라이싱으로 업무별 안정성 확보 하여, 유선네트워크 구축이 물리적/경제적으로 어려운 상황에 효과적
- 기관내 통신장비를 최소화하고 네트워크 운영을 통신운영전문가(5G 통신사)에 위탁 검토



# 1. 5G 개요

## □ 5G 표준과 Market의 Radio 환경 변화/발전

- Phase 1 (칩셋, 단말기, 통신사)
- Phase 2 (New 칩셋, New 단말기, 상용 서비스)

주파수	Sub 6GHz		Above 6GHz		
	<3GHz	3~5 GHz	6~24 GHz	24~30 GHz	30~40 GHz
Operator					
SKT		3.6~3.7 GHz (100MHz)		28.1~29.0 GHz (800MHz)	
KT		3.5~3.6 GHz (100MHz)		26.5~27.3 GHz (800MHz)	
LGU+		3.42~3.5 GHz (80MHz)		27.3~28.1 GHz (800MHz)	

5G NR (100MHz) 1.5 Gbps } 배터리, latency 고려 동시지원 가능  
 4G LTE (145MHz) 1.2 Gbps }

# 1. 5G 개요

- 28GHz용 Access Unit (AU) 약 10Kg 무게와 10L 부피이며 최대 용량은 10 Gbps.



Access Unit



출처: Case study: Orange Romania, Samsung

# 1. 5G 개요

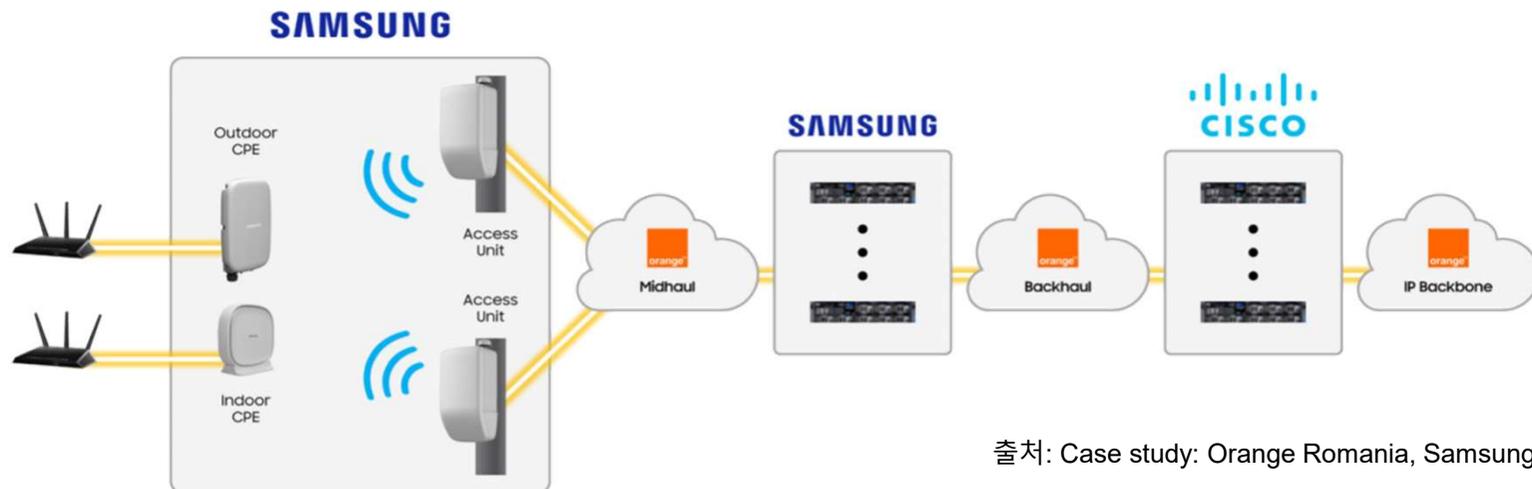
## □ 무선 브로드밴드 구성 - Orange Romania 5G FWA Friendly User Trial Architecture



Indoor CPE

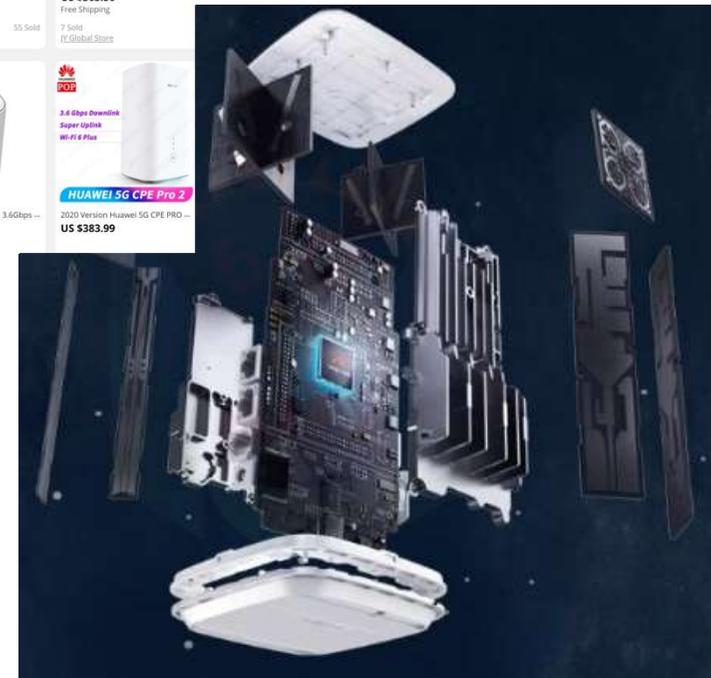
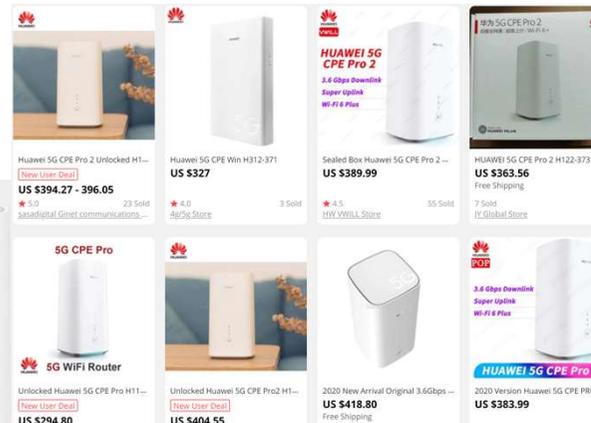


Outdoor CPE



# 1. 5G 개요

- Huawei 5G CPE Pro(H112-372) 5G NSA+SA CPE Wireless router wif 5g wifi modem router H112 router lan port H112-370 5g router
- US \$325.60 - 830.28



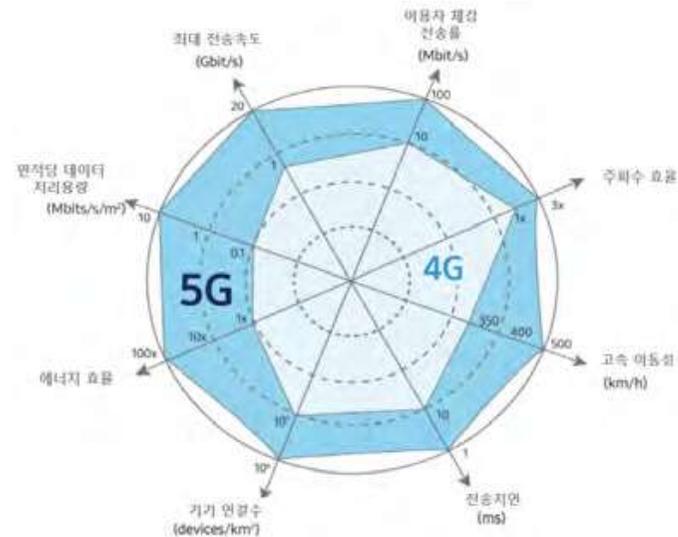
출처: <https://www.aliexpress.com/>

# 1. 5G 개요

- 전송속도 향상뿐 아니라 사물인터넷 등 다수 기기접속 및 초저지연 연동을 포함하는 개념으로 목표를 설정하고 기술개발 진행 중
- 5G는 4G 대비 약 10배 이상의 성능 향상을 기대

Item	4G	5G
최대 전송속도	1Gbps	20Gbps
이용자 체감 전송율	10Mbps	100Mbps
주파수 효율	-	x 3
면적당 데이터 처리 용량	0.1Mbps/m <sup>2</sup>	10Mbps/m <sup>2</sup>
전송지연	10ms	1ms
최대 연결 기기 수	100,000/km <sup>2</sup>	1,000,000/km <sup>2</sup>
네트워크 에너지 효율	-	x100
고속 이동성	350km/h	500km/h

<4G와 5G 핵심성능 비교>



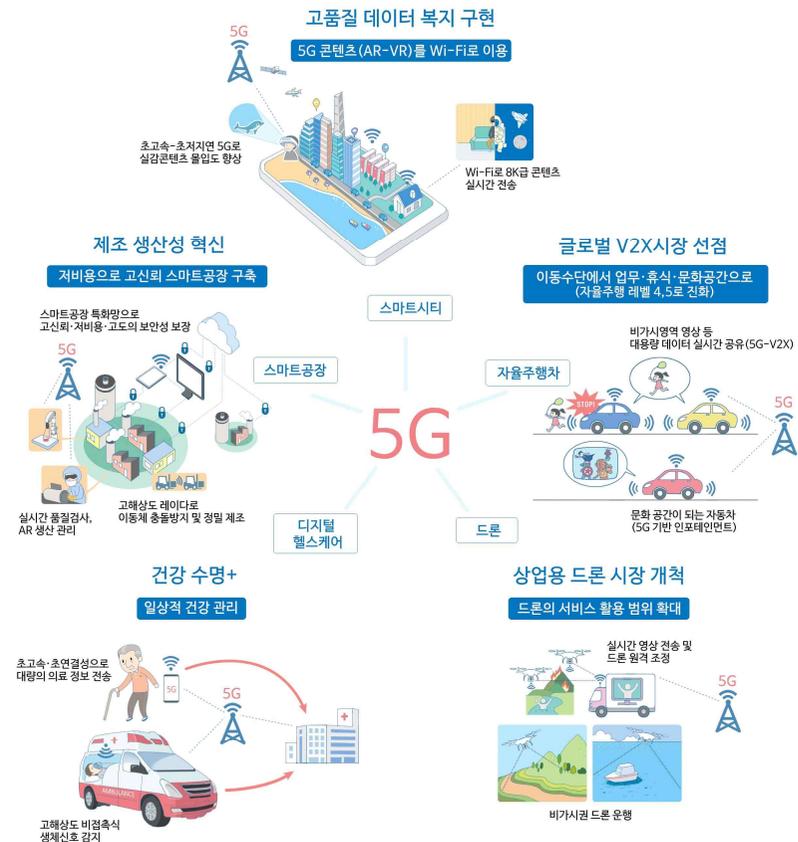
출처: 5G 이슈와 성공전략, 정보화진흥원

# 1. 5G 개요

- 5G와 결합·보조하는 비면허 기술을 5G 성능으로 고도화 전략 (과기정통부)
- 비면허 주파수는 국민 일상과 산업 전반에 걸쳐 필수재

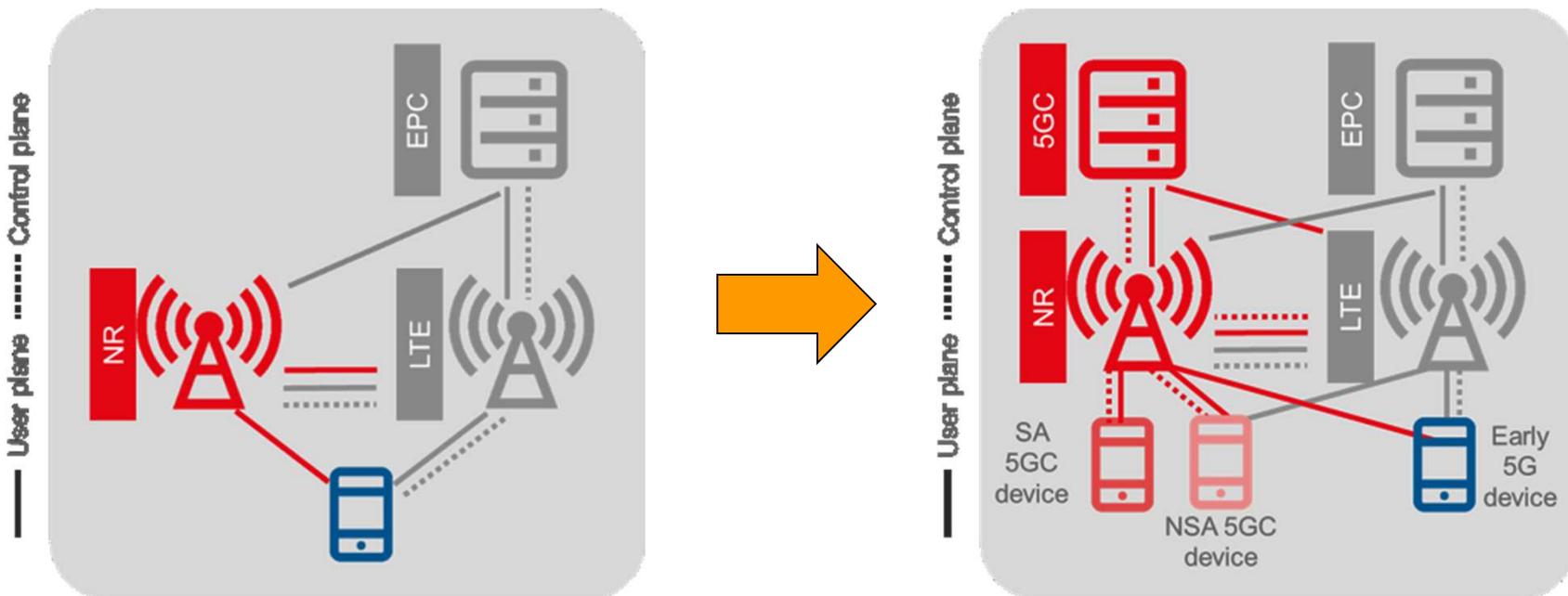


출처: 5G+ 스펙트럼 플랜, 과학기술정보통신부



# 1. 5G 개요

- **비단독표준(NSA, Non Standalone):** 5G 액세스 네트워크를 4G 네트워크와 연동시키는 구조
- **단독표준(SA, Standalone):** 5G 전용 무선 접속망과 5G 전용 유선망을 이용하는 구조



출처: Road to 5G: Introduction and Migration (GSMA, 2018)

# 1. 5G 개요

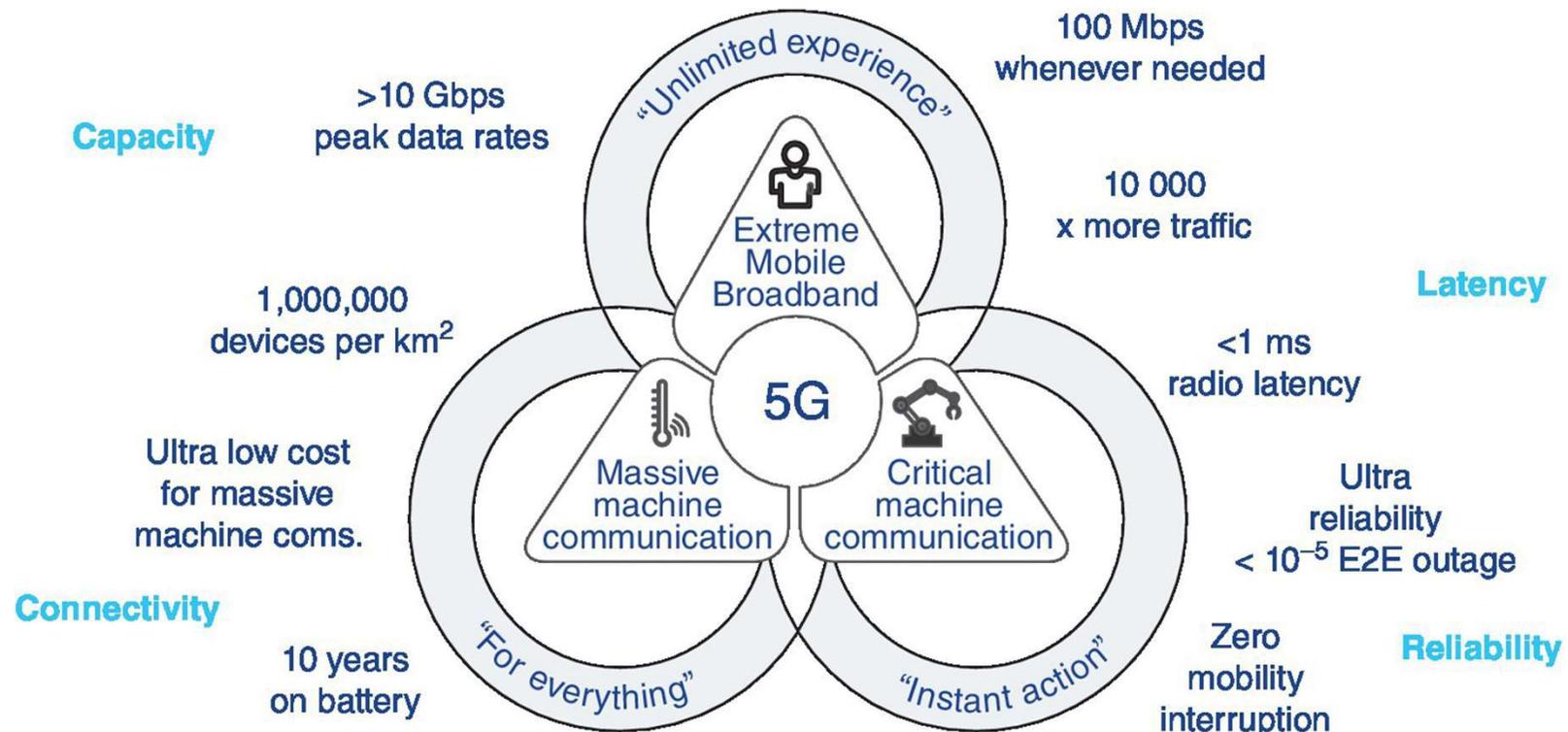
## □ 4차 산업혁명과 5G 시대의 주요 변화

- IoT를 기반 생산기기와 생산품 간 통신체계를 구축하여 전체 생산과정을 최적화
- 자율주행차의 고도화,
- AR 및 VR의 대중화와 엔터테인먼트 산업의 성장



# 1. 5G 개요

- 최대 전송속도 향상(eMBB: Enhanced Mobile Broadband)
- 초저지연 실시간 서비스(URLLC: Ultra-reliable and Low Latency Communication)
- 다수 기기 연결(mMTC: Massive Machine Type Communication)



A Comprehensive Guide to 5G Security by Andrei Gurtov; Madhusanka Liyanage; Ahmed Bux Abro; Mika Ylianttila; Ijaz Ahmad Published by Wiley, 2018

1. 5G개요
- 2. 5G 보안 개요**
3. 5G 네트워크 보안
4. 5G 기기와 사용자 보안
5. 5G 클라우드와 가상네트워크 보안

## 2. 5G 보안 개요

- 5G; Security architecture and procedures for 5G System (3GPP TS 33.501 version 15.4.0 Release 15)

ETSI TS 133 501 V15.4.0 (2019-05)

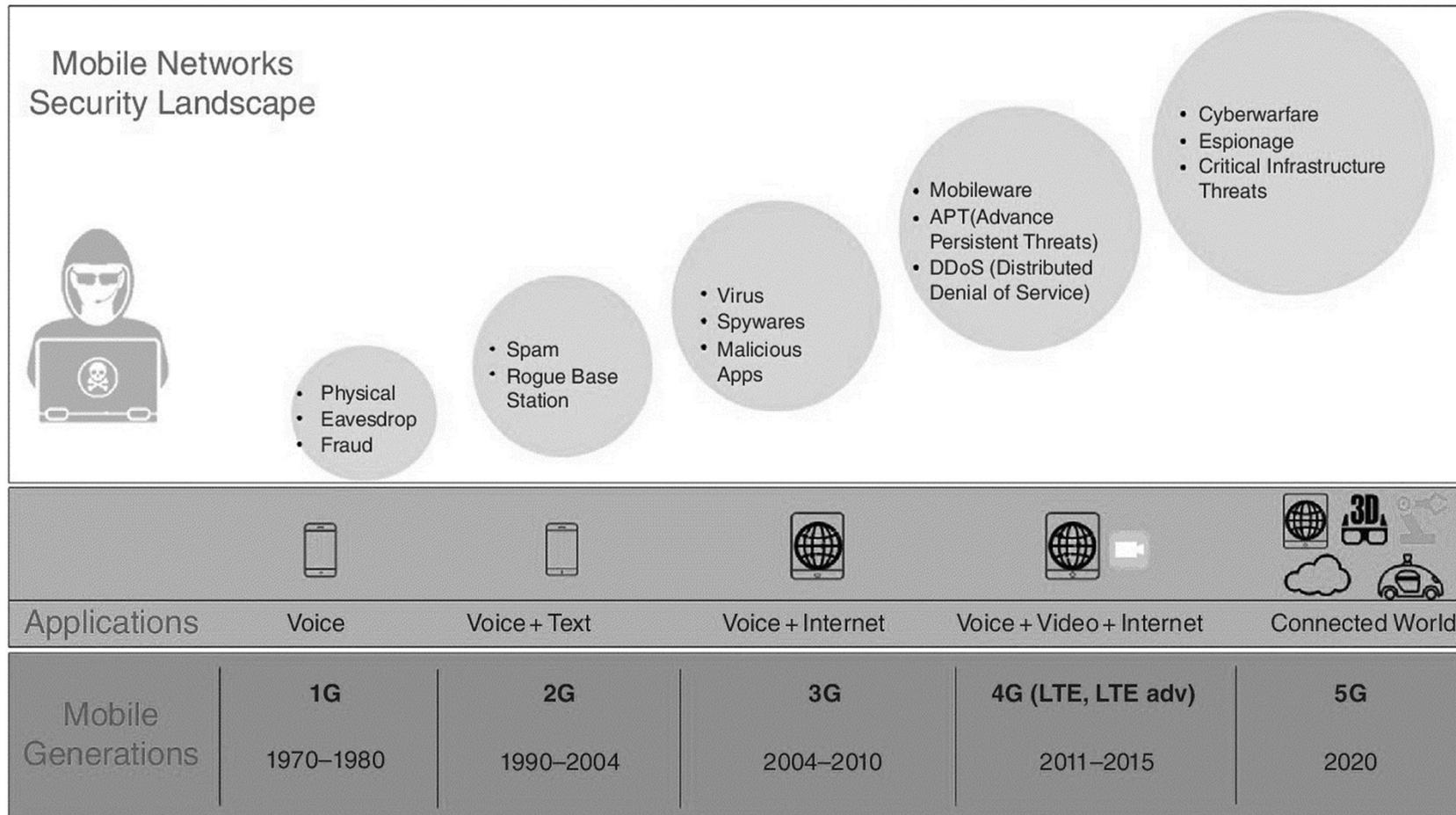


5G;  
Security architecture and procedures for 5G System  
(3GPP TS 33.501 version 15.4.0 Release 15)



# 2. 5G 보안 개요

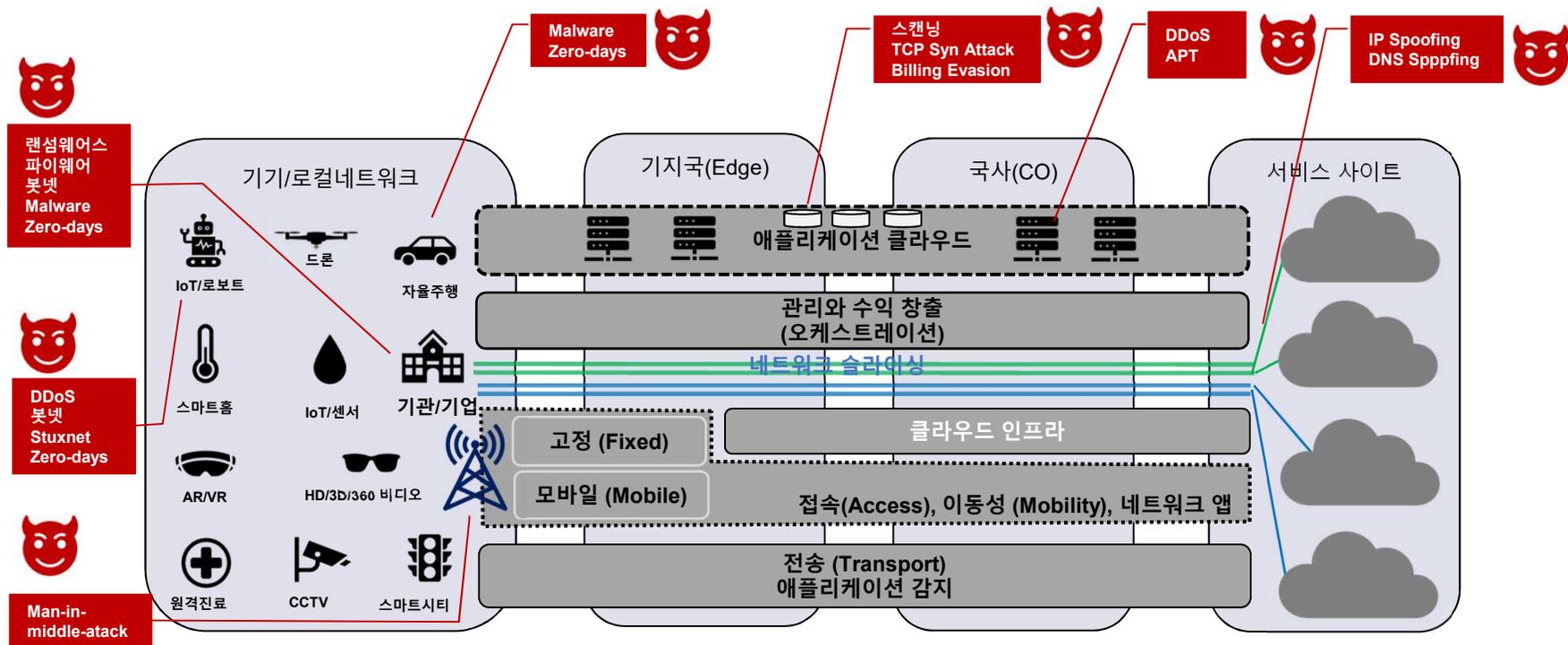
## □ 모바일 네트워크 보안 변화



A Comprehensive Guide to 5G Security by Ijaz Ahmad; Andrei Gurtov; Mika Ylianttila; Madhusanka Liyanage; Ahmed Bux Abro Published by Wiley, 2018

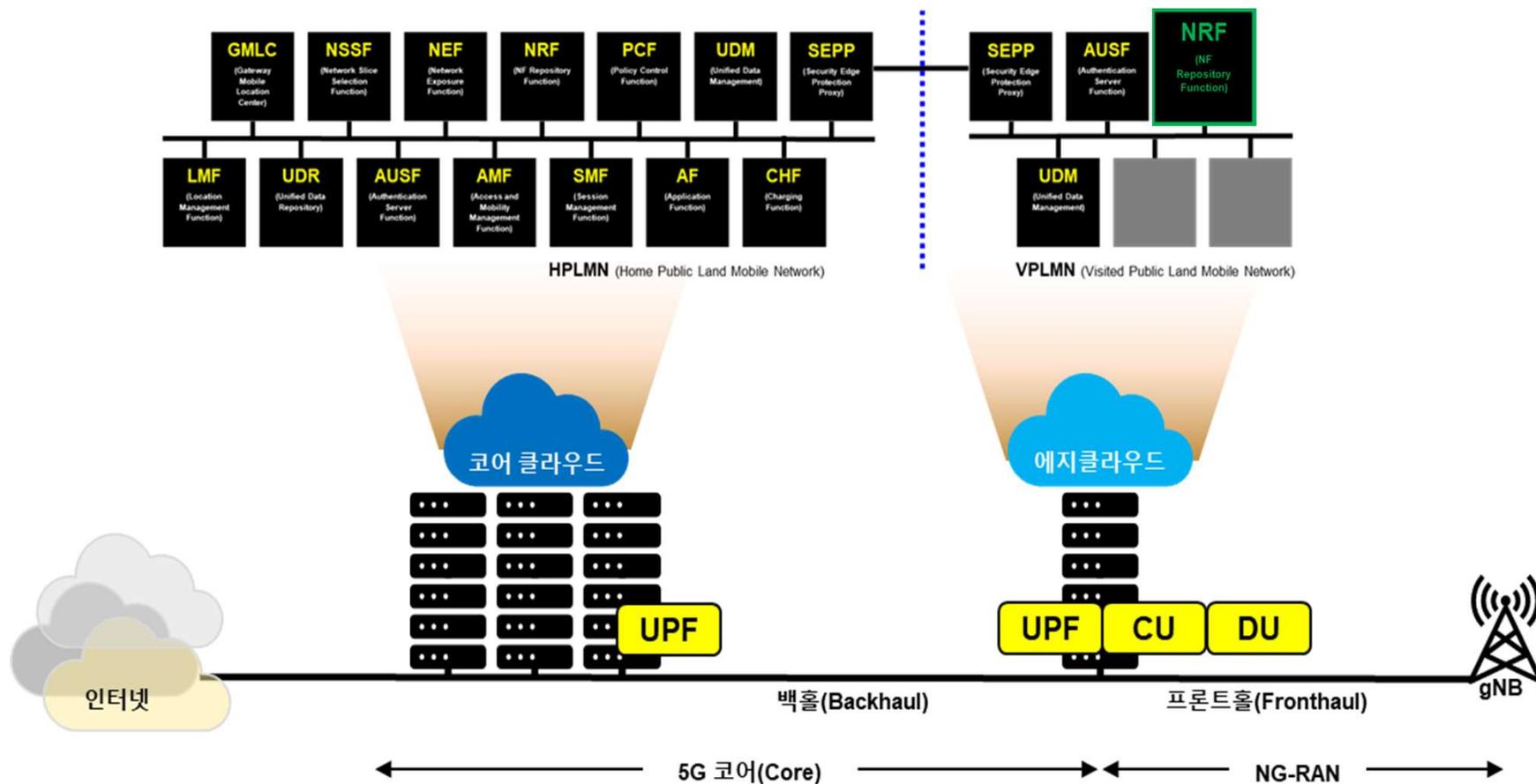
# 2. 5G 보안 개요

- Edge(기지국)와 Central Office(국사)의 데이터센터 화 진행
- 클라우드 네이티브화
- 네트워크 슬라이싱
- 기기 클러스터링 확장



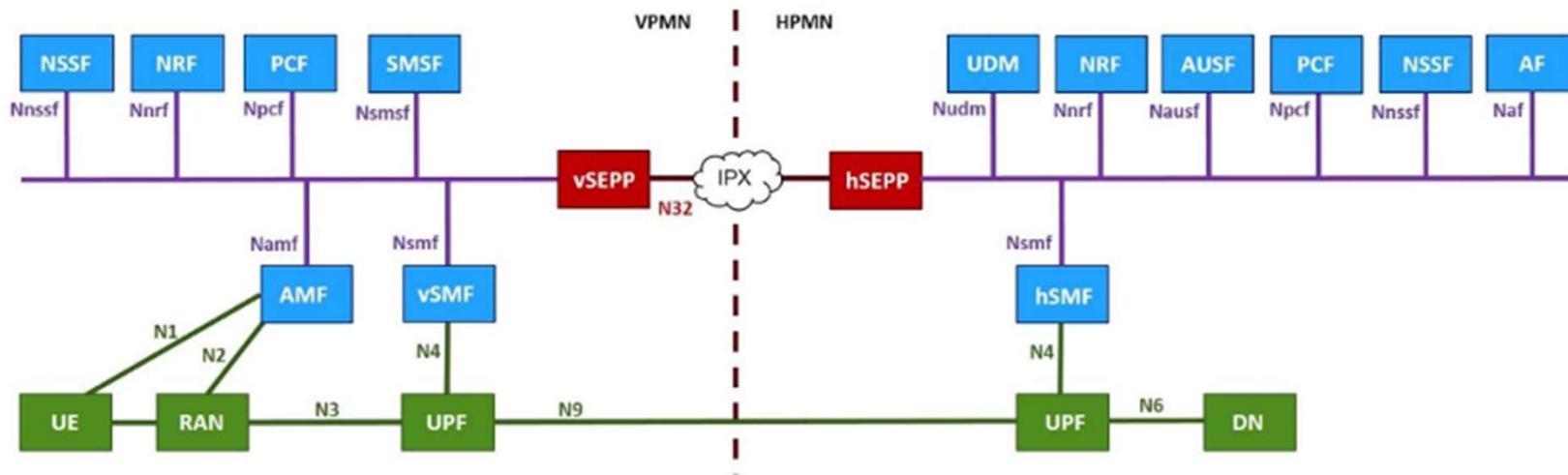
# 2. 5G 보안 개요

- Authorization of NF service access
- Framework based on Oauth 2.0



## 2. 5G 보안 개요

- If SA deployment is selected, a completely new protocol -HTTP/2- will be used for 5G signaling. Operator-to-operator interconnection will be done through a new module Secure Edge Protection Proxy (SEPP). Standards are not yet completed.
- Inter-operator signaling (API calls)
- SEPP: Security Edge Protection Proxy
- SEPP2SEPP security considering IPX intermediaries
- E2e signalling Message flow over N32



Source: GSMA Roaming Implementation Guide NG.113-v1.0

# 2. 5G 보안 개요

## □ 5G 보안 위협 분석

위협	설명	피해 수준 (Minor, Moderate, Severe, Extreme)	발생 빈도 (1-5, Low-High)
랜섬웨어	Specialized malwares use exploit, encrypt and lock access to critical data. Access granted after paying demanded ransom money	Severe	3
멀웨어	Advance malwares targeting billions of mobile and IoT devices with capability to exploit the OS and network vulnerabilities	Extreme	3
IoT 봇넷	IoT and mobile devices hosting a control agent/bot receiving remote commands and continuously leaking telemetry information to a remote bot-master running a central command and control (C&C) system. Used for both passive and active attacks	Severe	2
인프라 위협	Threats that are focused, damaging critical infrastructure services such as SCADA, i.e. Stuxnet, Shamoon attacks	Extreme	3
제로데이 공격	An advance attack exploiting the undiscovered vulnerabilities of a system. Can be a combination or package of multiple attack types, malware, rootkits and botnets	Extreme	1

A Comprehensive Guide to 5G Security by Ijaz Ahmad; Andrei Gurtov; Mika Ylianttila; Madhusanka Liyanage; Ahmed Bux Abro Published by Wiley, 2018

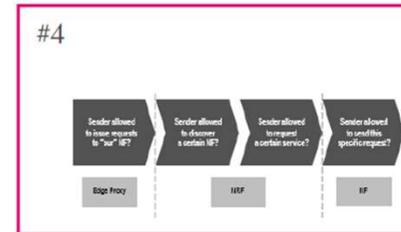
# 2. 5G 보안 개요

## □ 보안 구성 가이드



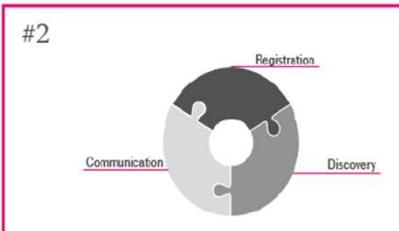
Authentication, authorisation, antispoofing, traffic protection

인증/권한/안티스푸핑, 트래픽 차단



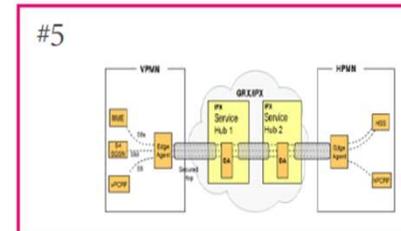
Authorisation at edge, NRF, and NF

에지의 권한, NRF와 NF



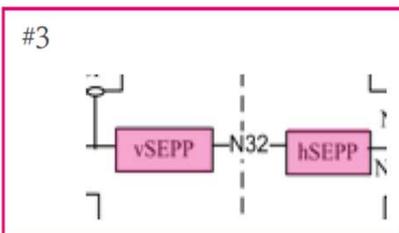
Apply goal #1 during registration, discovery, communication

등록, 디스커버리, 통신 중 위 #1 기능 제공



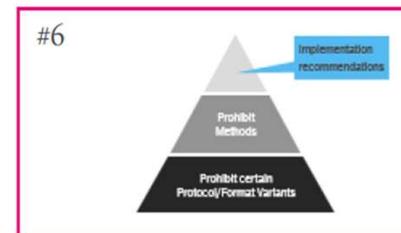
Hop-by-hop plus end-to-end security for IPX

홉단위와 종단간 보안



Establish edge proxy in 5G architecture

5G 아키텍처의 에지 프록시 구축



Security guidelines for new protocol stack

새로운 프로토콜 스택을 위한 보안 가이드



Source: GSMA Roaming Implementation Guide NG.113-v1.0

# 2. 5G 보안 개요

## □ 표준화 활동

### ■ NGMN: Security Competence Team (SCT) formed in May 2017

### ■ SCT Activities @ ITU 2018

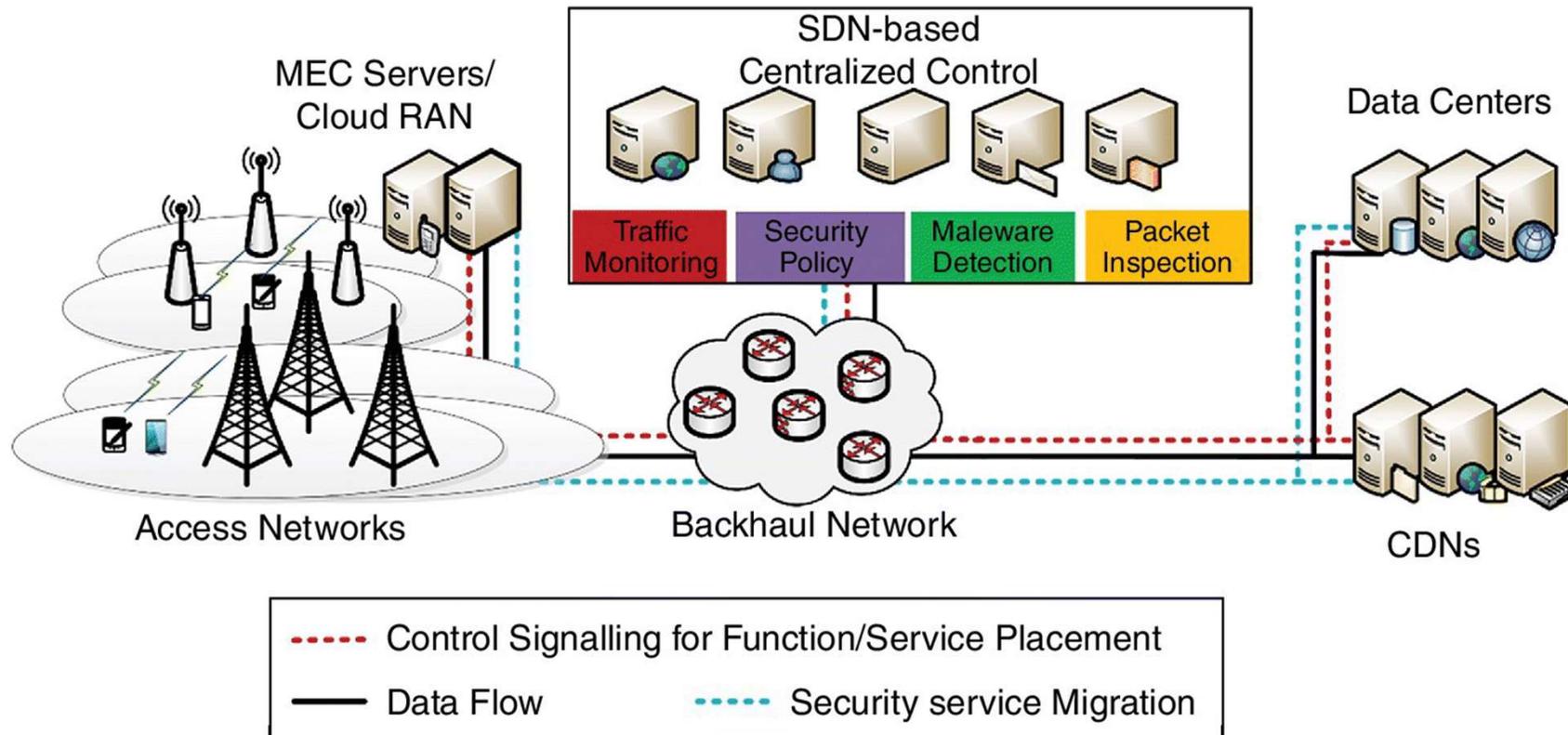
- 5G E2E Architecture Framework – Security requirements
- Cellular V2X – Security and privacy aspects
- Network Capabilities Exposure – Security aspects and requirements
- 5G RAN Functional Decomposition – Security of new interfaces
- Update of “5G Security – Package 3: Mobile Edge Computing / Low Latency / Consistent User Experience” (NGMN, Oct. 2016) with respect to law enforcement requirements for MEC
- Pre-commercial 5G Network Trials & Testing – Security Tests

Standardization bodies	Workgroups	Major security areas in focus	Milestones
3GPP	Service and System Aspects Security Group (SA3)	Security architecture, RAN security, authentication mechanism, the subscriber privacy, network slicing	TR 33.899 Study on the security aspects of the next generation system, TS 33.501: Security architecture and procedures for 5G System
5GPPP	5GPPP Security WG	Security architecture, the subscriber privacy, the authentication mechanism	5G PPP Security Landscape (White Paper) June 2017.
IETF	I2NSF, DICE WG, ACE WG, DetNet WG	Security solutions for massive IoT devices in 5G, User privacy, Network security functions (NSFs)	RFC 8192, RFC 7744, Deterministic Networking (DetNet) Security Considerations
NGMN	NGMN 5G security group (NGMN P1 WS1 5G security group)	Subscriber privacy, Network slicing, MEC security	5G security recommendations: Package 1 and 2, and 5G security: Package 3
ETSI	ETSI TC CYBER, ETSI NFV SEC WG, ESTI MEC ISG	Security architecture NFV security, MEC security, privacy	ETSI GS NFV-SEC 010, ETSI GS NFV-SEC 013 ETSI GS NFV-SEC 006 and ETSI GS MEC 009
NIST	Security working group	IoT security guidelines and assessment	Draft Interagency Report, NISTIR 8200

1. 5G 개요
2. 5G 보안 개요
- 3. 5G 네트워크 보안**
4. 5G 기기와 사용자 보안
5. 5G 클라우드와 가상네트워크 보안

# 3. 5G 네트워크 보안

## Centralized security architecture for mobile clouds and MEC security

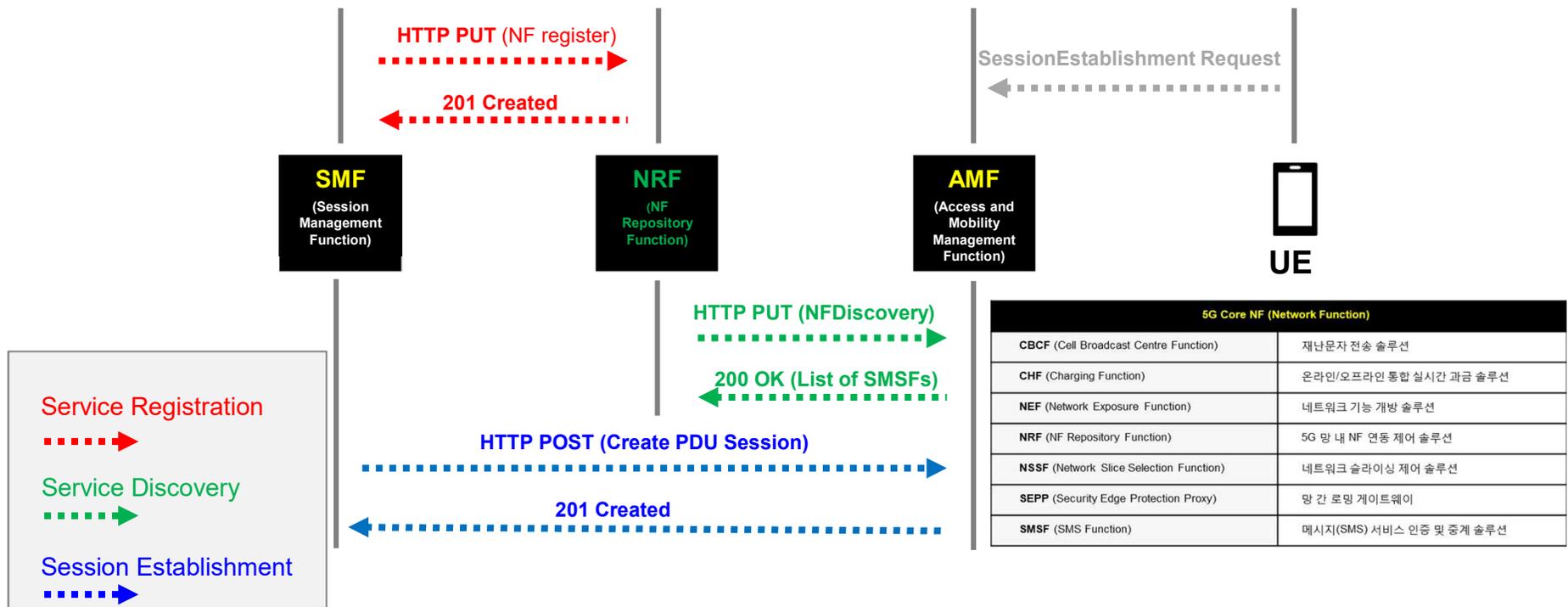


A Comprehensive Guide to 5G Security by Andrei Gurtov; Madhusanka Liyanage; Ahmed Bux Abro; Mika Ylianttila; Ijaz Ahmad Published by Wiley, 2018

# 3. 5G 네트워크 보안

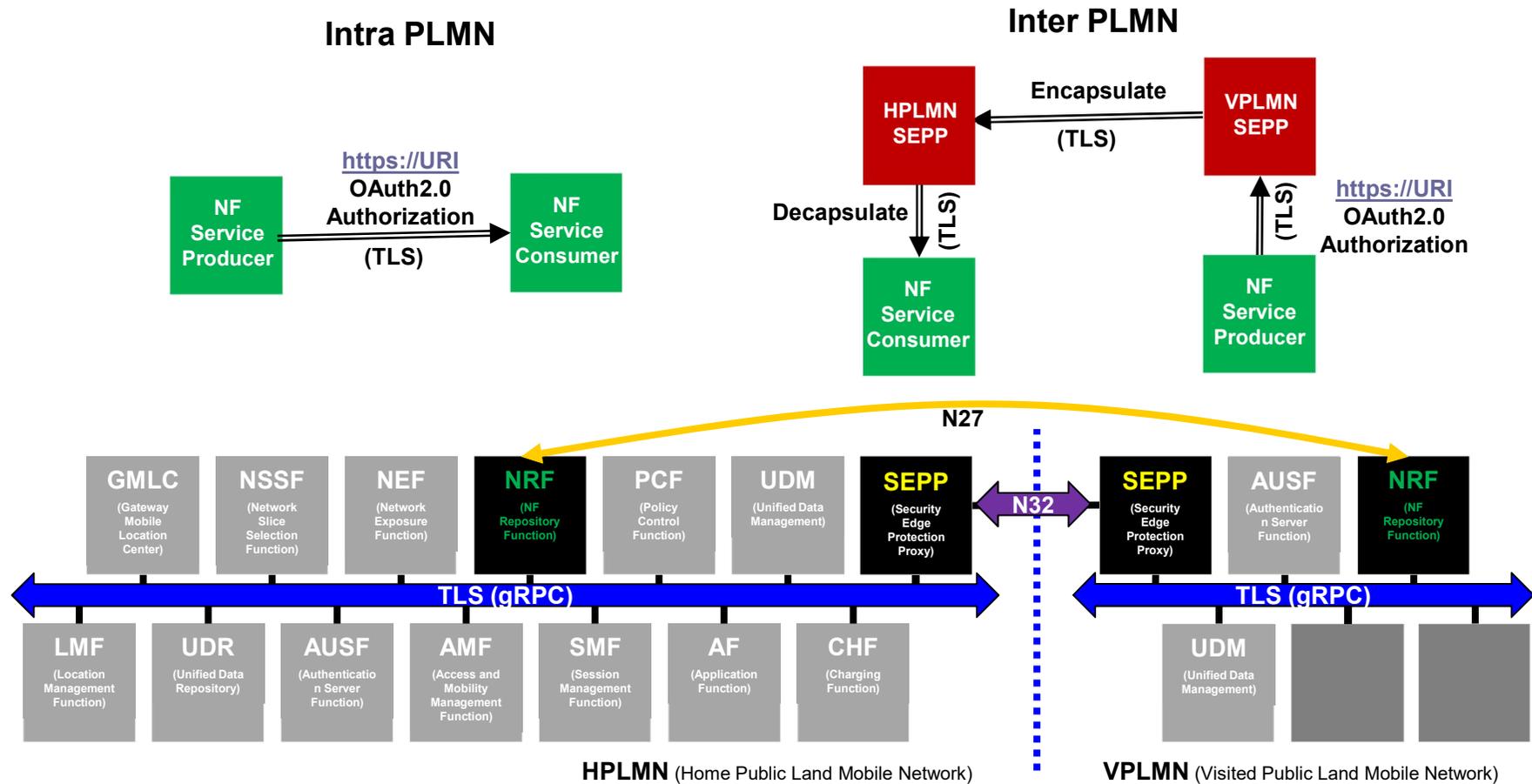
## □ NRF (NF Repository Function)

- Service Registration
- Service Discovery
- Session Establishment



# 3. 5G 네트워크 보안

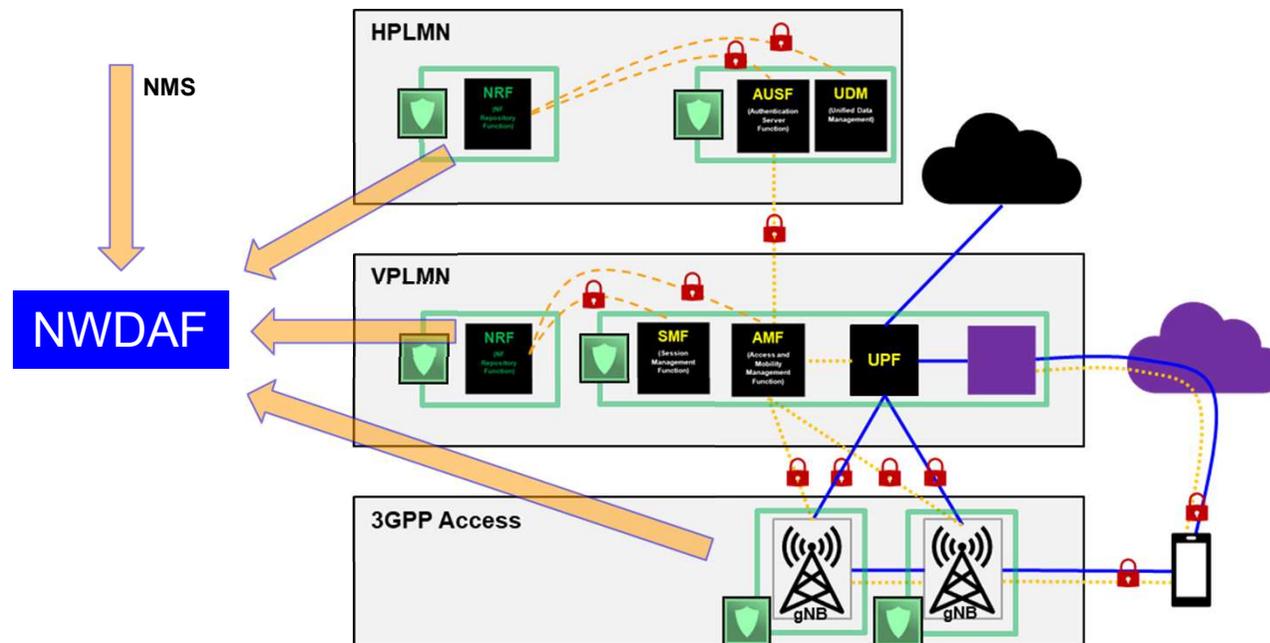
## □ NRF의 PLMN 간 통신 (N27)



# 3. 5G 네트워크 보안

## □ NRF의 Security architecture

- 인증 (Authentication framework), 가입자 프라이버시 (Subscriber privacy)
- SBA(Service based architecture) 와 보안 연결
- User Plane의 통합 보안 고려
- NWDAF: Network Data Analytics Function



1. 5G 개요
2. 5G 보안 개요
3. 5G 네트워크 보안
- 4. 5G 기기와 사용자 보안**
5. 5G 클라우드와 가상네트워크 보안

# 4. 5G 기기와 사용자 보안

## □ Hardware Root of Trust

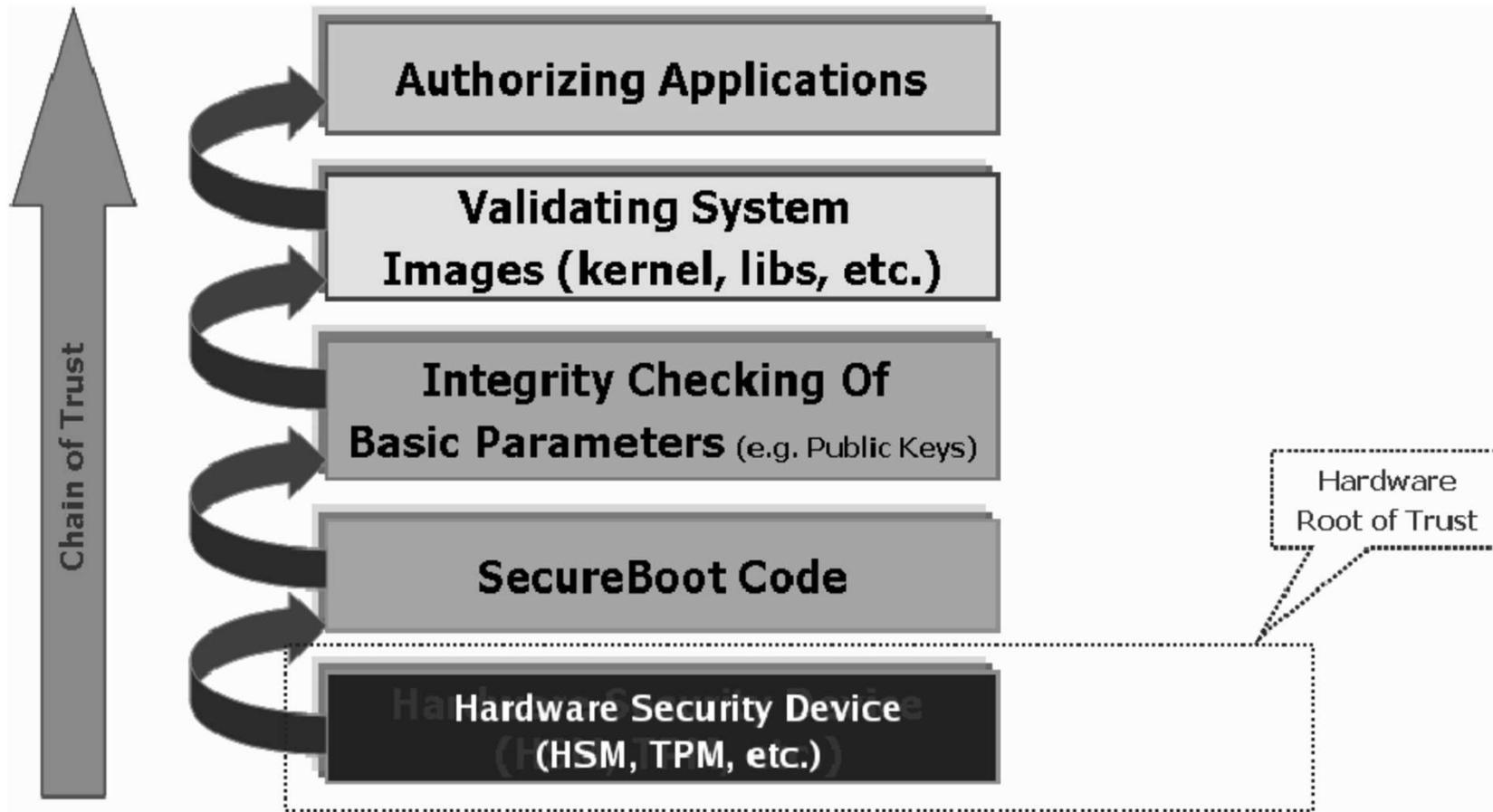
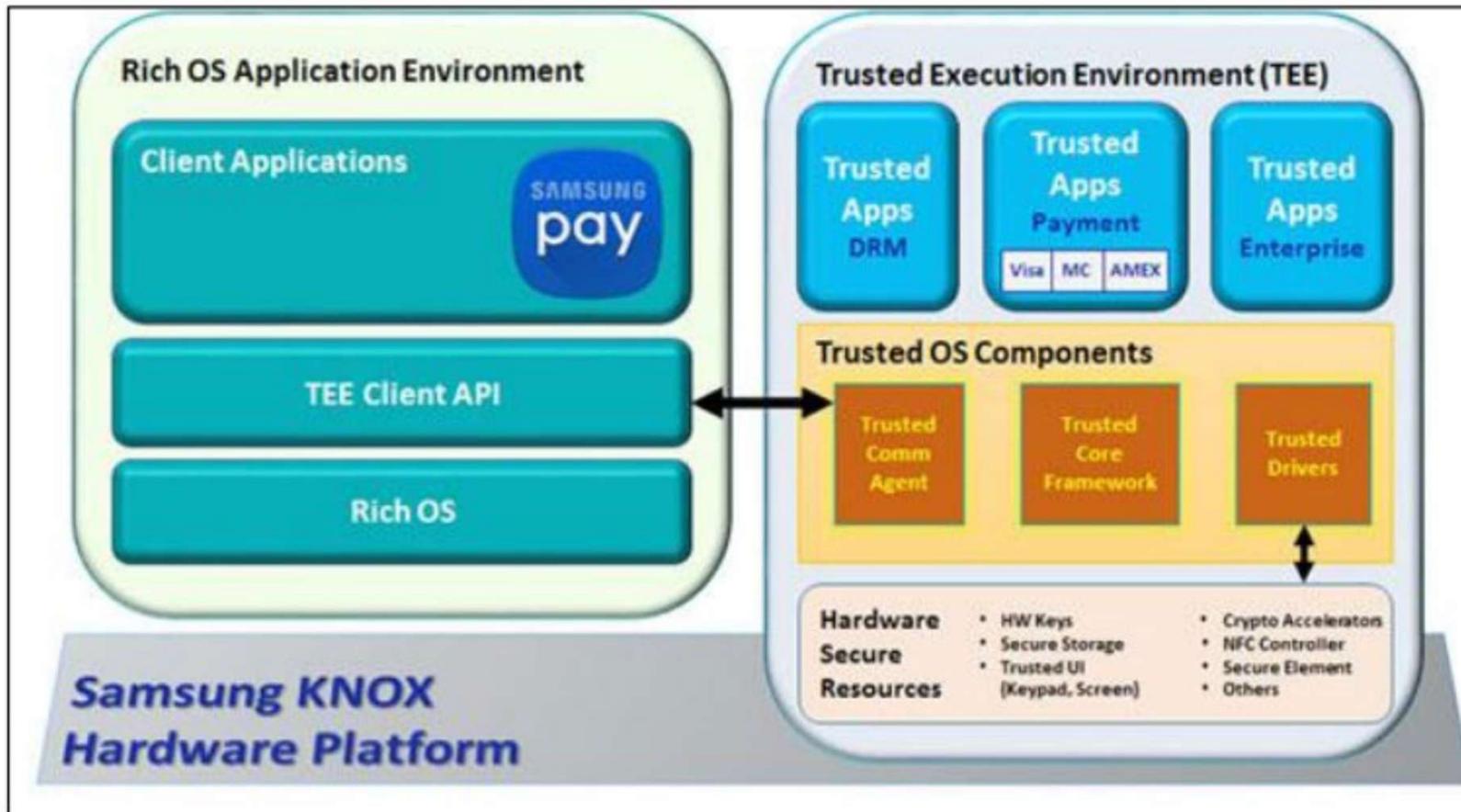


Image: [www.semanticscholar.org](http://www.semanticscholar.org)

# 4. 5G 기기와 사용자 보안

## □ Samsung KNOX Hardware Platform



Source: <http://developer.samsung.com/tech-insights/pay/device-side-security>

# 4. 5G 기기와 사용자 보안

□ 계층별 IoT 5G 보안

□ Security threats in automation IoT and their possible mitigation



Layer	Threat type	Mitigation
Physical	Tampering Denial of Service	tamper-resistant packaging spread-spectrum techniques
Networking	Denial of Service Eavesdropping	active firewalls, passive monitoring (probing), traffic admission control, bi-directional link authentication encryption, authorization
Data processing	Back door attack Social Engineering Exhaustion Malware	properly configured firewalls on all system entry point educating employees to security awareness traffic monitoring malware detection
Application	Client app. Comm. channel Integrity Modifications Multi-user access Data access	anti-virus filtering proper authentication, authorization, integrity verification testing validation process planning and design Traceability

# 4. 5G 기기와 사용자 보안

## □ IoT 5G 기술별 보안

## □ Security challenges in 5G technologies



Security Threats	Target Point/Network Element	Effected Technology				
		SDN	NFV	Channels	Cloud	Privacy
DoS attack	Centralized control elements	✓	✓		✓	
Hijacking attacks	SDN controller, hypervisor	✓	✓			
Signaling storms	5G core network elements			✓	✓	
Resource (slice) theft	Hypervisor, shared cloud resources		✓		✓	
Configuration attacks	SDN (virtual) switches, routers	✓	✓			
Saturation attacks	SDN controller and switches	✓				
Penetration attacks	Virtual resources, clouds		✓		✓	
User identity theft	User information data bases				✓	✓
TCP level attack	SDN controller-switch communication	✓		✓		
Man-in-the-middle attack	SDN controller-communication	✓		✓		✓
Reset and IP spoofing	Control channels			✓		
Scanning attacks	Open air interfaces			✓		✓
Security keys exposure	Unencrypted channels			✓		
Semantic information attacks	Subscriber location			✓		✓
Timing attacks	Subscriber location				✓	✓
Boundary attacks	Subscriber location					✓
IMSI catching attacks	Subscriber identity			✓		✓

# 4. 5G 기기와 사용자 보안

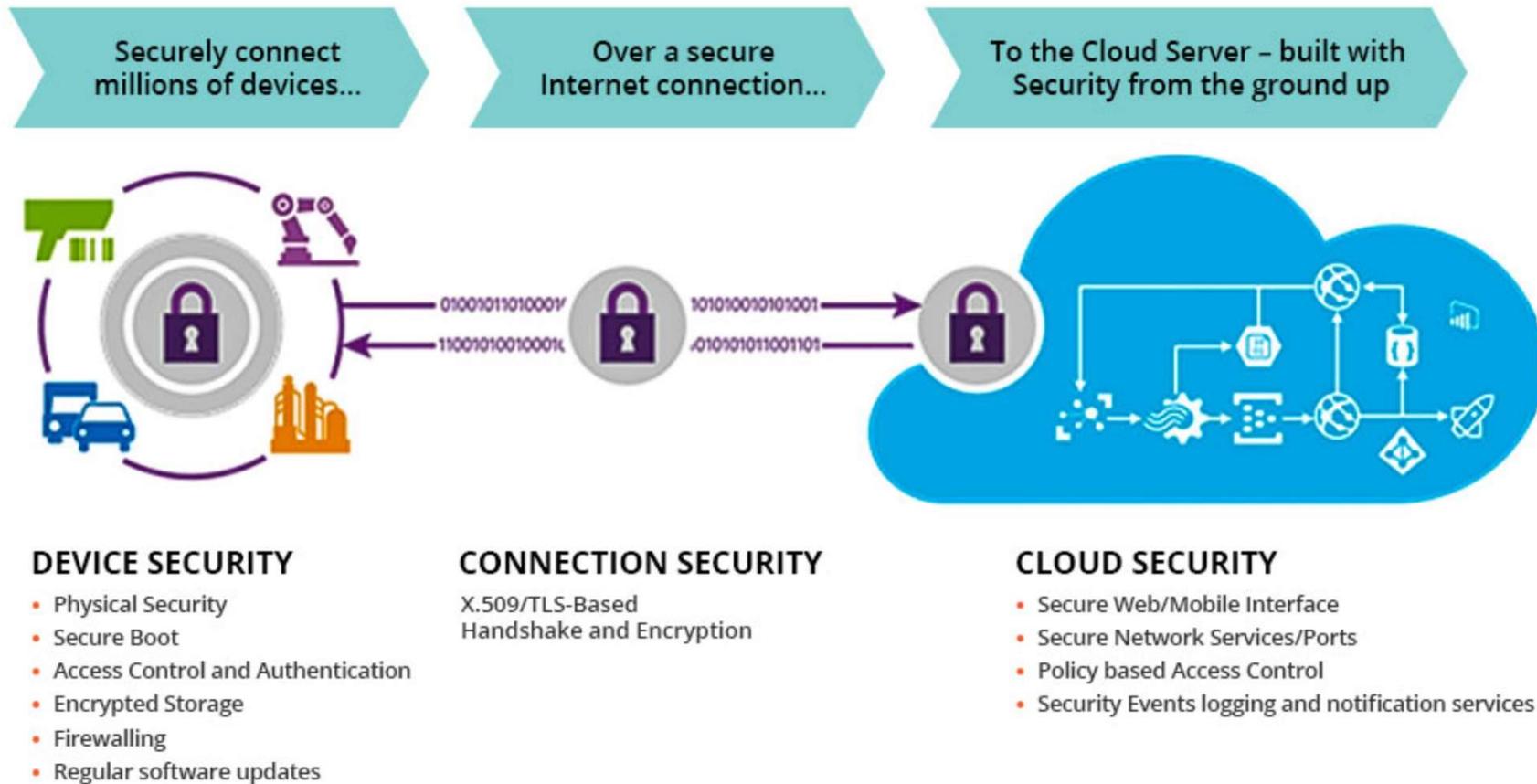
- Some advantages and drawbacks of blockchain usage when compared to traditional data handling.



Area to Consider	Advantage	Drawback
Ledgers	Ledgers as distributed and trusted databases	Mixed usage of private and public blockchains are not clearly solved in practice
Transaction speed	Accelerated transactions when compared to industrial bulk commissioning	Number of transactions are still less than 100 per second
Transaction as event logging	Possibility of micropayments	Limitations for resource constrained devices
Security	Advanced, inherited security Trust Data Privacy Confidentiality, Integrity, Availability	Security vulnerabilities, such as 51% attack race attack, finney attack, bugs in Smart Contracts are not patchable
Leaving out third parties	Anonymity Cost reductions by removing middlemen	Legal issues are not easy to solve

# 4. 5G 기기와 사용자 보안

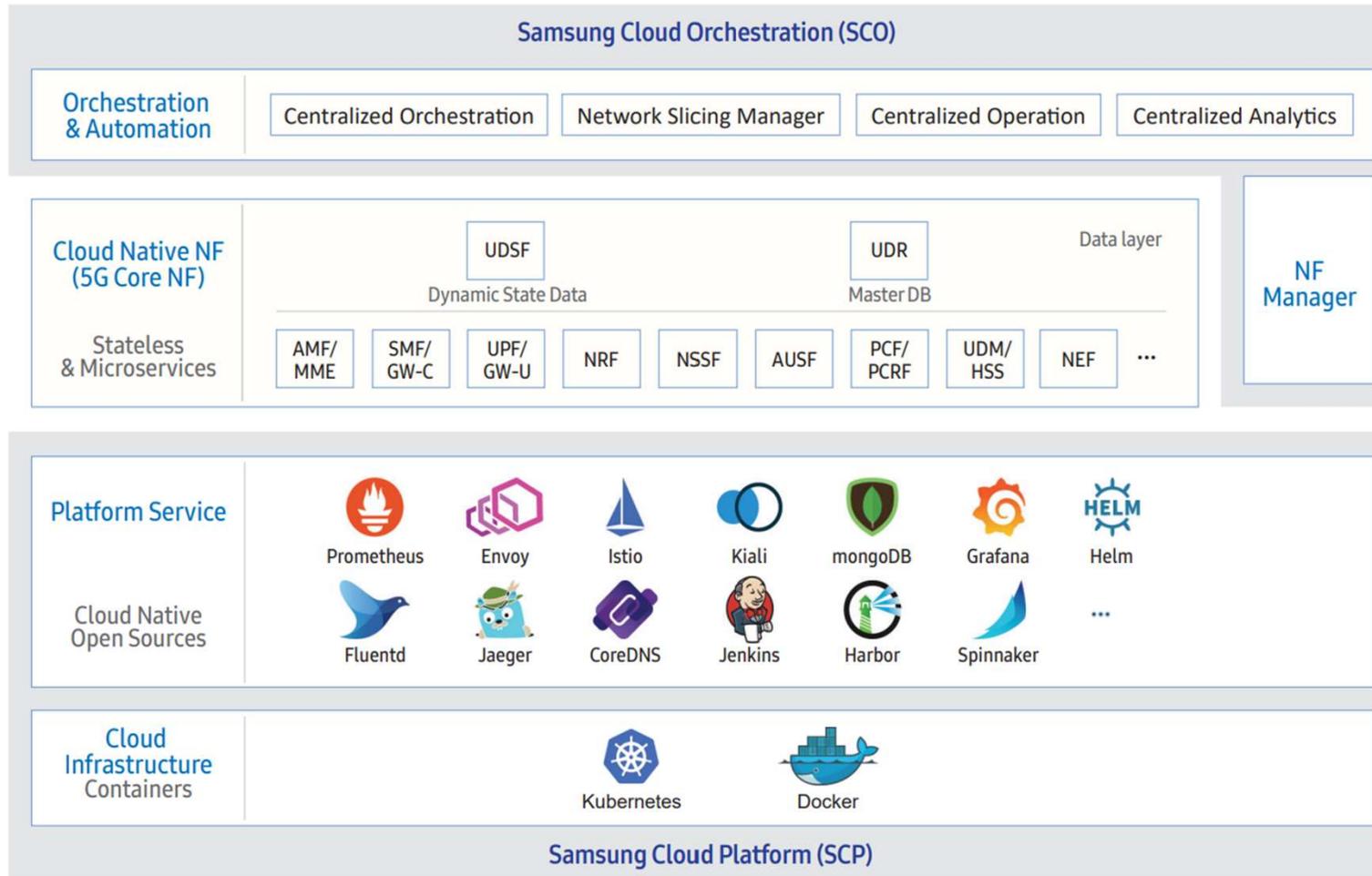
## □ System owner: Define End-to-End security



1. 5G 개요
2. 5G 보안 개요
3. 5G 네트워크 보안
4. 5G 기기와 사용자 보안
- 5. 5G 클라우드와 가상네트워크 보안**

# 5. 5G 클라우드와 가상네트워크 보안

## Cloud Native 5G Core

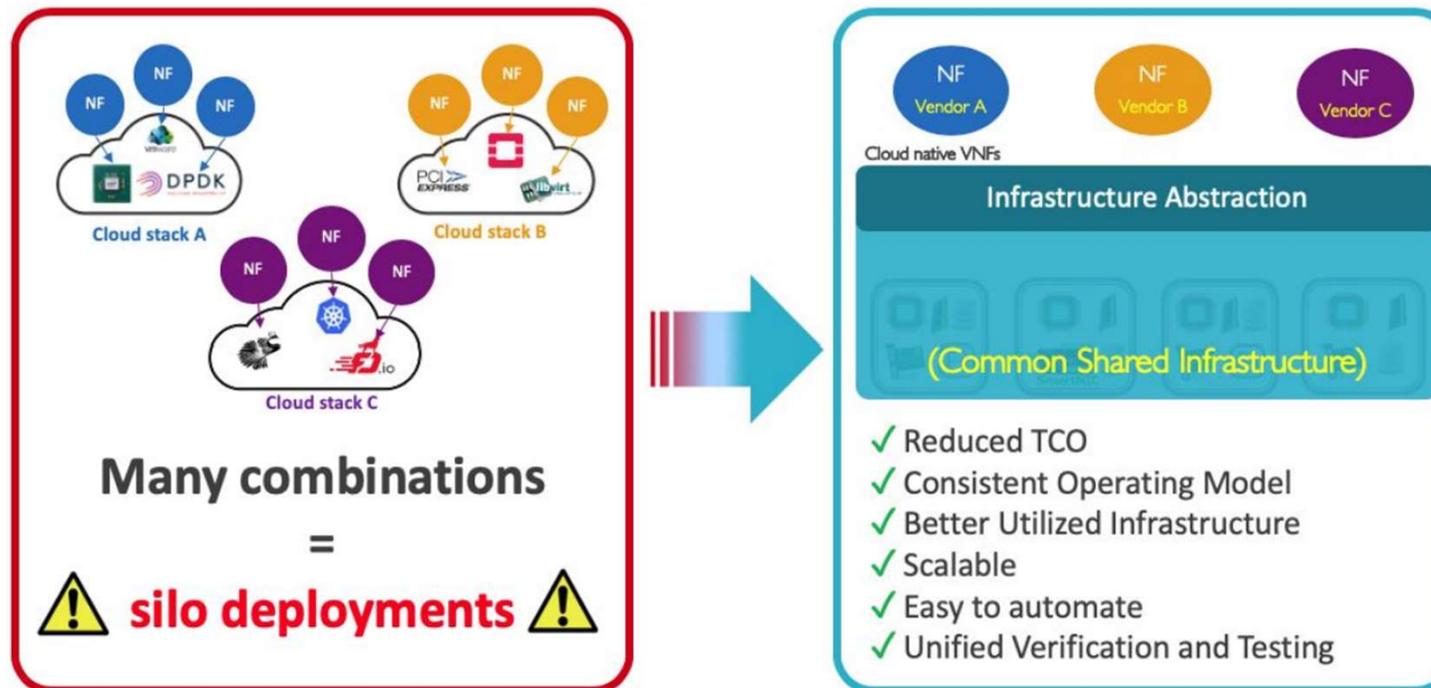


Samsung 5G Core's Cloud Native Enabled Architecture

# 5. 5G 클라우드와 가상네트워크 보안

- Cloud iNfrastructure Telco Taskforce (CNTT)
- CNTT Problem Statement

## LF NETWORKING



#5G, #Cloud Native, #CNTT, #Edge, #OPNFV, #Publications, #Resources

# 5. 5G 클라우드와 가상네트워크 보안

---

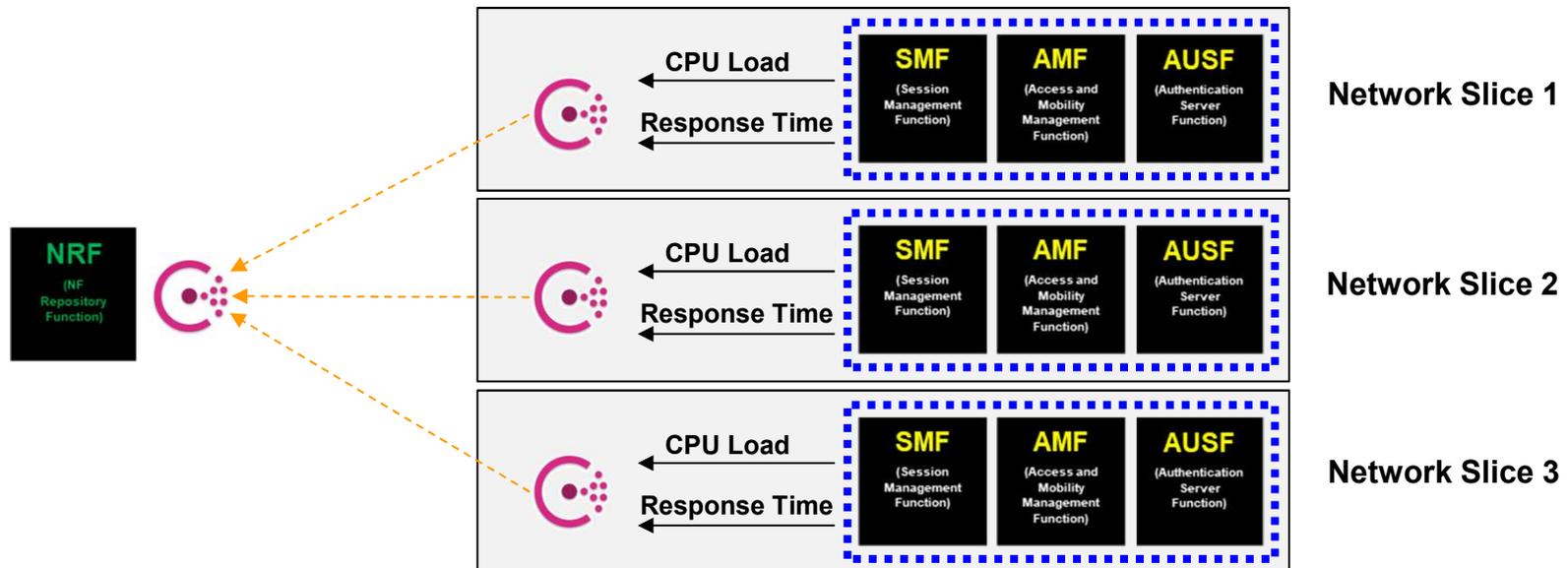
## □ CNTT Reference Model

- Compute
- Storage
- Network
- Acceleration
- Application programming interface (API)
- Multi-tenancy
- Operations and lifecycle management (LCM)
- **Security**
- **Platform and access**
- **Confidentiality and integrity**
- **Workload security**
- **Image security**
- **Security life cycle management**
- **Monitoring and security audit**
- **Standards compliance**

# 5. 5G 클라우드와 가상네트워크 보안

## □ Service Mesh

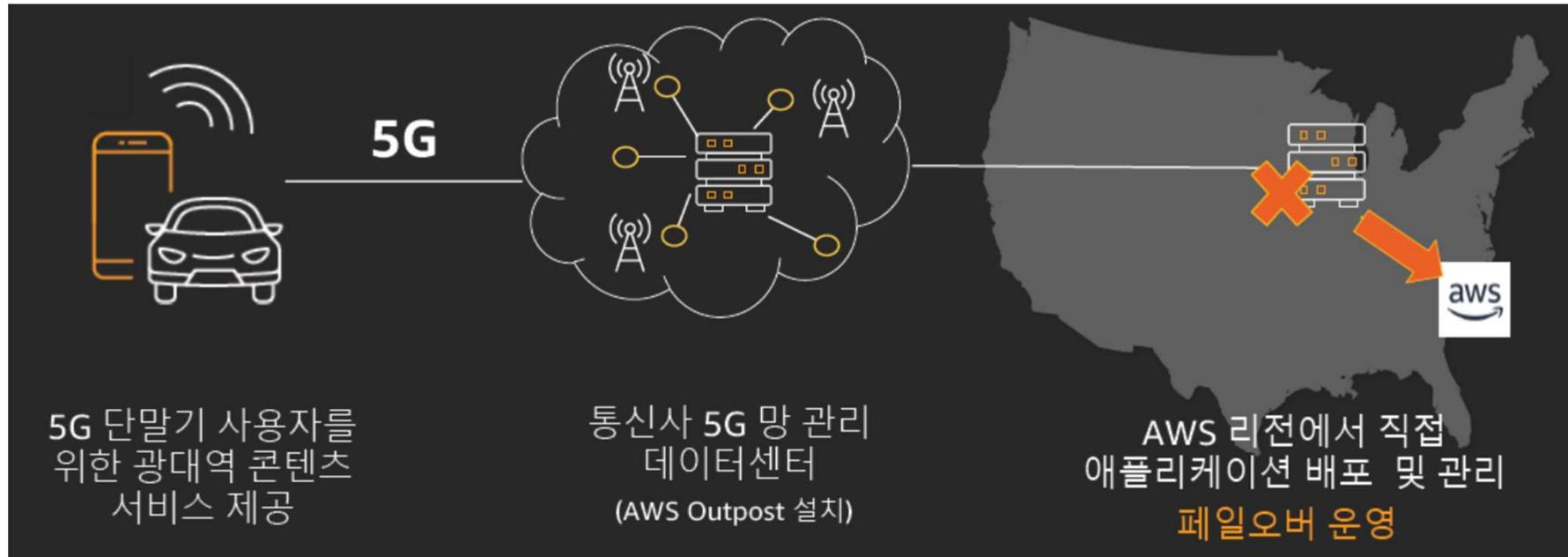
- Management 부가 기능: Consul Cluster (HashiCorp)
- Management Trend 고려: Service Mesh (Istio)



# 5. 5G 클라우드와 가상네트워크 보안

## □ Amazon AWS Wavelength

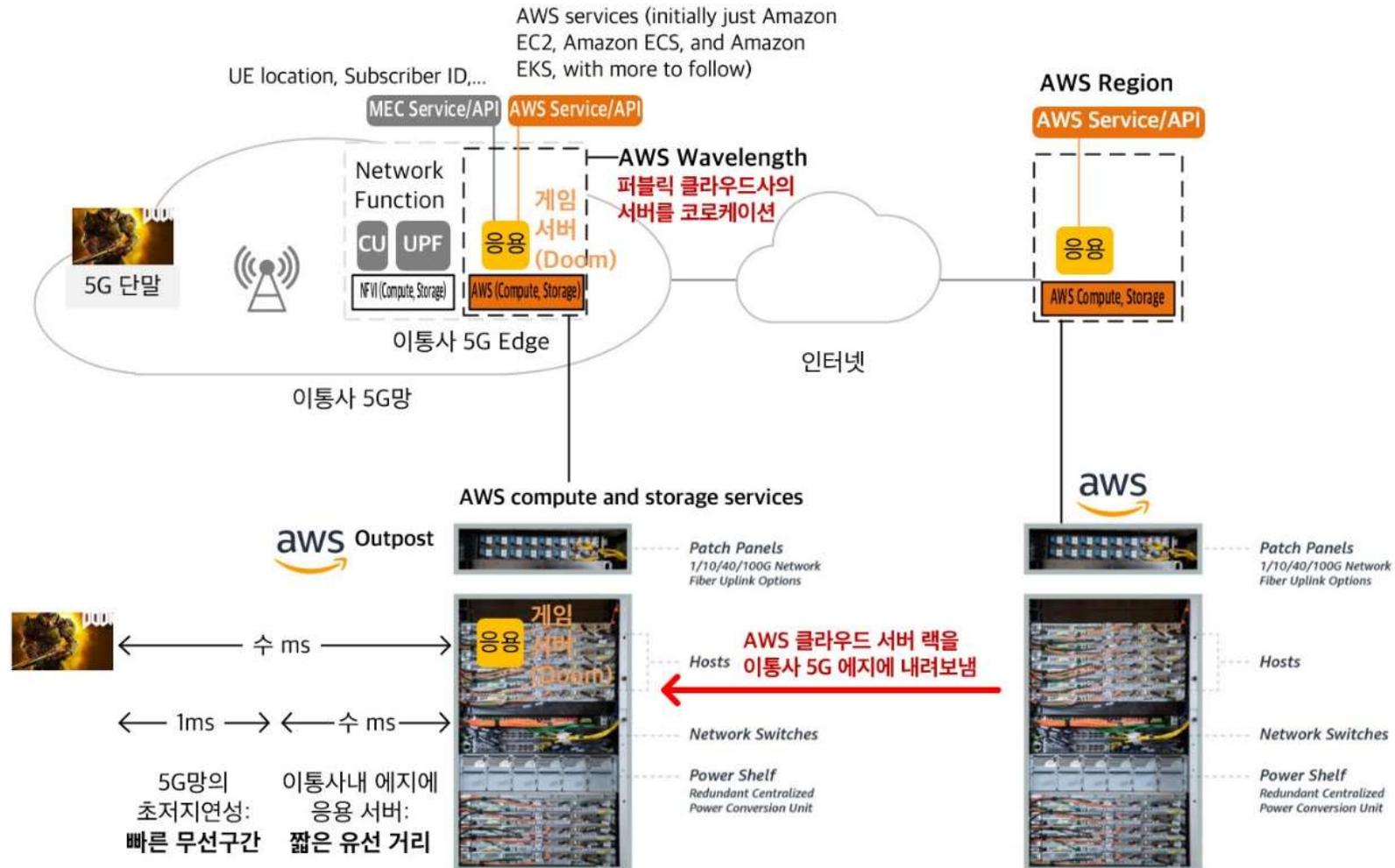
- 5G 네트워크 에지에서 AWS 컴퓨팅 및 스토리지를 사용하여, 5G 기반 모바일 기기 및 사용자에게 초저지연 서비스를 제공하는 애플리케이션 제공 가능 (AWS Outpost 기반)
- AWS 리전과 통신사 5G 망을 직접연결
- 로컬 컴퓨팅, 스토리지, 데이터베이스 및 기타 서비스제공
- 5G 기반 새로운 모바일 앱 제공



출처: AWS re:Invent 2019

# 5. 5G 클라우드와 가상네트워크 보안

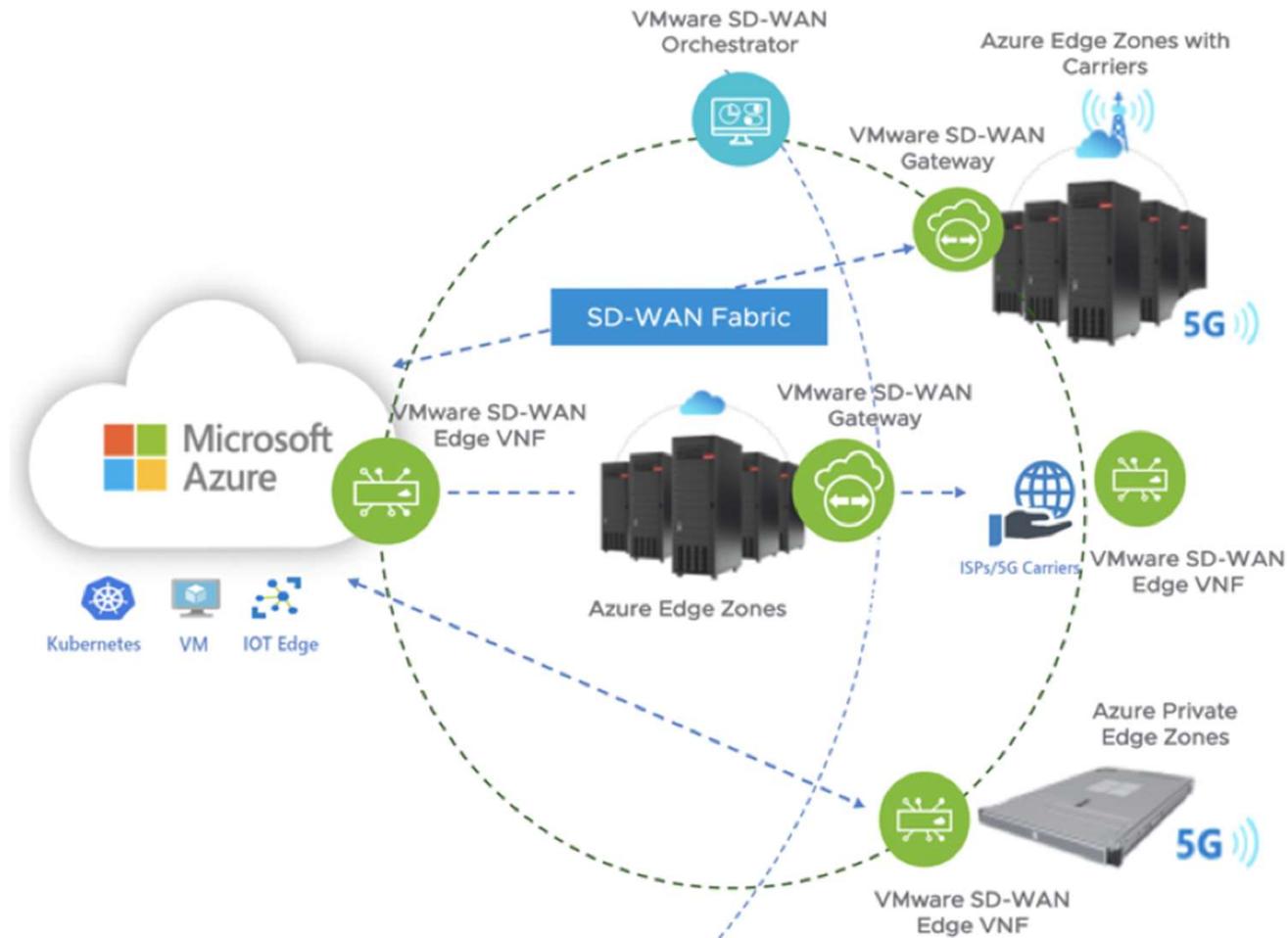
## Amazon AWS Wavelength



출처: <https://www.netmanias.com/ko/post/blog/14591/5g-edge-iot-mec/aws-wavelength>

# 5. 5G 클라우드와 가상네트워크 보안

- Microsoft Azure Edge Zones: 5G 통신사와 연결하여 기업에 설치하는 사설망 구성



출처: <https://blogs.vmware.com/velocloud/2020/03/31/vmware-to-deliver-networking-solutions-with-azure-edge-zones/>

# 5. 5G 클라우드와 가상네트워크 보안

## □ 5G의 AI 응용 (예)

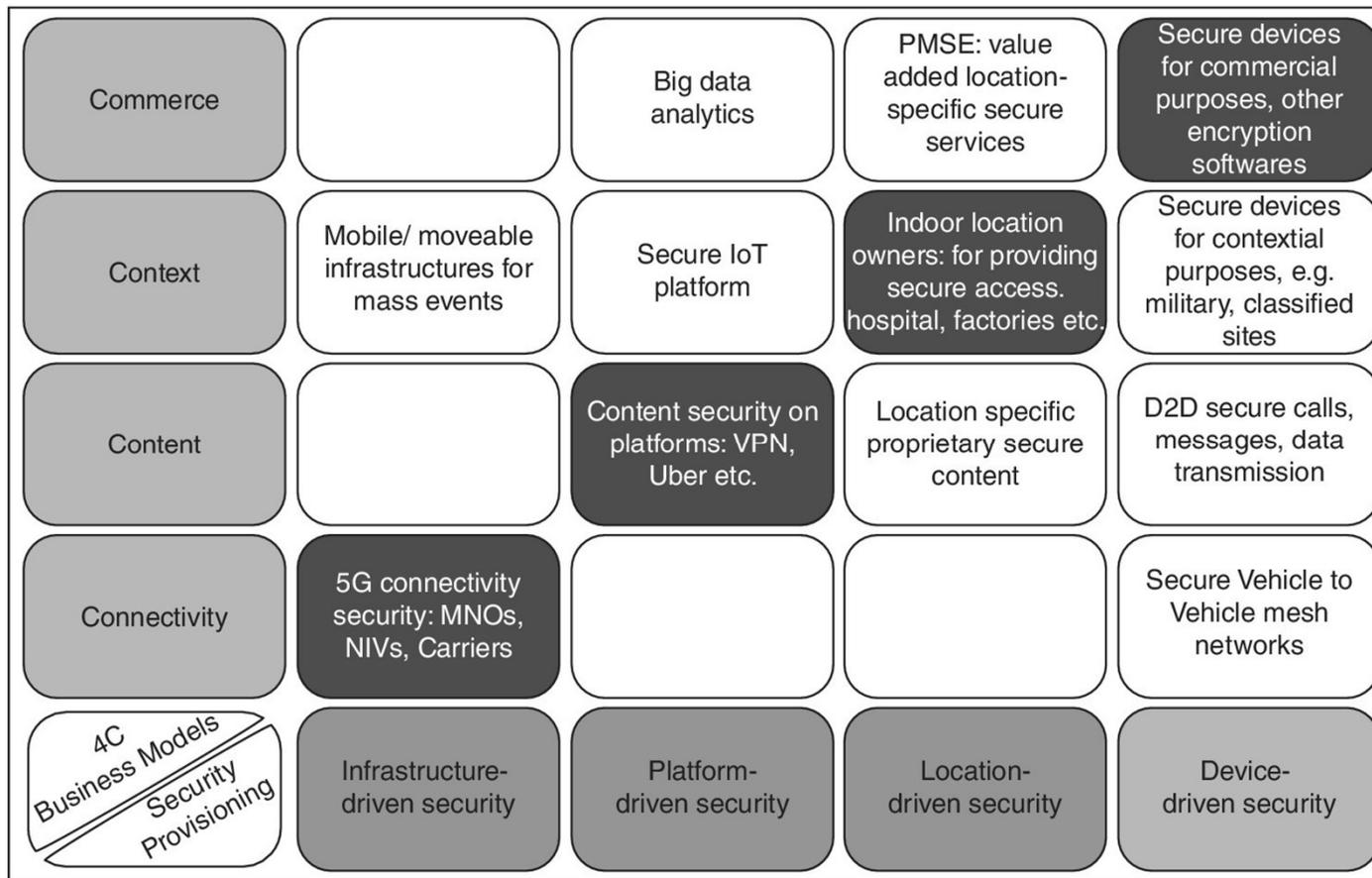
- 서비스 관리 : operations support systems, resource provisioning, fault localization, failure root cause analysis, business support systems, security;
- 네트워크와 클라우드 자원 관리: flexible function deployment, NFV orchestration, network slicing, green operation
- 무선 관리: air interface coordination, site collaboration, user mobility

Comparison shopping of vision API providers (as of Aug. 2019)

	Algorithmia	Amazon Rekognition	Clarifai	Microsoft Cognitive Services	Google Cloud Vision	IBM Watson Visual Recognition
Image classification	✓	✓	✓	✓	✓	✓
Image detection	✓	✓		✓	✓	
OCR	✓	✓		✓	✓	
Face recognition	✓	✓		✓		
Emotion	✓		✓	✓	✓	
Logo recognition			✓	✓	✓	
Landmark recognition			✓	✓	✓	✓
Celebrity	✓	✓	✓	✓	✓	✓
Multilingual tagging			✓			
Image description				✓		
Handwriting				✓	✓	
Thumbnail generation	✓			✓	✓	
Content moderation	✓	✓	✓	✓	✓	
Custom classification training			✓	✓	✓	✓
Custom detector training				✓	✓	
Mobile custom models			✓	✓	✓	
Free tier	5,000 requests per month	1,000 requests per month	7,500			

# 5. 5G 클라우드와 가상네트워크 보안

## 5G의 사이버 보안 비즈니스 모델



A Comprehensive Guide to 5G Security by Andrei Gurtov; Madhusanka Liyanage; Ahmed Bux Abro; Mika Ylianttila; Ijaz Ahmad Published by Wiley, 2018

