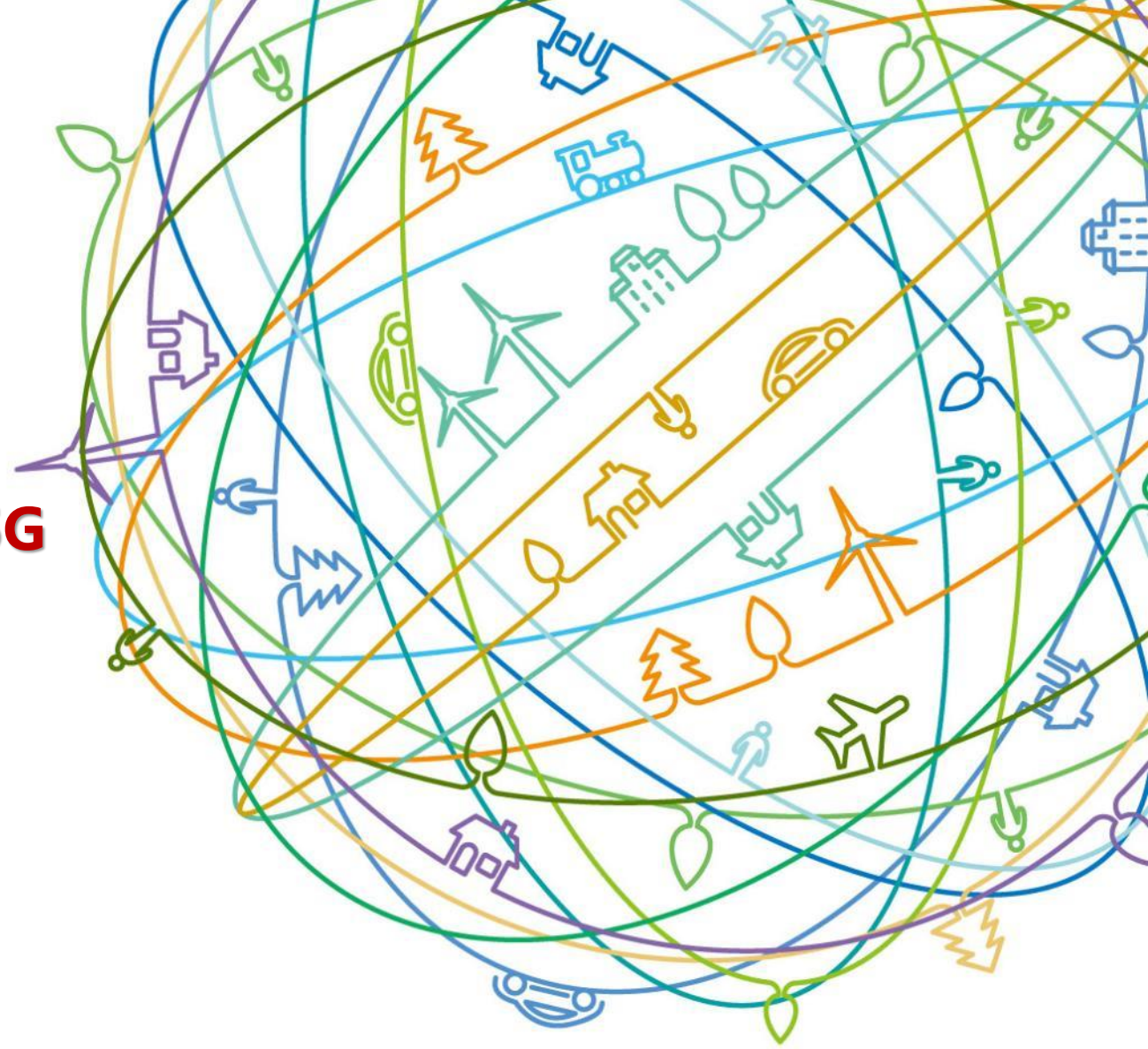
Evoluzione della rete mobile verso il 5G



HUAWEI

Contenuti

01 Introduzione Huawei

02 Trasformazione Digitale
E sicurezza

03 Evoluzione delle reti verso
il 5G

Huawei: Primario Costruttore Mondiale di Infrastrutture ICT e Terminali Intelligenti

Portare il Digitale ad ogni persona, casa ed organizzazione per un mondo totalmente connesso ed intelligente

Il portafoglio prodotti di Huawei si estende a tutta la filiera del settore Telecomunicazioni, solutioni e servizi competitivi e securi. Attraverso la collaborazione reciproca ed aperta con I nostril partners, creiamo valore costante nel tempo, lavoriamo per sostenere la crescita delle persone, arricchire la vita delle famiglie e della società ed ispirare l'innovazione nelle organizzazioni di ogni forma e dimensione.

In Huawei, l'innovazione si concentra sui bisogni dei nostril Clienti. Facciamo rilevanti investimenti nella ricerca di base, ci concentriamo sulle innovazioni tecnologiche che muovono Avanti il mondo.

188,000

Impiegati

80,000+

Ricercatori

14 Centri R&S di cui

8 in Europa, 1 in Italia

170+

Paesi

68

Più conosciuti
TOP 100 Brand

72

Classifica

Fortune 500

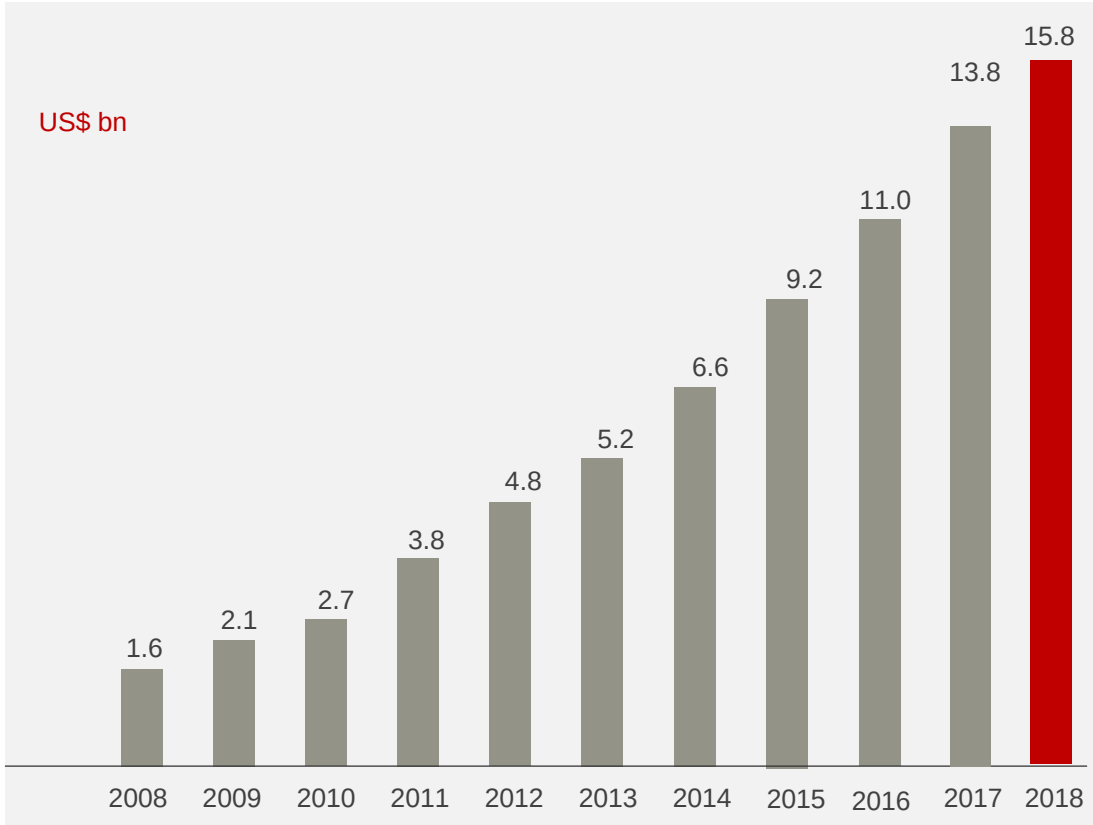
105,2

Fatturato mondiale

In B$

HUAWEI

Sustained Investment in R&D Drives Technology Breakthroughs



70 Miliardi USD Investimenti in R&S negli ultimi 10 anni

Nel 2018 occupa il 5 posto nella classifica globale dei maggiori investitori in R&S

- Concentrazione della R&S sulle aree strategiche
- Il 15% circa del fatturato reinvestito ogni anno in R&S
- Azienda maggiormente innovative al mondo
- **87,805 Brevetti totali di cui: 43,371 autorizzati in Cina e 44,434 autorizzati fuori dalla Cina.**
- Membro e Presidenza di 400+ comitati di standardizzazione a livello mondiale; partecipazioni industriali, e comunità open source con 400+ posizioni apicali; 5,000+ proposte depositate nel corso del 2018 e 60,000+ in totale.

HUAWEI

Huawei in Italia

800+ Impiegati

85% Locali

Programmi Future Seed per gli studenti delle università italiane

Rome + Milan 2 HQ

1 Centro R&S per Ponti Radio e onde millimetriche

4 Centri per l'innovazione:

Telecommunication, networking, core network, smart city

1 Business Innovation Center

2018 Ricavi

1.67B Euro

2018 Acquisti e investimenti

453M Euro

2020-2023 investimenti in Italia

3 Miliardi Dollari

HUAWEI

Contents

01 Introduzione Huawei

02 Trasformazione Digitale E sicurezza

03 Evoluzione delle reti verso il 5G

La Digital Economy è il nuovo modello di crescita.

Germania: Industria 4.0, Strategia Digitale 2025

ITALIA: prima ad avere lanciato il trial 5G e stimolato lo sviluppo dell'ecosistema

UK: Strategie per l'Economia Digitale

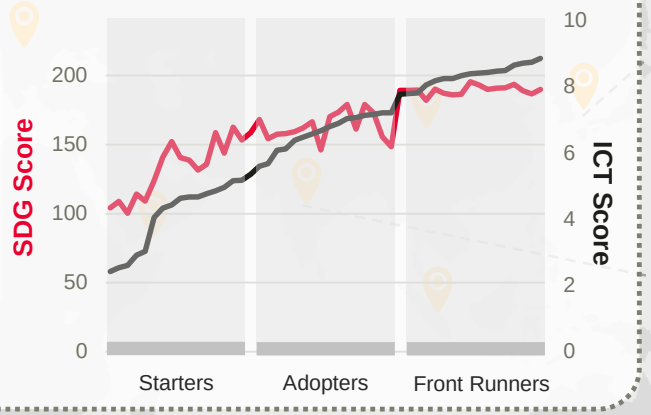
Russia: Strategia per l'Economia Digitale

Cina: Cina Digitale, Made in China 2025, Internet+

Canada: Canada Digitale 150

- 20% investimenti in ICT = 1% PIL
- Ritorno dell'investimento in ICT è 6.7x maggiore di quello non ICT
- La crescita dell'Economia Digitale è 2.5x volte più veloce dell'economia tradizionale

ICT è un indicatore chiave di sostenibilità (correlazione al 90%)



Giappone: White Paper su industrie manifatturiere
Corea del Sud: Industria manifatturiera Innovazione 3.0

Stati Uniti: Strategie per il primato americano nell'industria manifatturiera avanzata, Industrializzazione di Internet

India: "Made in India" e "India Digitale" per il futuro

Brasile: Brasile Efficiente

Saudi Arabia: "Visione al 2030"
Trasformazione Digitale per la crescita

Singapore: Nazione Intelligente 2025
Tailandia 4.0
Malesia Digitale

Australia: Strategie per l'Economia digitale

156 Nazioni al mondo hanno ufficializzato piani per la trasformazione Digitale(ITU)

HUAWEI

4th Rivoluzione Industriale

La Tecnologia influenzerà la direzione dello sviluppo socio-economico

1st Rivoluzione Industriale	2nd Rivoluzione Industriale	3rd Rivoluzione Industriale	4th Rivoluzione Industriale
			
Potenza Vapore	Elettricità	Tecnologie IT	Tecnologie Intelligenti

Macro Tendenze Globali

- Sostenibilità
- Nuovo impulso alla crescita
- Città intelligenti e sicure
- Trasformazione Digitale del sistema
- Migliore Efficienza
- Nuove soluzioni

Contents

01 Introduzione Huawei

02 Trasformazione Digitale
E sicurezza

03 Evoluzione delle reti verso il 5G

Il 5G è il fattore abilitante di significativi benefici economici e sociali

Impatti socio economici del 5G

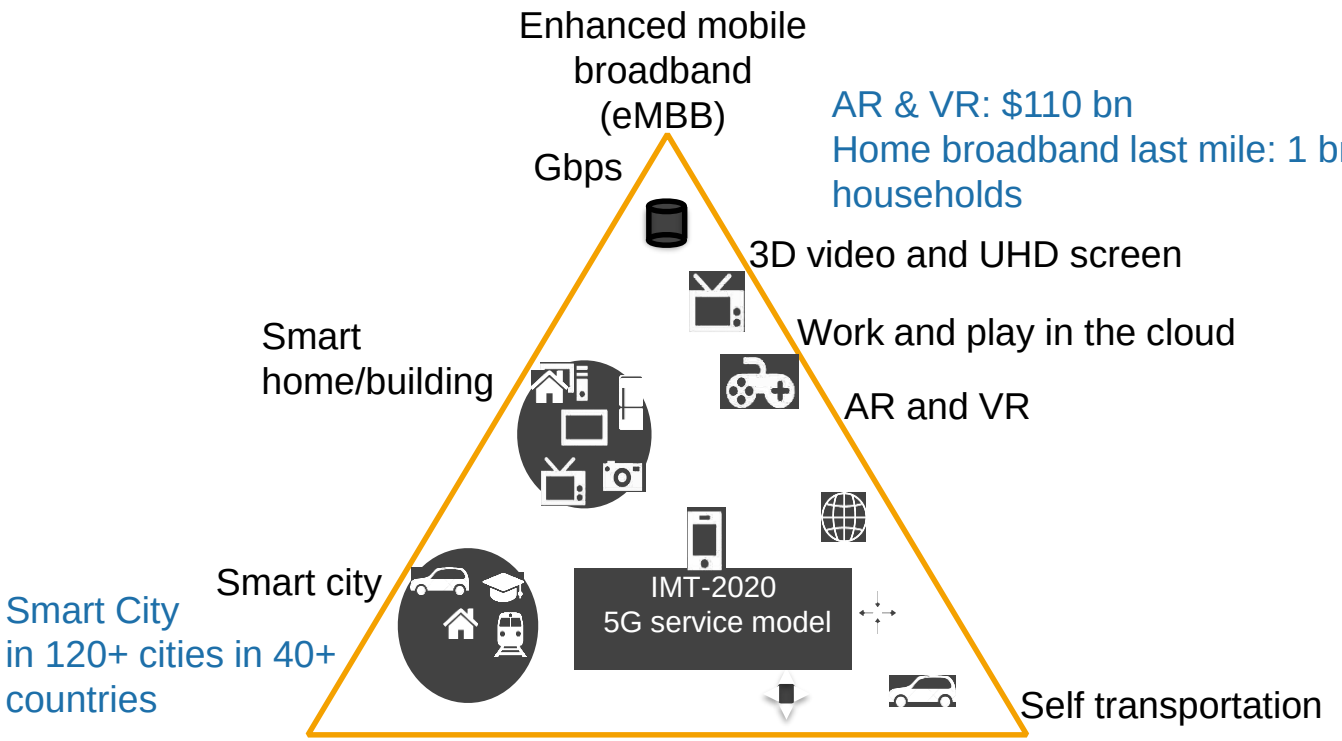
$12.3
trillioni
Economia globale incrementale 2035

$200
miliardi
Investimenti annuali

22
milioni
Posti lavoro nel 2035

0.2%
Crescita mondiale del PIL
2020–2035

Il 5G nasce pensato per abilitare tre grandi aree di sviluppo di nuovi servizi



5G City: dalle connessione tra persone alla connessione delle cose

Safety
Everywhere

Intelligent
Transport

Intelligent
Manufacturing

Smart
Energy

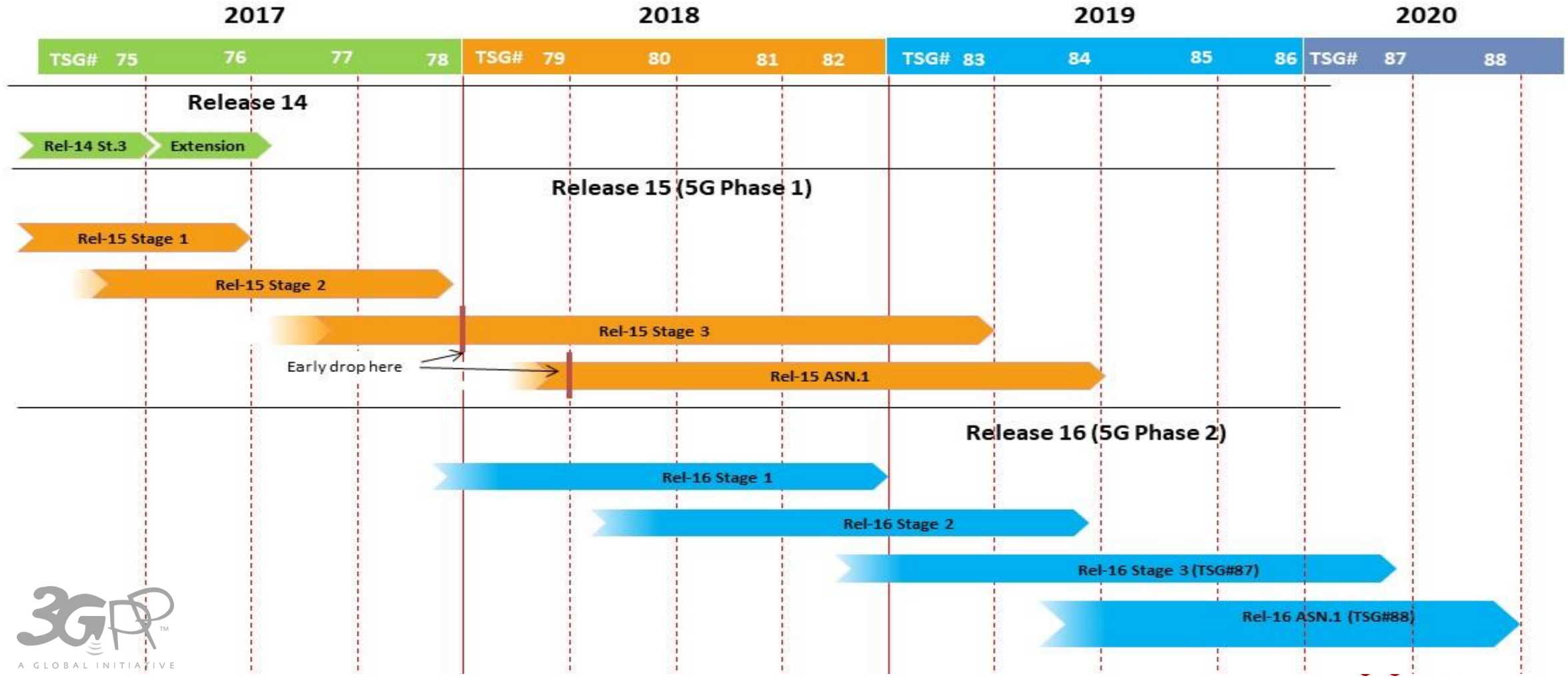
Green
Living

Smart
eHealth

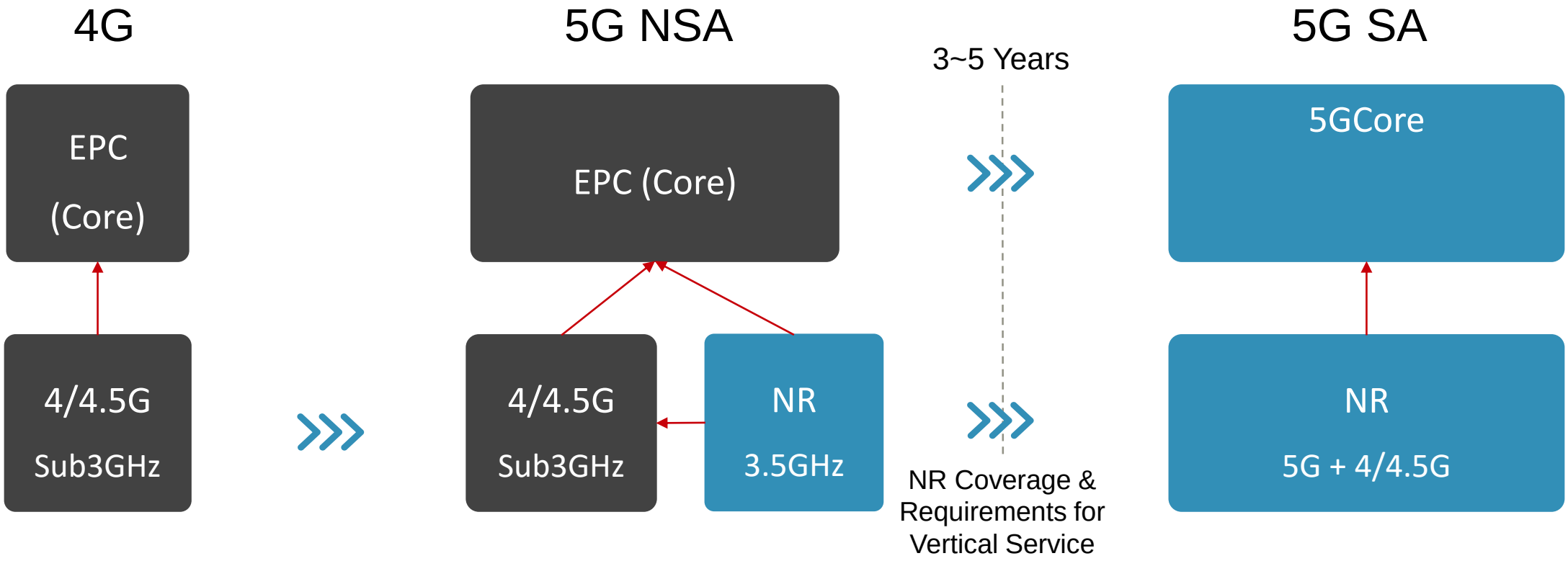
HUAWEI

5G: roadmap della standardizzazione in ambito 3GPP

Il 3GPP e' l'ambito di standardizzazione entro cui sono state sviluppate le tecnologie mobile a partire dalla 3G, 4G, 4.5G e 5G. A questo processo di standardizzazione partecipano la quasi totalita' player del settore: Telco, manifatturieri, enti di ricerca, istituzioni governative etc… Gli standard prodotti hanno ottenuto il totale consenso della comunita' tecnico scentifica internazionale.



Transizione verso il full 5G



NSA:Non-Standalone
SA:Standalone

5GC:5G Core
NR:New Radio

Gli operatori inizieranno ad implementare il 5G usando la versione NSA, che come mostra la figura, si appoggia totalmente alle reti 4 e 4.5 G esistenti e solo successivamente si muoveranno verso la soluzione full 5G stand alone. *Questo implica che tutti gli investimenti finora effettuati sul 4 e 4.5 G possono essere interamente riutilizzati per sviluppare la rete 5G ottimizzando gli investimenti che gli Operatori dovranno fare nella prima fase di sviluppo del 5G*

Security Roadmap del 3GPP

2018 2019 2020 3GPP Release plan

Rel-15	Rel-16	Rel-17+
Meccanismi e funzionalita' di base sono disponibili in questa release	Miglioramenti per I mercati verticali • uRLLC • Ottimizzaizione dei meccanismi di sicurezza per velocita' di trasmissione elevate • Riduzione del ritardo di elaborazione dei processi di sicurezza • Cloud IoT • Meccanismi di sicurezza piu' "leggeri" per dispositive a bassa velocita' e basso consumo • Riduzione dell'overhead informativo legato alla parte di sicurezza	Ulteriori miglioramenti • Algoritmi di crittografia a 256 bit • Meccanismi di autenticazione ancora piu' robusti • Stesso meccanismo di autenticazione per tutti I tipi di servizi • Uso di pseudonimi anziche' l'identificativo dell'utente (SIM)

3GPP Security Standard e' molto avanzato rispetto allo stato del mercato

Vertical Market

2018 2019 2020 ..... 2023 ..... 2025+

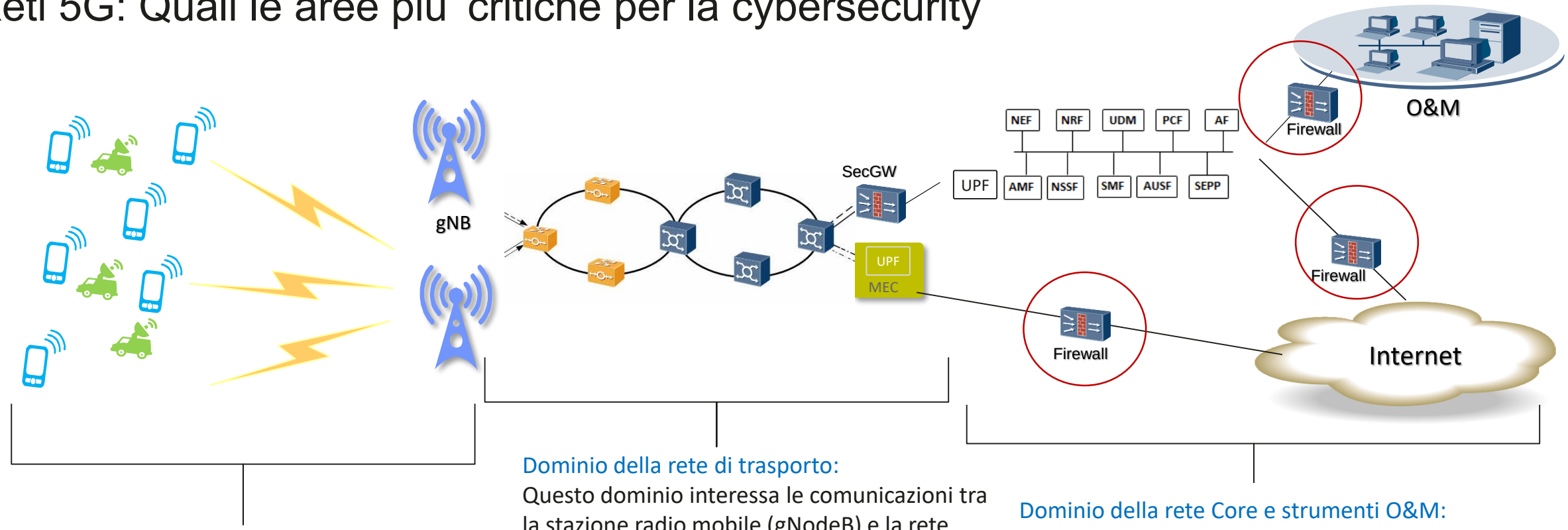
Deployment plan

eMBB

uRLLC

HUAWEI

Reti 5G: Quali le aree piu' critiche per la cybersecurity



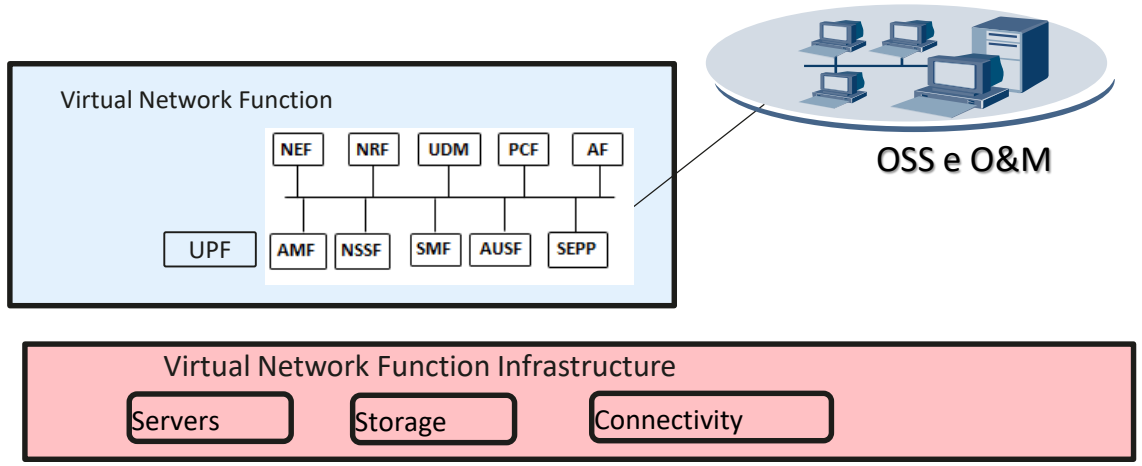
Dominio della rete di accesso:
In questo dominio le comunicazioni risultano prottete da sistemi di crittografia tra la stazione radio mobile (gNodeB) e i terminali utenti.
Il rischio associato ad una potenziale vulnerabilita' e' percio' ridotto, cosi' come ridotto sarebbe l'impatto in termini di numero di utenti o sull'integrita' di rete.

Dominio della rete di trasporto:
Questo dominio interessa le comunicazioni tra la stazione radio mobile (gNodeB) e la rete Core.
Normalmente gli Operatori utilizzano sistemi di protezione che impiegano chiavi crittografiche gestite dall'Operatore stesso (Ipsec tunnel).
Quindi in questo dominio la probabilita' di un attacco e' molto ridotta.

Dominio della rete Core e strumenti O&M:
Questo dominio interessa la parte delle funzioni centrali (Core) della rete nonche' degli strumenti quali sistemi di gestione, strumenti per la diagnostica di rete, la gestione della configurazione, la raccolta dei dati prestazionali.
Nella slide sucessiva approfondiremo le ragioni che portano a considerare questa area come la piu' critica dal punto di vista della cybersecurity

Gli operatori utilizzano sistemi di protezione (Firewall), per prevenire, identificare e mitigare attacchi alla rete core provenienti dalla rete Internet pubblica.

Rete Core 5G



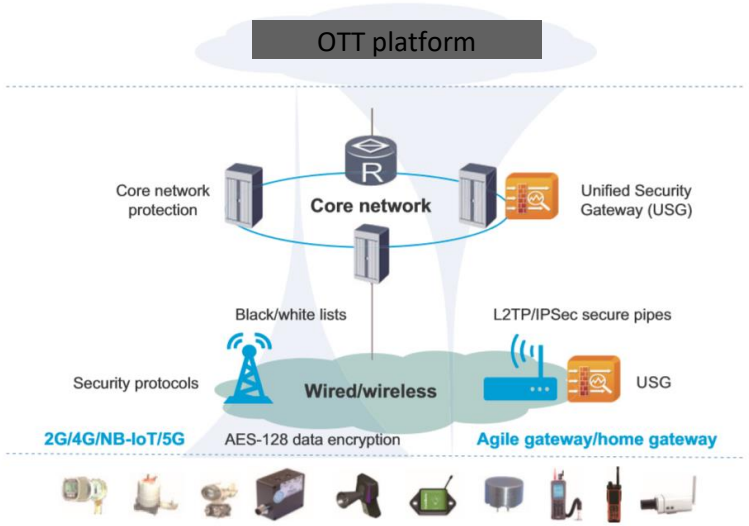
La rete 5G Core e' basata su architettura "Cloud", cioe' e' suddivisa su due livelli:

1. Livello infrastrutturale (VNFI) che fornisce la piattaforma hardware formata dai server, lo storage e la connettvita' di rete IP
2. Il livello delle Funzioni Virtuali di Rete (VNF), puro software , che realizzano le diverse funzionalita' definite in ambito di standardizzazione per la rete core 5G

Le motivazioni per cui queste componenti della rete 5G sono a piu' alto rischio sono riassunte qui di seguito:

- I potenziali punti di attacco da parte degli hackers sono molteplici considerate la numerosita' delle interfacce coinvolte e per il numero di componenti hardware e software coinvolti. Pertanto, in caso di attacco alla rete Core, il numero potenziale degli utenti che sarebbero impattati (data l' interruzione di servizio) potrebbe essere molto alto e potrebbe essere compromessa l'integrita' della rete stessa
- La violazione o intrusione, esterna o interna, alla rete Core su uno o più elementi di rete potrebbe estendersi a tutti i collegamenti attivi nella rete stessa, qualunque sia la tecnologia in collegamento (smartphone, sensori IoT, auto a guida autonoma, etc…), catturandone i contenuti della comunicazione;
- Quanto sopra riportato, inoltre, a causa dell'evoluzione dell'architettura delle reti Core 5G che saranno sempre piu' distribuite, tendera' a spostarsi verso i nodi fisici periferici di accesso della rete. Questo avra' l'effetto di rendere la rete Core ancora piu' vulnerabile non solo da un punto di vista logico, come detto in precedenza, ma anche da un punto di vista fisico dato che la numerosità dei nodi di accesso alla rete conseguenti alla distribuzione degli accessi, aumenteranno la vulnerabilità della rete.
- Le motivazioni per cui si ritiene che i sistemi di supervisione OSS e gli strumenti di O&M (Esercizio e Manutenzione), siano a piu' alto rischio sono analoghi a quelli presentati per gli elementi del Core.

Ruoli e responsabilita’ nello sviluppo di soluzioni E2E



Operatori TLC

Il ruolo degli Operatori:
Si focalizza sulla Progettazione della Rete, Connessioni e Servizi
Responsabili esercizio e sicurezza
Posseggono e controllano I dati essenzialmente degli end user
Titolari delle chiavi di criptazione dei dati relativamente al trasporto IP

Vendors

Il ruolo dei Vendor:
Forniscono gli apparati di rete

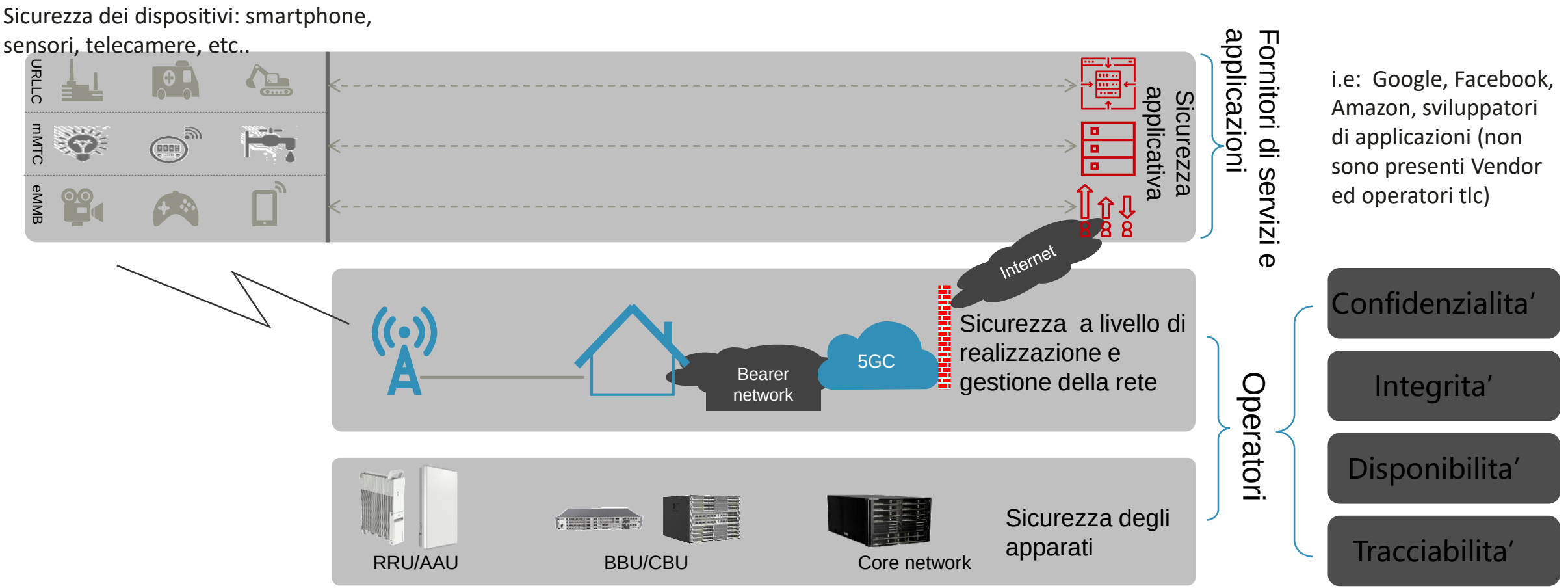
Non possiedono i dati
Non operano la rete
Non possiedono chiavi decriptaz.

OTT (Over the Top*)

Il ruolo degli OTT:
Posseggono le applicazioni online dove la maggior parte dei dati dell’utenza sono raccolti e salvati
Posseggono e controllano I dati
Eseguono profilazione dei dati
Hanno chiavi di criptazione sofisticate per proteggere i contenuti

(*) Amazon, Google, Netflix, Facebook

La cybersecurity non riguarda solo le reti 5G ma coinvolge l'intera filiera



- Confidenzialita' e integrita' : Protezione delle informazioni private degli utenti (anagrafica, localizzazione, etc.), dei dati degli utenti e delle informazioni chiave detenute dall'operatore (dati statistici,cartellini di traffico and etc.)
- Disponibilita' della rete: identificazione dei potenziale attacchi e mitigazione degli impatti sui servizi di rete
- Tracciabilita': Registrazione degli interventi effettuati dal personale sugli apparati di rete

Sicurezza degli apparati di rete: Huawei realizza un Sistema di verifica multi livello con piu’ enti indipendenti

Tutti gli interventi garantiscono l’aggiornamento dei processi, degli standard utilizzati e delle policy Huawei e, viene conseguentemente applicato a tutti i prodotti e servizi tramite un “circolo virtuoso”

Processo di sviluppo integrato del Prodotto (IPD)

Concept | Plan | Development | Qualify | Launch | Lifecycle

Penetration Test indipendente

ICSL (HQ)

Compliance Test indipendente

Bruxelles

Centro di Cyber Security Europeo

Test da parte di Clienti e terze parti

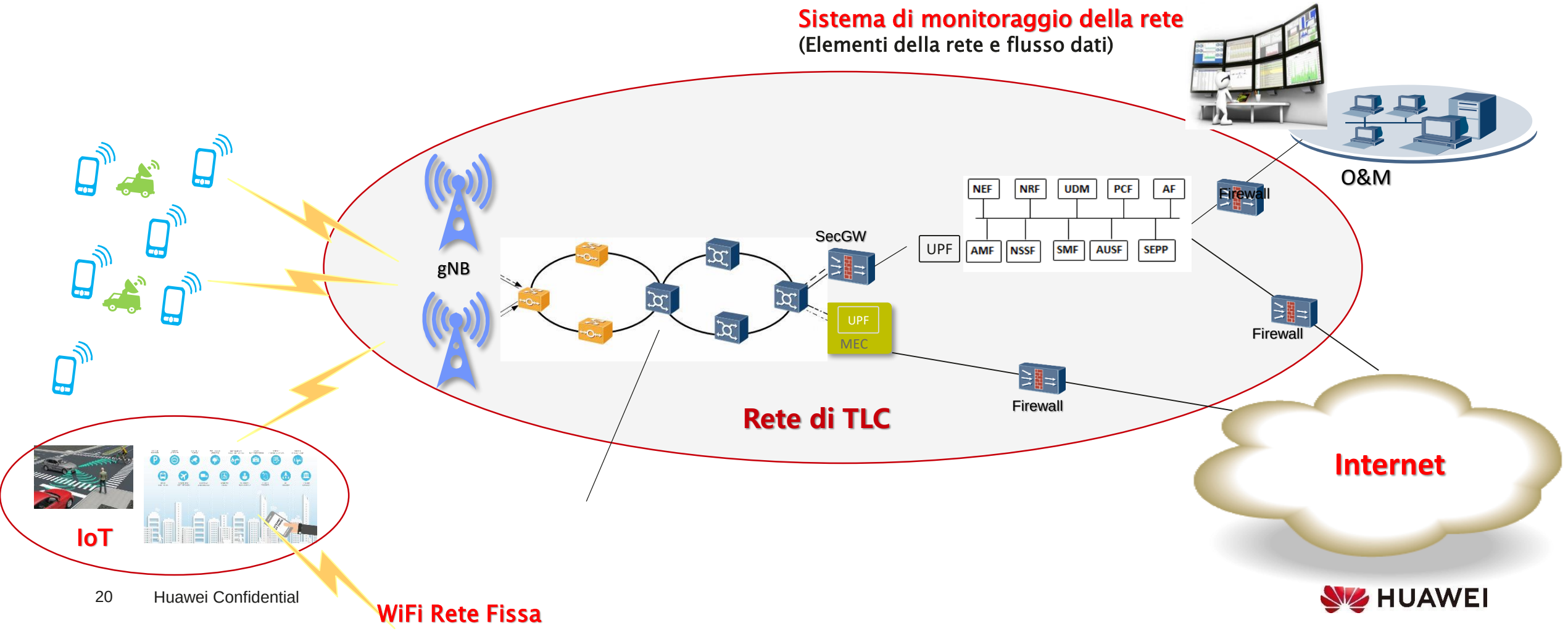
Certificazioni industriali

Communication, Innovation and Verification




I rischi globali su cui progettare la sicurezza

Nel mondo Globale interconnesso, le reti 5G sono solo una parte del rischio sicurezza. Spesso, erroneamente, si associa Internet alle reti di Telecomunicazioni trascurando il ruolo degli OTT, ma ancora più spesso si ignora la filiera globale delle TLC che vede un utilizzo condiviso di brevetti e tecnologie tra tutti i vendor. Questo implica che la Sicurezza della rete gestita da tutti gli operatori Europei e non, deve essere globale.



HUAWEI

Thank you.

Bring digital to every person, home, and organization for a fully connected, intelligent world.

HUAWEI

Punti salienti dell'audizione

1. **Il 5G è il fattore abilitante per la trasformazione digitale ma ha bisogno di un ecosistema più ampio per esprimere tutte le sue potenzialità.**

2. **Il 5G si appoggerà alle reti 4G e 4.5G già esistenti, il che permetterà agli operatori di ottimizzare i loro investimenti.**

3. **Nel mondo interconnesso, la cyber security è una questione globale che riguarda l'intero ecosistema.**

4. **Tutti gli standard delle reti TLC mobili, ivi inclusi quelli di sicurezza, sono definiti per tutto il mondo delle TLC da comitati internazionali partecipati da operatori, vendor e Istituzioni governative (in particolare il 3GPP, la GSMA, ITU e IETF). Cosa che non accade nel mondo degli OTT.**

5. **La sicurezza è incrementale. Ogni nuova tecnologia ingloba tutti i livelli di sicurezza che avevano i precedenti sistemi.**

6. **Una eventuale emarginazione dei Vendor cinesi dal mercato UE, ha stimato la GSMA, costerebbe agli operatori circa 55 miliardi di euro.**

7. **Il quadro normativo sul Golden Power che va delineandosi, rischia di mettere Huawei in una posizione di difficoltà tale da discriminarla dalla competizione.**

Audizione di Huawei Italia
presso la IX Commissione Trasporti, Poste e Telecomunicazioni della Camera dei deputati.
Indagine conoscitiva sulle nuove tecnologie delle telecomunicazioni, con particolare riguardo alla transizione verso il 5G ed alla gestione dei big data.
Roma, 17 luglio 2019

La transizione al 5G e le strategie per la sicurezza

Nel mondo globale interconnesso, le reti 5G sono solo una parte dell'intero sistema di Comunicazioni a rischio sicurezza. Spesso, erroneamente, si associa il mondo Internet a quello delle reti di Telecomunicazioni (2G, 3G, 4G, 5G), confinando il mondo del WEB ad una tecnologia di rete, ma dove il ruolo degli Over The Top (OTT-Google, Facebook, Amazon) è primario e determinante nella gestione dei dati.

Ancora più spesso si ignora il fatto che la filiera delle Telecomunicazioni è globale ed è usuale un utilizzo condiviso di brevetti e tecnologie per le quali ciascun Vendor, a fronte del pagamento di opportune licenze d'uso (royalties), può integrarle nelle proprie architetture. Questo aspetto non trascurabile estende il programma di Sicurezza e protezione dei dati a tutti i fornitori di apparati di rete indipendentemente dalla loro provenienza geografica ed implica che la Sicurezza, gestita direttamente da tutti gli operatori Europei e non, deve essere globale.

La Posizione di Huawei

Sulla base della posizione di leadership di Huawei nelle reti di nuova generazione (circa 2 anni di vantaggio competitivo sulla R&S della tecnologia 5G rispetto a tutti gli altri vendor), ma anche sulla base della share che ha acquisito nelle reti 4G, la presenza di Huawei è fondamentale sia per contenere i costi del passaggio al 5G, sia nell'accelerare la trasformazione digitale in Italia consentendo di recuperare e superare il gap esistente con altri paesi.

Proprio in questa direzione Huawei intende promuovere ogni possibile iniziativa per agevolarla.

Sulla base di quanto sopra, Huawei ritiene necessario armonizzare anche il quadro

normativo in tema di Golden Power, al fine di assicurare le stesse condizioni commerciali a tutti i fornitori ed evitare un ritardo nella diffusione della rete 5G da parte degli Operatori di Telecomunicazione.

1. Le incertezze in ambito regolatorio e legale potrebbero rallentare la roadmap 5G in Italia

L'articolo 1 del decreto n. 22 del 25 marzo 2019, n.22 (c.d. Decreto Brexit), convertito in legge n. 41 del 20 maggio 2019, estende l'obbligo di notifica alla Presidenza del Consiglio dei ministri agli acquisti da parte di aziende, pubbliche o private, su beni o servizi relativi alla progettazione, realizzazione, manutenzione e gestione di reti di comunicazione elettronica basate sulla tecnologia del 5G, quando effettuate con soggetti fuori dall'Unione Europea.

La nuova Legge stabilisce che le società di telecomunicazioni che intendono acquisire beni e servizi da fornitori non UE collegati a reti 5G devono comunicarlo in modo che il Governo possa valutare se esercitare il diritto di veto sull'operazione o imporre regole o condizioni specifiche.

Di recente, inoltre, il Consiglio dei ministri ha licenziato un Decreto-legge, depositato al Senato della Repubblica, che integra la disciplina in materia di esercizio dei poteri speciali di cui al decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56, e definisce una specifica regolamentazione procedurale finalizzata a dotare la Presidenza del Consiglio dei ministri e le amministrazioni - coinvolte nell'applicazione della disciplina dei poteri speciali - di tempistiche molto dilatate e di strumenti istruttori più complessi per le valutazioni da svolgere.

Il quadro normativo che va delineandosi rischia di rallentare il processo di sviluppo della tecnologia 5G e danneggiare l'industria mettendo in gioco gli investimenti effettuati dagli operatori per l'implementazione delle reti, limitando la capacità degli stessi di prendere decisioni commerciali indipendenti. Una disciplina di questo tipo potrebbe compromettere i seguenti aspetti:

a) Aumentare i costi degli operatori che hanno investito nell'acquisizione delle frequenze e sono disposti a distribuire rapidamente il 5G in Italia;
b) Influenzare il *time to market* dell'economia digitale;

c) Congelare l'efficienza e la produttività dell'Italia;
d) Aumentare il divario tra l'Italia e tutti i paesi europei che hanno assunto una decisione diversa sul 5G;
e) Ritardare la necessaria costruzione di un ecosistema tra aziende private e pubbliche nello sviluppo di applicazioni 5G per consentire all'Italia di entrare nel mercato internazionale.

2. La Global Supply Chain & la Standardizzazione

Le minacce alla sicurezza informatica delle reti sono indipendenti dal paese di origine o dall'ubicazione di un Vendor. Inoltre, molto spesso un'attrezzatura tecnologica include componenti provenienti da diversi paesi, UE e non UE e spesso integrati nelle medesime apparecchiature. Infatti, le aziende che operano nel mercato globale fanno riferimento a centri di sviluppo, progettazione e produzione situati in diverse parti nel mondo, al fine di garantire l'integrazione delle migliori soluzioni nella composizione di un complesso apparato di Telecomunicazioni. Anche per Huawei, come per qualsiasi altro Fornitore, i prodotti finali sono realizzati con componenti hardware e software provenienti da Cina, Corea, Stati Uniti e altri Paesi nel mondo.

Il 5G non è una proprietà di Huawei, è basato su standard internazionali definiti e periodicamente migliorati da organismi indipendenti che mirano a garantire il massimo livello di sicurezza e interoperabilità.

I prodotti 5G di Huawei sono pienamente conformi alle specifiche 3GPP, ITU e IETF. L'azienda dispone di un sistema completo di garanzia della cyber security ed è munita di una comprovata esperienza in materia di sicurezza informatica, senza incidenti rilevanti nel corso degli anni.

La valutazione e la risoluzione delle vulnerabilità è un processo fondamentale, dalla fase di progettazione allo sviluppo dei prodotti e il continuo miglioramento del livello di sicurezza rappresenta una priorità per l'azienda.

Le Direttive europee guideranno l'evoluzione dei livelli di sicurezza attraverso l'implementazione del Cyber Security Act a cui tutti i paesi faranno pieno riferimento. Huawei si conformerà a ogni legge e disposizione relativa.

3. Diversi requisiti normativi per i diversi livelli della rete

In genere una rete di telecomunicazioni è composta da tre diversi livelli:

1) Rete di Accesso: questo è il livello esterno della rete che si occupa della connessione tra i dispositivi dell'utente (ad esempio smartphone, sensori IoT) e le stazioni radio base (il primo punto di ingresso nella rete di operatori Telco);
2) Rete di Trasporto: questo è il livello della rete che trasporta i dati utente aggregati dalla rete di accesso attraverso gli uffici centrali principali dell'Operatore;
3) Rete Core: questo è il livello interno della rete in cui risiede l'intelligenza per gestire la connessione con l'utente, che si tratti di una chiamata vocale o di una sessione di dati (http, streaming video, giochi, ecc.).

Quando si tratta di definire la normativa sulla cyber security, bisogna capire che domini diversi pongono minacce diverse e meritano un diverso livello di attenzione.
Di norma si comprende che, nel dominio della rete di Accesso, il traffico tra i terminali utente e le stazioni radio base è altamente crittografato in modo da prevenire qualsiasi violazione non autorizzata. Ciò renderà estremamente improbabile ed economicamente non conveniente per qualsiasi malintenzionato cercare di intercettare uno specifico traffico di dati dell'utente. In quest'area, la standardizzazione è molto attiva e definisce un robusto algoritmo di crittografia basato su chiavi molto lunghe (128 bit oggi, 256 bit nella prossima versione degli standard 5G in arrivo per il 2020-2021).
Nel dominio della rete di Trasporto, il traffico utente viene trasferito su canali altamente aggregati (in genere si tratterà di canali da oltre 100 Gbit/s) a livello ottico o IP in cui non c'è assolutamente alcuna conoscenza dei singoli flussi di traffico dell'utente. La probabilità di violazione dei dati o di rischi di cyber security in questo dominio è estremamente bassa.
La rete Core è invece il livello interno in cui vengono analizzati tutti i dati generati nella connessione. L'utente viene riconosciuto e autenticato per essere poi autorizzato all'uso dei servizi di rete specifici di cui necessita e solo alla fine connesso alla destinazione finale richiesta (ad es. per una chiamata vocale per connettere il chiamante all'utente chiamato, per una sessione http per inviare traffico ai server di destinazione: Google, Yahooo, Netflix, ecc.), dove i dati devono effettivamente essere protetti localmente.

Sulla base delle considerazioni semplificate di cui sopra, è possibile trarre una serie di conclusioni. I livelli della rete di Accesso e di Trasporto sono per loro natura meno esposti ai rischi di ciber security, sia perché vengono adottati standard di crittografia forti, sia perché l'identità dell'utente rimane effettivamente sconosciuta.

Le reti Core, come suggerisce il nome stesso, rappresentano sicuramente un dominio più critico in una rete di Telecomunicazioni e sono il luogo dove i dati dell'utente e "la sua identità" vengono gestiti per autenticare e autorizzare gli utenti stessi a utilizzare i vari servizi di rete. Dato che le reti Core sono il luogo in cui vengono elaborati i dati, nonostante gli enti di Standardizzazione lavorino costantemente per implementare misure tecniche e aumentare la sicurezza nella rete, le probabilità di vulnerabilità e di bug nei prodotti di rete Core potrebbero essere effettivamente superiori rispetto agli altri due livelli.

Alla luce della descrizione di cui sopra, secondo un approccio simile già adottato da altri paesi europei come il Regno Unito e la Germania, si suggerisce che i prodotti di rete di Accesso e Trasporto non siano soggetti a particolari procedure di approvazione, poiché non rappresentano alcun serio rischio di cyber security. In questo modo la costruzione della rete nazionale 5G non verrebbe rallentata da complesse procedure di certificazione, consentendo così agli Operatori italiani di Telecomunicazioni di accelerare la copertura nazionale. Sulla base della semplificazione di cui sopra, l'Italia sarà in grado di mantenere i vantaggi acquisiti grazie alle sperimentazioni 5G già effettuate.

Gli operatori, infatti, inizieranno ad implementare il 5G usando la versione NSA, che si appoggia totalmente alle reti 4 e 4.5G esistenti e solo successivamente si muoveranno verso la soluzione full 5G stand alone. Questo implica che tutti gli investimenti finora effettuati sul 4 e 4.5G possono essere interamente riutilizzati per sviluppare la rete 5G ottimizzando gli investimenti che gli Operatori dovranno fare nella prima fase di sviluppo del 5G.

Per i prodotti del dominio di rete Core, tuttavia, potrebbe essere messo in atto un processo di verifica e certificazione più accurato per garantire che le potenziali vulnerabilità vengano prontamente identificate e risolte prima ancora di passare alla rete live.

4. Collaborazione end-to-end sulla cyber security di tutta la rete

La salvaguardia della sicurezza informatica è considerata un obiettivo condiviso di tutte le parti interessate, compresi i fornitori di apparecchiature, gli Operatori di

telecomunicazioni e il Legislatore.

L'Europa ha pubblicato il regolamento generale sulla protezione dei dati personali (GDPR), che è uno standard aperto e trasparente a livello Europeo in corso di adozione anche da molti altri paesi nel mondo. Huawei ritiene che il Legislatore e i governi europei siano sulla buona strada per guidare la comunità internazionale in termini di standard di sicurezza informatica e meccanismi di regolamentazione e si impegna a lavorare più a stretto contatto con tutte le parti interessate, comprese le Autorità, gli Operatori e gli Istituti di Standardizzazione, per costruire un sistema basato su fatti e verifiche.