icom
istituto per la competitività

Il 5G per rilanciare l'Italia in sicurezza

Osservatorio sulla sicurezza del 5G
Roma, 12 novembre 2020

INDICE

1. L'IMPORTANZA DEL 5G E LO SVILUPPO DELLE RETI TRA COMPETITIVITÀ E SICUREZZA
2. SICUREZZA DELLE RETI TRA DISCIPLINA COMUNITARIA E INIZIATIVE NAZIONALI
3. Il 5G IN ITALIA
4. L'EVOLUZIONE DELLA NORMATIVA SULLA SICUREZZA NAZIONALE E L'APPLICAZIONE ALLE RETI 5G
5. CONCLUSIONI

icom
istituto per la competitività

1. L'IMPORTANZA DEL 5G E LO SVILUPPO DELLE RETI TRA COMPETITIVITÀ E SICUREZZA

IL RUOLO DELLE RETI DURANTE LA PANDEMIA E I TREND DEL POST COVID-19

- ✓ Durante il lockdown **il volume di traffico dati è aumentato del 57% su rete fissa e del 29% su rete mobile** rispetto ai valori registrati a febbraio.

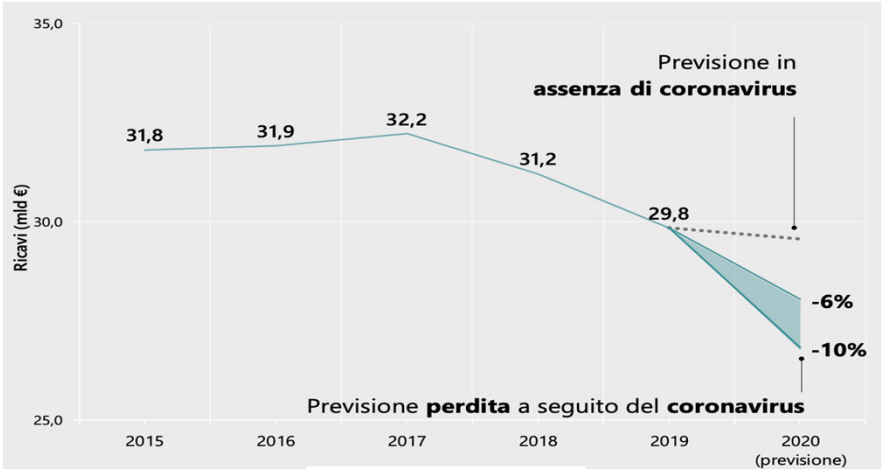
- ✓ Con l'inizio della fase 2 i valori si sono lievemente ribassati, facendo segnare comunque **un incremento medio di traffico ormai stabilizzato**
  - ➢ **+28% su rete fissa** e del **+15% su rete mobile** rispetto a **febbraio 2020**.

- ✓ Già a giugno 2020 l'Agcom prevedeva un **impatto negativo** del **Covid-19** sui **ricavi** del settore delle **telecomunicazioni** per un valore stimato **dal 6%** al **10%** rispetto al **2019.**

Aumento del volume medio di traffico dati e voce durante la pandemia (febbraio – maggio 2020)

		Lockdown	Fase 2
Reti Fisse	Volume medio del traffico dati	+57%	+28%
	Volume medio del traffico voce	+49%	+29%
Reti mobili	Volume medio del traffico dati	+29%	+15%
	Volume medio del traffico voce	+37%	+25%

Previsione dei ricavi del settore delle telecomunicazioni in Italia (2015-2020)



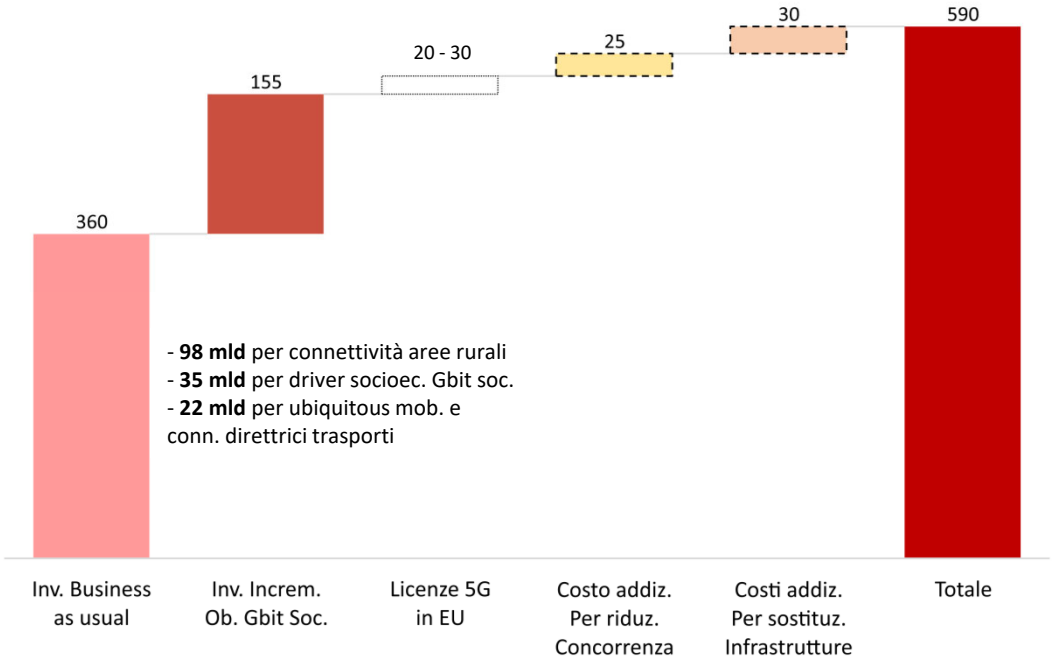
Fonte: AGCOM

GLI INVESTIMENTI PREVISTI IN EUROPA

- ✓ Il **fabbisogno** complessivo di **investimenti** necessari in Europa per l'**ammodernamento** delle **reti** e l'**implementazione** delle **nuove** equivale a **€ 535 miliardi**:
  - €**360** miliardi **business as usual** (manutenzione e ammodernamento);
  - €**155** miliardi necessari per rispettare gli **obiettivi** stabiliti nel quadro della **Gigabit Society**;
  - **€20-30** miliardi per l'acquisizione delle **licenze 5G** nell'Unione Europea.

- ✓ Secondo GSMA, in caso di **esclusione** dei **fornitori extraeuropei** il **fabbisogno complessivo crescerebbe** a **€590**
  - ➢ **€55 miliardi** di extra costi tra riduzione della concorrenza (€25 miliardi) e sostituzione delle apparecchiature non compatibili (€30 miliardi).

Stima investimenti necessari per l'implementazione delle reti 5G in Europa (in € mld, 2019-2025)



Fonte: Elaborazioni I-Com su dati Commissione Europea e GSMA

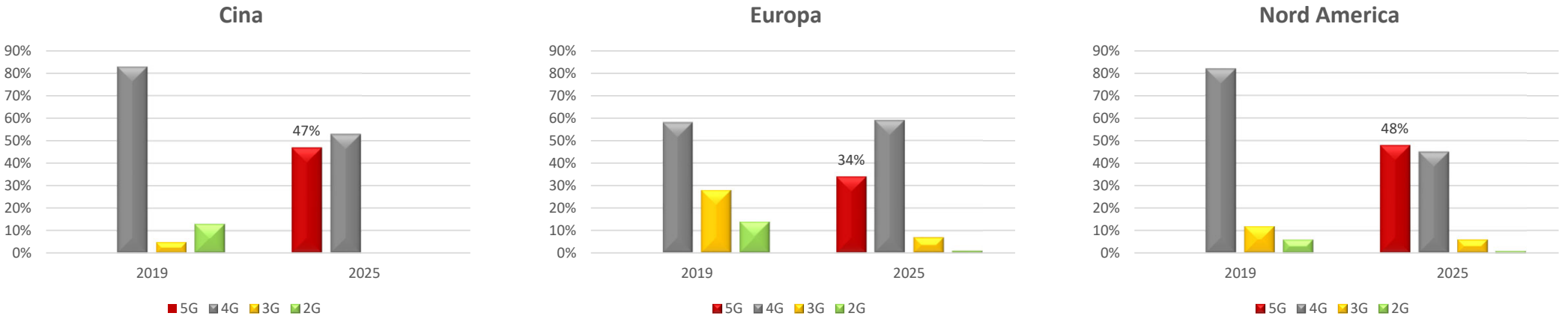
IL DEPLOYMENT DELLE RETI A LIVELLO GLOBALE

- ✓ Osservando i dati sul mix tecnologico delle reti mobili nelle principali aree avanzate del globo emerge che la **Cina** è il Paese con la **quota maggiore** di **infrastrutture 4G** sul totale delle reti.

- ✓ In **Europa** più della **metà** delle **infrastrutture** di rete mobile continentale **è 4G** anche se resiste ancora una quota rilevante di connettività 2G (14%).

- ✓ Le **proiezioni** al **2025** di GSMA vedono l'Europa (con il **34%** di infrastrutture **5G**) **notevolmente indietro** rispetto a **Nord America** (**48%** di infrastrutture **5G**) e **Cina** (**47%**), che viaggeranno di pari passo in termini di copertura della rete di quinta generazione.

Mix tecnologico delle reti mobili per area geografica (2019 – stime 2025)



Fonte: GSMA, 2020

DIFFUSIONE DEL 5G A LIVELLO GLOBALE

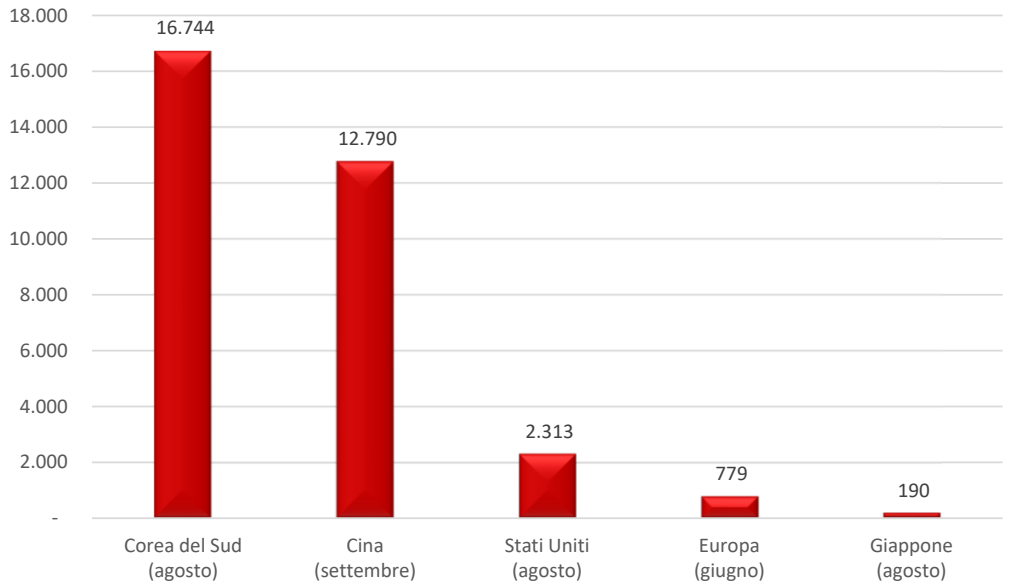
- ✓ I-Com ha stimato il numero di **utenti attivi ogni 100.000 abitanti** utilizzando dati provenienti da molteplici fonti primarie.

- ✓ La **Corea del Sud** è il Paese che può vantare la **maggior diffusione** dei servizi **5G** in **relazione** alla **popolazione**
  - ➢ **Corea**: **16.744** ogni **100 mila** abitanti
  - ➢ **Cina**: **12.790** ogni **100 mila** abitanti

- ✓ **Gli Stati Uniti** risultano notevolmente indietro con **2.313** utenti 5G ogni 100.000 abitanti ed ancor più l'**Europa** con **779 utenti 5G**

- ✓ Nel complesso si osserva **la necessità per l'Europa di accelerare in termini di infrastrutturazione e di offerta di servizi attrattivi per gli utenti**, incrementando e favorendo gli **investimenti** nelle reti anche per mezzo di politiche che agevolino le attività degli operatori di settore.

Utenti 5G per area geografica (per 100.000 abitanti, 2020)



Note: Alcuni operatori (Unicom – China, KDDI – Giappone, SoftBank – Giappone) non hanno rilasciato dati sul numero di utenze 5G sottoscritte. Il dato degli Stati Uniti è relativo al numero di terminali 5G venduti dagli operatori.

Fonte: Elaborazioni I-Com su dati Ministero della scienza e dell'ICT della Corea del Sud, China Mobile, China Telecom, M-Science, DOCOMO, Ericsson, World Bank

IL 5G E LA SICUREZZA: TRA DISCRIMINAZIONE GEOGRAFICA E RISK ASSESSMENT

icom istituto per la competitività

DISCRIMINAZIONE GEOGRAFICA

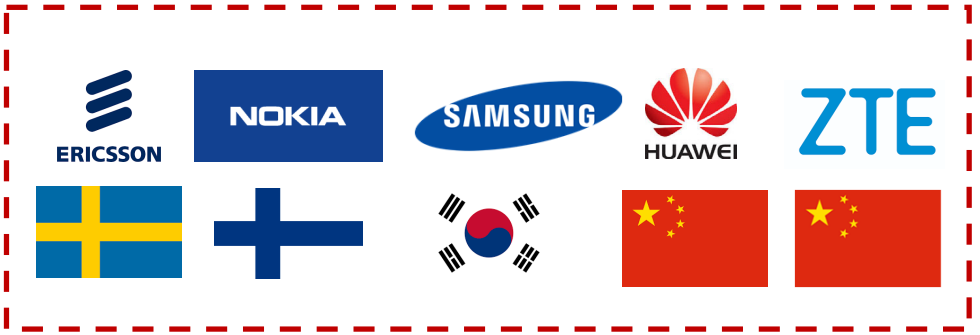
→ Input **amministrazione Trump** e **Five Eyes**

→ **Relazione Copasir:** preoccupazioni circa le attività di installazione, configurazione e mantenimento delle infrastrutture delle reti 5G di provenienza cinese.

3 CRITICITA'

- **Rischio** di limitare ex ante la presenza di vendor 5G nel mercato nazionale (non coerenza con i principi economici e commerciali di un'economia)
- **Ampiezza mercato** (solo 4/5 fornitori)
- **Cyber Supply Chain Risk Management**

Produttori di componentistica per il 5G



Mercato limitato a 4/5 fornitori

- Quote del mercato delle **apparecchiature di rete s**econdo **GSMA** (2018):
  - Ericsson sopra il 25%
  - Nokia sopra il 20%
  - Huawei e Zte >40%
  - Samsung intorno al 5%
- Quote di mercato delle apparecchiature di rete secondo **Dell'Oro** (2019):
  - Huawei al 28%
  - Nokia vicino al 20%
  - Ericsson al 15%
  - Zte al 10% (così come Cisco).

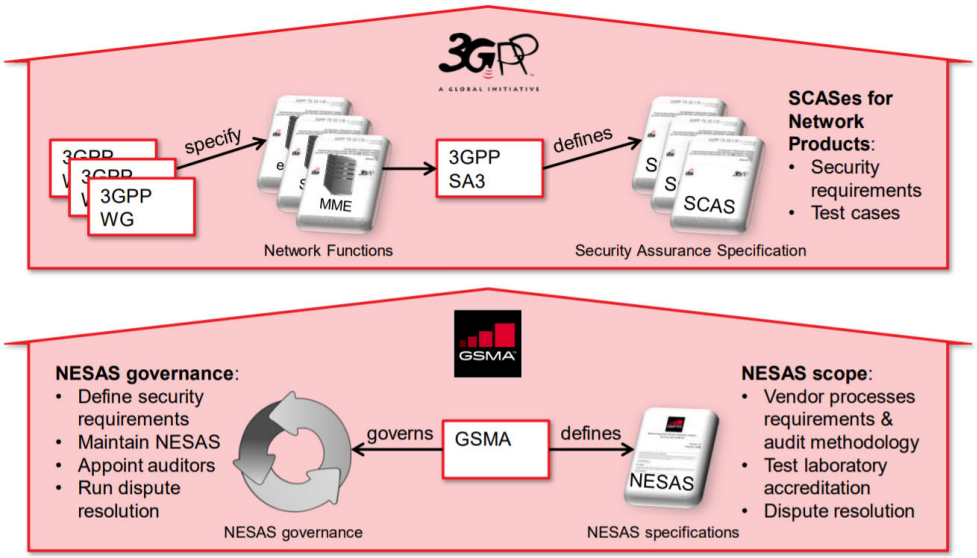
STANDARD E PROTOCOLLI DI SICUREZZA INTERNAZIONALI PER LE RETI MOBILI: SECAM, SCAS E NESAS

IL 3GPP ha introdotto la **SECAM (Security Assurance Methodology)** ed il processo di valutazione ad essa collegato, definendo attività e ruoli dei diversi soggetti coinvolti. Tra questi ci sono:

- Lo stesso **3GPP** → definisce requisiti di sicurezza e specifiche per i test, le **SCAS** (Security Assurance Specifications).
- Gli **auditor,** che effettuano l'assessment sul fornitore e procedure
- I **laboratori** di analisi, che valutano i prodotti sulla base delle SCAS
- **GSMA,** che funge da *Accreditation body* e:
  - ✓ definisce i **requisiti** di sicurezza dei **prodotti** dei vendor e la **metodologia** per l'**audit**;
  - ✓ gestisce l'**accreditamento** SECAM per **vendor** e **laboratori**
  - ✓ **definisce** il **proprio schema** per coprire questi task

NESAS
(Network Equipment Security Assurance Scheme)

Ruoli e compiti di 3GPP e GSMA nel SECAM / NESAS



Fonte: GSMA - 2019

IL NESAS: FUNZIONAMENTO E VANTAGGI

Obiettivo: mettere insieme un **singolo set** di **requisiti** che **definiscano** la **capacità** di un **prodotto** di **resistere** agli **attacchi**.

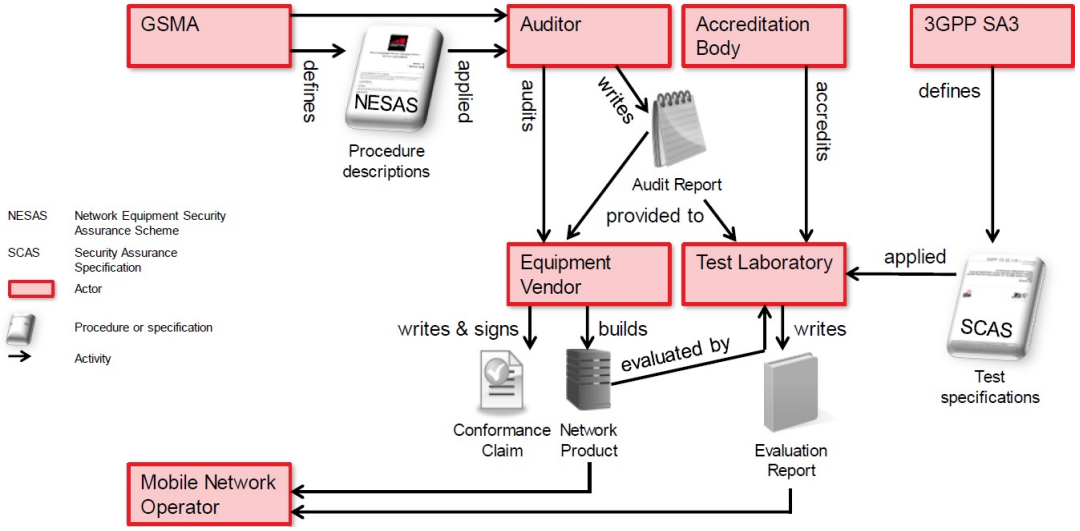
1. **SPECIFICHE** test definite dal **3GPP**

2. **GSMA** accredita i laboratori e fornisce i **requisiti** e la **metodologia** per l'Auditor

3. L'**AUDITOR** effettua l'assessment su fornitore e procedure

4. I **LABORATORI**
   i. applicano **test**
   ii. verificano le **prove** di **conformità** con **l'audit**
   iii. emettono un **rapporto**, verificabile anche dall'**operatore** di **rete**

Il funzionamento del NESAS



Fonte: GSMA - 2019

VENDOR	OPERATORI DI RETE	AUTORITÀ NAZIONALI
evitare moltiplicazione dei **requisiti** di sicurezza e migliorare le **procedure** di sicurezza **interne**	requisiti di sicurezza realizzati su **base associativa** (all'interno di GSMA) e quindi dividendosi i **costi**	**sistema** di sicurezza **universalmente applicabile** e **interoperabile** con le certificazioni **nazionali**

2. SICUREZZA DELLE RETI TRA DISCIPLINA COMUNITARIA E INIZIATIVE NAZIONALI

Il framework europeo sulla sicurezza 1/2

06/07/2016
Direttiva NIS (n. 1148/2016)

Procedura di revisione della direttiva in corso

17/04/2019
Reg. n. 881/2019
Cybersecurity Act

- ✓ Poteri ed organizzazione ENISA
- ✓ Introduzione sistemi europei di certificazione della cybersecurity
- ✓ Istituzione Gruppo europeo per la certificazione della cybersecurity

26/03/2019
Raccomandazione n. 2019/534 sulla cybersecurity delle reti 5G

- ✓ Individuazione rischi
- ✓ Set di azioni e misure
- ✓ Roadmap per Stati membri

09/10/2019
relazione sulla valutazione coordinata a livello di UE dei rischi per la cybersicurezza delle reti 5G (NIS)

- ✓ Tassonomia delle minacce
- ✓ Individuazione minacce più rilevanti e principali autori
- ✓ Individuazione delle risorse più sensibili e delle principali vulnerabilità (di natura tecnica e di altro tipo)

Il framework europeo sulla sicurezza 2/2

21/11/2019

Threat Landscape for 5G Networks (ENISA)

- ✓ Individuazione sfide e possibili minacce
- ✓ Definizione diagramma degli asset
- ✓ Identificazione l'esposizione dei diversi asset e valutate le motivazioni dell'agente di minaccia.

29/01/2020

- Dispiegamento del 5G sicuro - Attuazione del pacchetto di strumenti dell'UE

- pacchetto di strumenti dell'UE (Toolbox sul 5G) - NIS

- ✓ Individuazione rischi
- ✓ Descrizione 8 misure strategiche e 11 tecniche e relative azioni di sostegno

24/07/2020

Relazione sui progressi degli Stati membri nell'attuazione del Toolbox sulla sicurezza 5G (NIS)

- ✓ Descrizione livello di maturità raggiunto dai vari paesi nell'implementazione delle misure contenute nel Toolbox
- ✓ Individuazione dei principali rischi avvertiti

TREND IN ATTO
NEI MAGGIORI PAESI EUROPEI 1/2

icom istituto per la competitività

BENCHMARK

- **In Francia**, Orange ha rinnovato anche per il 5G gli accordi con i propri precedenti fornitori 4G, Ericsson e Nokia. Sulla stessa lunghezza d'onda si sono mossi Bouygues Telecom e SFR, che hanno rinnovato gli accordi rispettivamente con Ericsson e Nokia e avevano espresso la volontà di fare lo stesso con Huawei, salvo l'ottenimento dei permessi da parte del Governo. Anche il quarto operatore francese, Free, ha confermato per il 5G il proprio partner commerciale utilizzato per il 4G, ovvero Nokia.
- **In Germania**, al netto di eventuali disposizioni normative attese nelle prossime settimane, tutti e tre gli operatori avevano rinnovato o erano in procinto di rinnovare gli stessi accordi multi-vendor con i fornitori già attivi sulla rete 4G: Ericsson/Huawei per Deutsche Telekom (sebbene la chiusura degli accordi sia in attesa delle decisioni politiche), Nokia/Huawei per Telefónica Germany (che punterà maggiormente sulla diversificazione anche della rete core dal 2024) ed Ericsson/Huawei per Vodafone.
- Un discorso simile per **la Spagna,** dove Vodafone España ha rinnovato con Ericsson e Huawei (già fornitori 4G); Orange Espagne ha rinnovato gli accordi con Ericsson e Huawei allargando la propria schiera di fornitori 5G anche a ZTE; e Telefónica (Movistar) ha rinnovato con Ericsson e Nokia e allargato la fornitura 5G anche Huawei.
- In **Gran Bretagna** il National Cyber Security Center (NCSC) ha disposto la rimozione di Huawei dalla rete 5G nazionale entro il 2027, oltre ad un divieto sull'acquisto di nuove tecnologie del vendor dopo il 31 dicembre 2020. La tendenza nel Paese verte in ogni caso verso un rinnovo multi-vendor con gli stessi operatori già fornitori nel 4G, ovvero Nokia e Huawei per 3 – Three; Ericsson e Nokia per Telefónica (O2); e Ericsson e Huawei sia per BT Group (EE), sia per Vodafone

TREND IN ATTO
NEI MAGGIORI PAESI EUROPEI 2/2

- il **mercato** si mantiene **ristretto** a 4 fornitori

- le posizioni di mercato sono direttamente collegate alla **compatibilità** delle apparecchiature

- **il principio di discriminazione geografica** sembra visto come una limitazione rispetto alla conclusione degli accordi

- per gli operatori di rete il 5G è un **must-have**.

Stato	Operatore	Vendor 4G	Vendor 5G
Francia	Bouygues Telecom	Ericsson/Huawei	Ericsson + in talks with Huawei (1)
	Free Mobile	Nokia	Nokia
	Orange	Ericsson/Nokia	Ericsson/Nokia
	SFR	Nokia/Huawei	Nokia + in talks with Huawei (1)
Germania	Deutsche Telekom (T-Mobile)	Ericsson/Huawei	Ericsson/Huawei (2)
	Telefónica Germany (O2)	Nokia/Huawei	Nokia/Huawei (3)
	Vodafone	Ericsson/Huawei	Ericsson/Huawei (2)
Spagna	Orange Espagne	Ericsson/Huawei	Ericsson/Huawei/ZTE (3)
	Telefónica (Movistar)	Ericsson/Nokia	Ericsson/Nokia /Huawei
	Vodafone España	Ericsson/Huawei	Ericsson/Huawei
	Yoigo	Ericsson	Ericsson
Regno Unito	3 - Three	Nokia/Huawei	Nokia/Huawei (4)
	BT Group (EE)	Ericsson/Huawei	Ericsson/Huawei (4)
	Telefónica (O2)	Ericsson/Nokia	Ericsson/Nokia (4)
	Vodafone	Ericsson/Huawei	Ericsson/Huawei (4)
Italia	Iliad	Nokia	Nokia
	TIM	Ericsson/Nokia/Huawei	Ericsson/ Nokia
	Vodafone Italia	Huawei/Nokia	Huawei/Nokia
	Wind Tre	ZTE/Ericsson	ZTE/Ericsson

Note:
1. **in attesa dell'approvazione del Governo Francese;**
2. **in attesa delle eventuali evoluzioni normative;**
3. **intendono cessare la partecipazione con Huawei nella rete core per ragioni tecniche;**
4. **era prevista la partecipazione di Huawei nella rete di accesso con cap al 35% del totale. Il successivo aggiornamento normativo prevede la rimozione di Huawei entro il 2027, e il divieto di acquisto di nuove tecnologie del vendor dopo il 31 dicembre 2020.**

3. IL 5G IN ITALIA

LO SVILUPPO DELLE RETI

L'**Italia** è il 3° Paese in Europa per n. di sperimentazioni 5G (Fonte: 5G Observatory)

Tuttavia si osserva come:

- il **n. di progetti importanti** (che coinvolgono almeno 2 siti e gli utenti) siano stati **solo 2**
- Il n. di **sperimentazioni**, sia in Italia che negli altri Paesi, sta **progressivamente scemando**
- La **copertura** del 5G è ancora **limitata** al lancio del servizio commerciali di alcuni operatori e solo in **alcune città** o **aree** delle maggiori città

Sperimentazioni nei maggiori Paesi europei 2015-2020 (settembre 2020)

	2015	2016	2017	2018	2019	2020	Totale Paese
Spain	1	3	6	11	7	3	31
Germany	1	5	4	6	4	2	22
Italy	0	3	4	9	3	2	21
France	0	1	5	11	2	0	19
United Kingdom	0	4	4	5	5	0	18
Totale per anno	2	16	23	42	21	7	111

Fonte: 5G Observatory

Sperimentazioni nei maggiori Paesi europei per livello di maturità (settembre 2020)

Paese	Conteggio di Level of maturity*			Totale Paese
	1	2	3	
Spain	5	9	17	31
United Kingdom	4	3	11	18
Germany	3	9	10	22
Italy	2	6	13	21
France	2	4	13	19
Totale per livello di maturità	16	31	64	111

* con il livello [1] vengono indentificati i progetti più importanti (2 cell sites); con livello [2] gli altri progetti pilota; con il livello [3] le sperimentazioni minori
Fonte: 5G Observatory

GLI INVESTIMENTI NECESSARI PER L'UPGRADE DELLE RETI

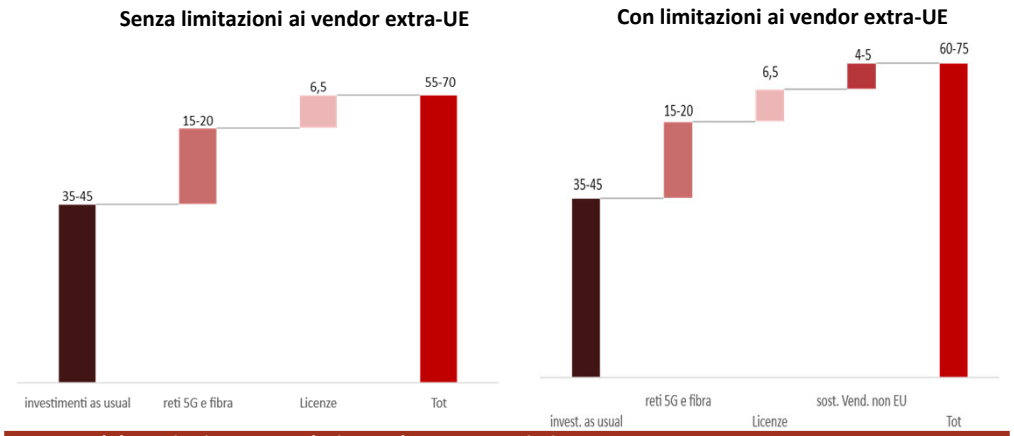
Negli ultimi **5 anni** sono stati investiti nella rete mobile circa **14 miliardi**

- secondo l'Authority, questi dati in **flessione** sono dovuti al venir meno dei fondi investiti per le **licenze 5G**.

Secondo le **elaborazioni EY** su dati CE e Asstel, in Italia gli **investimenti** necessari per l'upgrade al 5G sono stimabili in:

- tra **55-70 miliardi senza limitazioni** ai vendor extra-UE
- tra **60-75 miliardi con** le **limitazioni** (oltre ad un ritardo fino a 18 mesi)
- gli operatori di rete nei **prossimi 5 anni** potrebbero dover **incrementare** i propri **investimenti** fino **a 5 volte**

Stima investimenti necessari per l'implementazione delle reti 5G in Italia (in € mld, 2019-2025)



Fonte: elaborazioni I-Com su dati Asstel, EY e Commissione Europea, 2020

Investimenti in immobilizzazione su rete fissa e mobile (€ miliardi, 2015-2019)

	2015	2016	2017	2018	2019	tot 2015-2019
Mobile	3,11	2,47	2,3	3,14	2,73	13,75
Fissa	4,18	4,58	4,88	5,16	5,14	23,94

Fonte: AGCOM, Relazione annuale 2020

4. L'EVOLUZIONE DELLA NORMATIVA SULLA SICUREZZA NAZIONALE E L'APPLICAZIONE ALLE RETI 5G

La sicurezza delle reti 5G nel contesto nazionale

D.L. n. 21/2012 cov. con legge n. 56/2012

Golden powers

D.L. 25 n. 22/2019

(c.d. Decreto Brexit)

- ✓ Ha aggiunto all'ambito previsto dalla legge n. 56/2012 l'art. 1 bis, rubricato *"Poteri speciali inerenti le reti di telecomunicazione elettronica a banda larga con tecnologia 5G"*
- ✓ **Ambito applicativo**: anche nel caso di forniture di materiali e servizi, per operazioni realizzate con soggetti esterni all'UE

21/09/2019

D.L. n. 105/2019 conv. con la legge n. 133/2019, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica

Obiettivo: assicurare un livello **elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici** delle amministrazioni pubbliche, degli enti e degli operatori da cui dipende l'esercizio di una **funzione essenziale** dello Stato, ovvero la prestazione di un **servizio essenziale** per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un **pregiudizio per la sicurezza nazionale.**

L’implementazione del perimetro di sicurezza nazionale cibernetica. L’adozione del primo DPCM

Il 21 ottobre 2020 è stato pubblicato in G.U. il **DPCM 30 luglio 2020, n. 131**, il quale:

- ✓ definisce le **modalità** e i **criteri procedurali** di individuazione dei soggetti (amministrazioni pubbliche, enti e operatori pubblici e privati) inclusi nel perimetro di sicurezza nazionale cibernetica e che, pertanto, saranno tenuti al rispetto delle misure e degli obblighi previsti dal D.L.;

- ✓ declina i **criteri** con i quali i soggetti inclusi nel perimetro predispongono e aggiornano l'**elenco** delle reti, dei sistemi informativi e dei servizi informatici di rispettiva pertinenza, comprensivo della relativa architettura e componentistica;

- ✓ attribuisce al **Centro di valutazione e certificazione nazionale (CVCN)** il potere di effettuare verifiche preliminari ed imporre condizioni e test di hardware e software secondo un approccio gradualmente crescente nelle verifiche di sicurezza;

- ✓ istituisce un **Tavolo interministeriale** per l'attuazione del perimetro di sicurezza nazionale cibernetica con funzioni di supporto del CISR, presieduto da un vice direttore del DIS, composto da due rappresentanti di ciascuna amministrazione CISR, un rappresentante per ciascuna delle due agenzie di informazioni (Agenzia informazioni e sicurezza esterna – AISE e Agenzia informazioni e sicurezza interna – AISI) e due rappresentanti dei ministeri di volta in volta interessati di cui almeno uno, in adesione ai rilievi espressi da Consiglio di Stato e Camere, in possesso di competenze tecnico-specialistiche nella materia della sicurezza cibernetica.

La proposta di DPR per l'attività di CVCN e CV

In attuazione dell'art. 1 c. 6 del decreto istitutivo del perimetro, è stato proposto uno **schema di DPR** che:

- ✓ individua le **tipologie di beni, sistemi e servizi ICT** oggetto di valutazione;
- ✓ fissa le **modalità** ed i **contenuti delle comunicazioni** da effettuare in favore di CVCN o CV da parte dei soggetti inclusi nel perimetro prescrivendo l'invio del **documento di analisi del rischio;**
- ✓ definisce le **procedure, le modalità ed i termini da seguire ai fini delle valutazioni** da parte dello stesso CVCN e dei centri di valutazione del Ministero dell'interno e del Ministero della difesa (CV) introducendo un **meccanismo di silenzio-assenso** per cui inutilmente decorsi i termini sopra indicati senza che CVCN o CV si siano pronunciati, i soggetti inclusi nel perimetro possono proseguire nella procedura di affidamento e nell'esecuzione del contratto
- ✓ descrive le **tipologie di valutazioni, test e verifiche realizzabili;**
- ✓ declina le **attività di verifica ed ispezione** cui possono essere sottoposti i soggetti inclusi nel perimetro.

Lo schema di decreto demanda al CVCN l'adozione (entro 60 gg. dall'entrata in vigore dello stesso decreto) di un atto che individui le metodologie da seguire nella redazione del documento di analisi del rischio e l'individuazione dei test corrispondenti ai livelli di severità derivanti dall'analisi del rischio.

5. CONCLUSIONI

Conclusioni

Tre **fattori-chiave** emersi dall'analisi:

- ✓ mercato dell'offerta di apparecchiature 5G ristretto a 3-4 fornitori
- ✓ necessità di compatibilità tra apparecchiature (e quindi fornitori) 4G e 5G
- ✓ evoluzione delle normative tendente ad un'ulteriore restrizione del mercato dell'offerta per ragioni geopolitiche

- ✓ Serio **rischio di stallo o rallentamento** nelle operazioni di infrastrutturazione che potrebbe avere a sua volta effettivi negativi in termini di minore sviluppo tecnologico e ritardati (e probabilmente anche minori) benefici economici derivanti dalla rivoluzione 5G.

- ✓ Obiettivi di **sicurezza** e di **competitività non** devono essere visti in una logica di **trade-off**, che rischia di comportare sacrifici eccessivamente onerosi, dall'una e dall'altra parte.

Spunti di policy – IL LIVELLO EUROPEO

- ✓ L'**Europa** nel prossimo futuro rischia di rimanere **indietro**, rispetto a **Cina** e **Stati Uniti**, nella corsa alla realizzazione delle **nuove reti**, con un conseguente **incremento del gap di competitività.**
- ✓ Già **oggi** si registra un **ritardo** negli **investimenti** e nell'**adozione** del 5G, sia rispetto all'Asia che agli Stati Uniti. Un **divario** che è ancora possibile **colmare** ma solo con un'**azione** sufficientemente **rapida** e il più possibile **coordinata** a livello europeo.

Per assicurare all'Europa di essere all'avanguardia e competitiva, a livello globale, nello sviluppo del 5G, è quindi indispensabile:

- ✓ adottare un **approccio comune** che garantisca la creazione di un **ecosistema** favorevole agli **investimenti**
- ✓ fissare, rispetto alla tematica della sicurezza, **obiettivi di armonizzazione**, soprattutto rispetto a **standard** e **certificazioni**, quanto più possibile ambiziosi.

Spunti di policy – IL LIVELLO ITALIANO

Dal punto di vista **normativo** è fondamentale:

- ✓ assicurare che la complessa procedura disegnata dal D.L. n. 105/2019 per la definizione del perimetro di sicurezza nazionale cibernetica sia portata a compimento secondo **tempistiche ragionevoli** e che il mosaico normativo si **armonizzi** con la vigente disciplina sul golden power

- ✓ **rendere operative le procedure di verifica** che vedono come protagonisti **CVCN** e **CV** e a creare così quella certezza indispensabile per gli investimenti nelle reti 5G, dotando il CVCN e i CV delle risorse adeguate per far fronte alle sfide particolarmente complesse per assicurare al contempo un obiettivo tecnologico sufficientemente ambizioso con un livello di sicurezza adeguato a proteggere l'Italia da minacce cibernetiche.