icom
istituto per la competitività

Lo sviluppo del 5G in Italia tra competitività e sicurezza nazionale

Roma, Camera dei deputati, 25 settembre 2019

INDICE

I. VANTAGGI TECNOLOGICI DEL 5G

II. USE CASES E BENEFICI ECONOMICI

III. IMPATTO ECONOMICO 5G IN UK

IV. 5G IN ITALIA

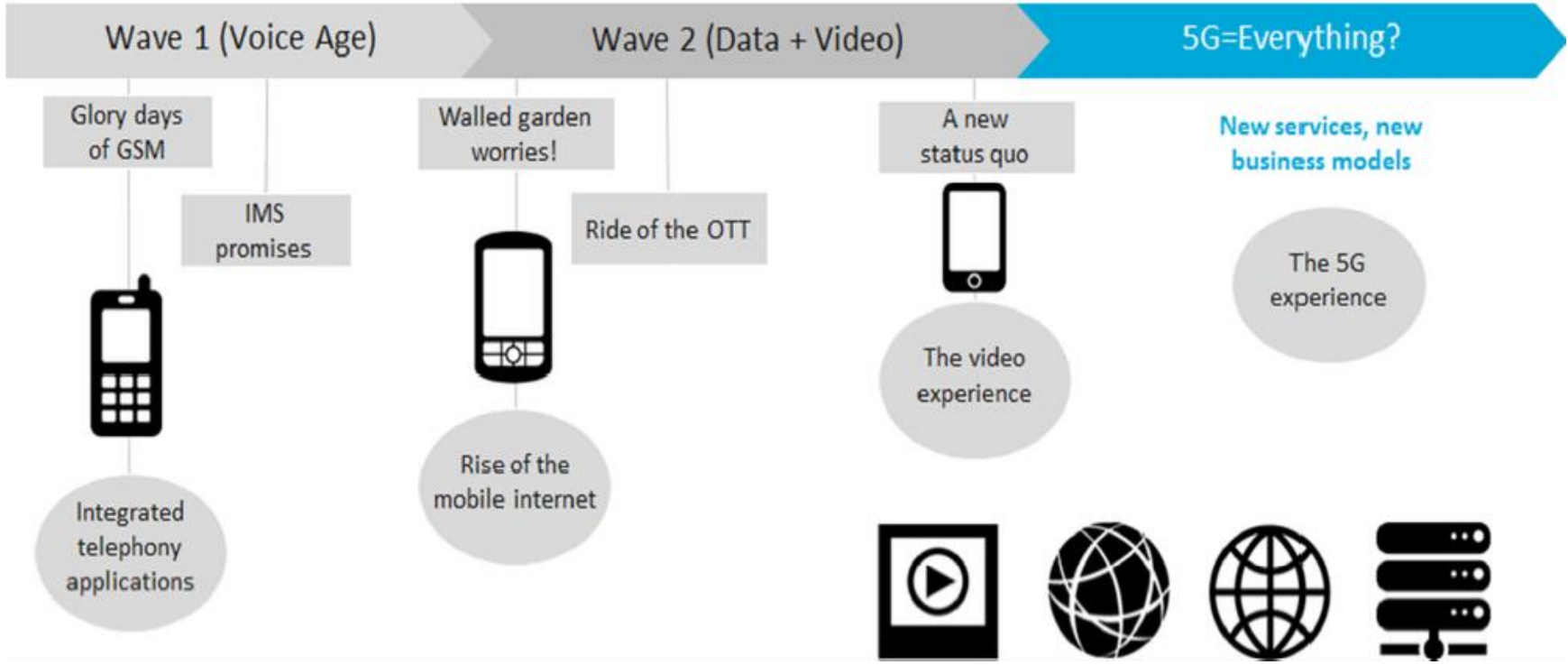
V. PROFILI TECNICI RELATIVI ALLA SICUREZZA

VI. MISURE ADOTTATE IN GERMANIA E UK

VII. L'EVOLUZIONE DELLA NORMATIVA ITALIANA E L'APPLICAZIONE ALLE RETI 5G

VANTAGGI TECNOLOGICI DEL 5G

- **Velocità** di trasferimento dei dati fino a 100 volte maggiore
- Sensibile **riduzione** della **latenza** che la avvicina allo zero
- Possibilità di gestire fino ad un **milione** di **dispositivi** per km^2
- Maggiore **longevità** delle **batterie** dei dispositivi
- **Flessibilità** e **indipendenza** di accesso



USE CASES E BENEFICI ECONOMICI

Secondo lo **studio** sul **5G** condotto per la **Commissione** europea da Trinity College, Tech4i2, Real Wireless e InterDigital, i benefici del 5G a livello di impatto economico ammonterebbero a:

- € **62 miliardi** **provenienti dai principali verticals** (automotive, trasporti, sanità, reti energetiche)

- Ulteriori € **51 miliardi** derivanti da **soluzioni smart cities**, aree extra urbane e digitalizzazione intelligente di **abitazioni** e posti di **lavoro**

→ per un totale di € **113 miliardi** l'anno già nel **2025**

Benefici annui derivanti da 5G al 2025 (mld €)	
Benefici da verticals per anno al 2025	**mld €**
Automotive	42,2
Salute	5,5
Trasporti	8,3
Utilities	6,5
Subtotale benefici da verticals	62,5
Benefici derivanti da evoluzioni "ambientali" per anno al 2025	**mld €**
Smart cities	8,1
Aree non-urbane	10,5
Smart homes	1,3
Smart workplaces (uffici e aziende)	30,6
Subtotale benefici "ambientali"	50,6
Benefici annuali totali	**113,1**

Fonte: Trinity College, Tech4i2, Real Wireless and InterDigital, "Identification and quantification of key socio-economic data to support strategic planning for the introduction of 5G in Europe).

BENCHMARK INTERNAZIONALE: IMPATTO DEL 5G IN UK E STIMA DELLE CONSEGUENZE DI POSSIBILI RESTRIZIONI

- Il Governo britannico stima **benefici** del **5G** per l'economia del paese nell'ordine di **£ 173 miliardi** complessivi fino al **2030**

Stima benefici economici del 5G in UK											
	2020	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**2028**	**2029**	**2030**
Totale (£mld)	0	2,19	4,62	7,3	10,3	13,7	17,9	23,9	28,4	30,5	34,4
Per mese	0	0,18	0,38	0,6	0,9	1,1	1,5	2,0	2,4	2,5	2,9
Fonte: Assembly, DCMS (2019)											

- **Stime** delle **telco britanniche** (EE, O2, Three, Vodafone) sugli **effetti** di una **restrizione** del mercato ai **vendor europei**
  - → **costi aggiuntivi** necessari a sostituire la **componentistica**
  - → **collo di bottiglia** dalla restrizione a due vendor (Ericsson e Nokia).
  - → il **costo** del **ritardo** tra **£ 4,5** e i **£ 6,8 miliardi** nel triennio 2020-2022

Stima riduzione dei benefici economici del 5G in UK causata da restrizioni e conseguenti ritardi nell'implementazione			
Riduzione dei benefici (m £) per ritardo	**2020**	**2021**	**2022**
Ritardo di 1 anno	0	2.190	2.190
Ritardo di 1,5 anni	2.190	2.313	4.503
Ritardo di 2 anni	2.190	4.625	6.815
Fonte: Assembly, DCMS (2019)			

IL 5G IN ITALIA

Nel **DESI 2019 l'Italia è tra i Paesi UE**

→ **24ª** per digitalizzazione dell'economia e della società

→ **2ª** per lo stato di **avanzamento del 5G**.

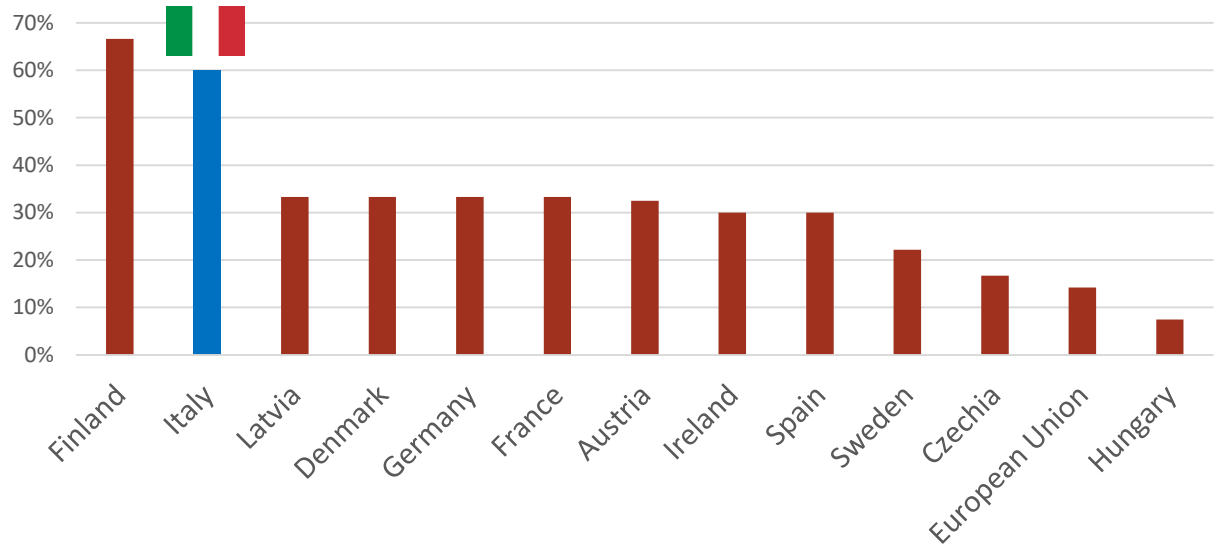
FATTORI DI SVILUPPO

- ✓ **Città per le sperimentazioni 5G** (bando 5 città in 5G, individuate già nel 2017 Milano, Prato, L'Aquila, Bari e Matera)
- ✓ **Altre sperimentazioni** sulla base di accordi volontari tra gli operatori e i comuni a Roma, Torino, Napoli e Genova.
- ✓ **Spettro** armonizzato a **livello UE** per la **bb mobile** assegnato al **94%**

  → bande **3,6 GHz**, **26 GHz** e **700 MHz** che però verrà messa a disposizione entro **luglio 2022** (da qui il valore che indica l'Italia pronta al **60%**, che la posiziona comunque seconda in Europa).

Importante **non perdere** questo **vantaggio**

5G readiness dei Paesi europei



Fonte: European Commission, Digital Scoreboard (giugno 2019)

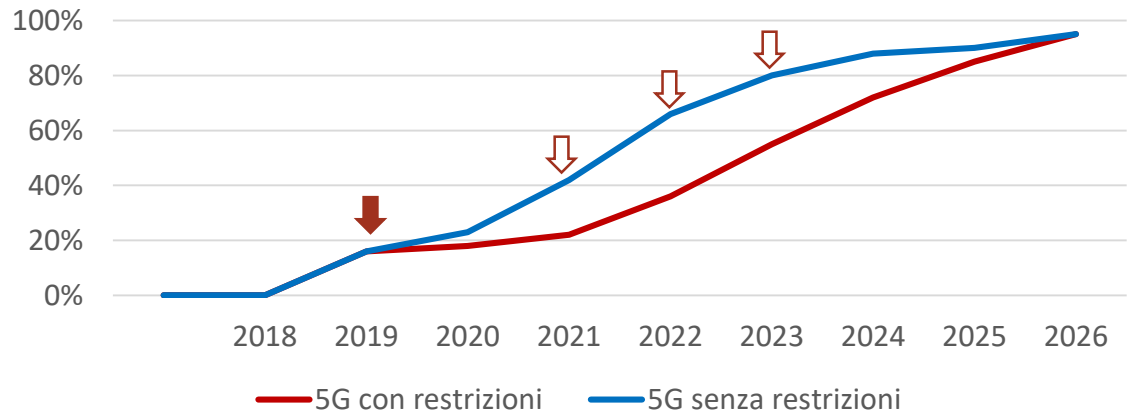
- il prezzo di assegnazione della **banda 3,6 GHz** in Italia è risultato fino ad ora il più alto in Europa= in media **36 centesimi di EUR/pop/MHz**.
- assegnazione **record per l'erario**, ma allo stesso tempo una **spesa** ingente per gli **operatori** (remunerazione **investimenti** per la partecipazione all'**asta** + investimenti per il **roll-out** delle **reti**).

→ importante garantire la **rapidità** nelle **procedure** amministrative relative ai permessi per l'implementazione delle **reti 5G**, in modo che questa sia efficace, veloce e sostenibile (oltre che sicura).

PROSPETTIVE DI CRESCITA E IMPATTO ECONOMICO DEL 5G IN ITALIA

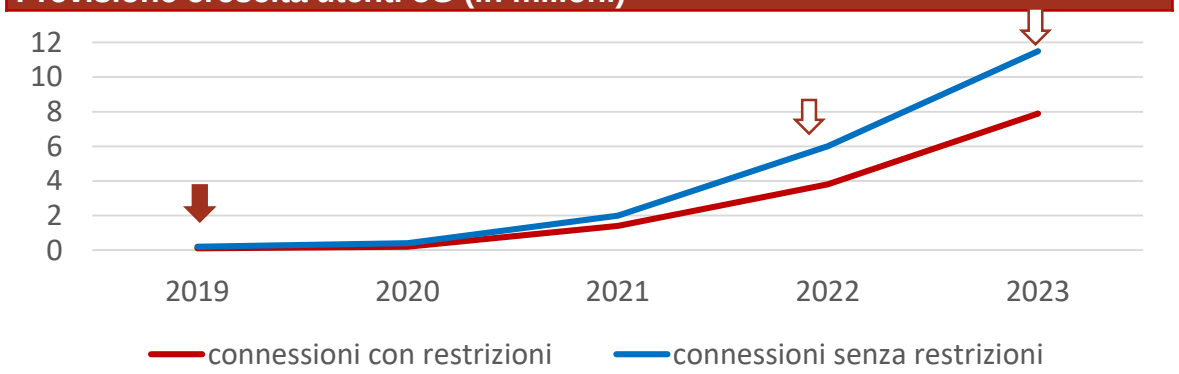
icom istituto per la competitività

Previsione copertura 5G



Fonte: EY, settembre 2019

Previsione crescita utenti 5G (in milioni)



Fonte: EY, settembre 2019

IMPATTO SUL PIL DEL 5G SECONDO EY

→ circa **€ 80 miliardi** in **15 anni**

→ incremento dello **0,29%** medio annuo

INVESTIMENTI

→ ammonteranno ad un valore compreso tra i €**60** e i €**75** miliardi di cui

- ✓ **€35-45** investimenti di manutenzione **reti esistenti**
- ✓ **€15-20** miliardi sviluppo **reti 5G** e diffusione **fibra**
- ✓ **€6,5** miliardi di **licenze 5G**
- ✓ Tra €**4 e €5** miliardi di **costi aggiuntivi** per sostituzione di **vendor extra Ue**

- ✓ **maggiori costi** per via della sostituzione di vendor extra UE con vendor UE
- ✓ **ritardo** nella diffusione della **copertura** e nell'**adozione** da parte degli utenti

→ **restrizione** verso **operatori extra UE** impatterebbe sul PIL italiano per **circa 10 miliardi**

icom
istituto per la competitività

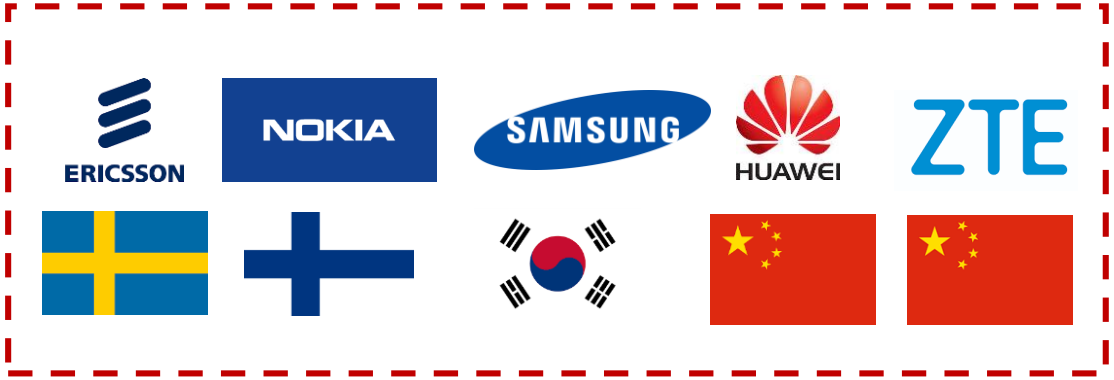
PROFILI TECNICI RELATIVI ALLA SICUREZZA

NAZIONALITÀ OPERATORI?

Pochi produttori di **componentistica** per il 5G:

Ericsson (Svezia), Huawei (Cina), Nokia (Finlandia), Samsung (Corea del Sud) e ZTE (Cina).

Produttori di componentistica per il 5G



Operatori di rete in Italia

Molteplici nazionalità anche degli azionisti degli **operatori di rete** in Italia

- francesi e americani a contendersi la leadership dell'ex monopolista Tim
- britannici alla guida di Vodafone
- cinesi prima con e poi senza russi in Wind Tre
- nuovi entranti francesi in Iliad
- svizzeri in Fastweb
- americani in Linkem

La **nazionalità** degli operatori sembrerebbe quindi essere un **problema secondario** rispetto alle tematiche tecniche relative alla **sicurezza nazionale** ed alle **misure** che possono essere assunte per **mitigare** i rischi.

IMPOSSIBILITÀ DI REALIZZARE RETI ICT CHE SIANO AL 100% SICURE

Le future reti ICT

- sono **sistemi interconnessi** composti da **miliardi** di **transistor** e milioni di **righe** di **codice**
- sono realizzate in forma **modulare** (i produttori acquistano in outsourcing il 99% di componenti e software)
- sono **aggiornate** di frequente

→ **interdipendenza**: la sicurezza dipende da tutti gli attori della catena

→ Il Nist parla di **Cyber Supply Chain Risk Management** (C-SCRM)

I sistemi di sicurezza IT tradizionali, come ad esempio i "**Common Standard Criteria**", appaiono inefficaci, mentre altre operazioni quali il **security assessment**, le **revisioni** del codice e i **penetration test** possono **migliorare** la **qualità** del software ma **non** possono **garantire** l'assenza di codici **malevoli** o **backdoor**.

5G AUMENTA LA SUPERFICIE DI ATTACCO

Vulnerabilità 5G → sistemi complessi e interconnessi

Massive IoT: diffusione di sensori, device e apparecchiature capaci di comunicare tramite protocollo e talvolta di agire nel mondo fisico.

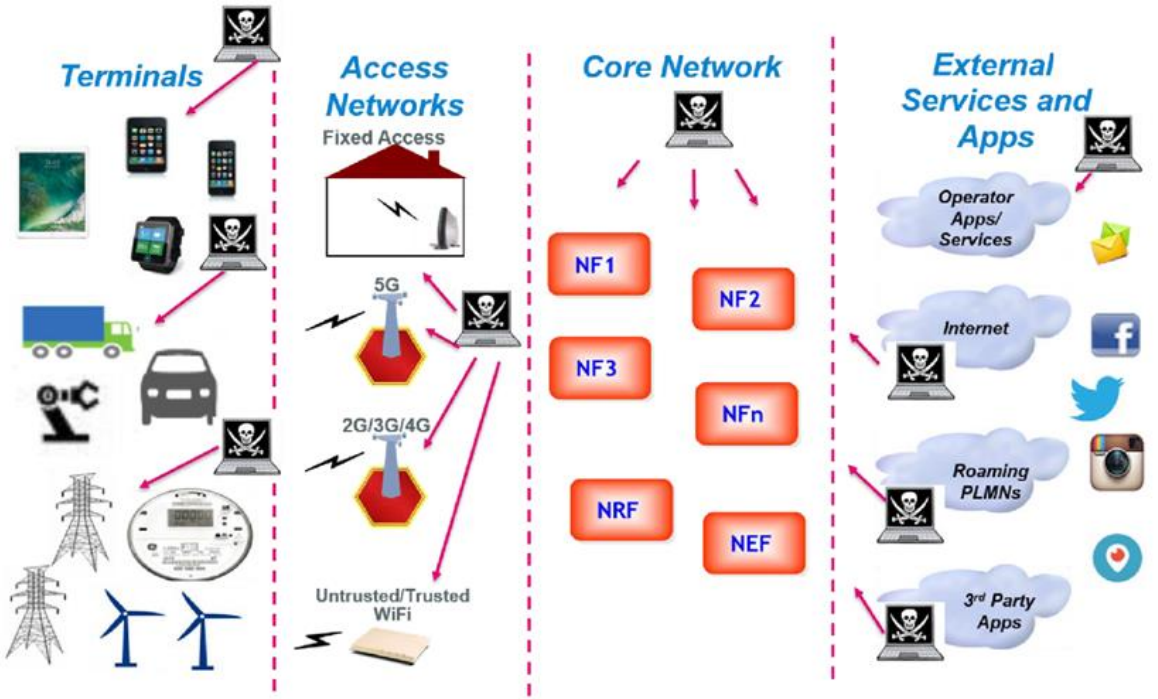
Reti 5G: **4 diversi domini** su cui possibili malintenzionati potrebbero attaccare:

1) i **terminali** (attacchi su altri terminali, infrastrutture o servizi)
2) la rete di **accesso** (anche reti precedenti, privacy – Rogue base station, Man in the middle)
3) la rete **core**
4) i **servizi** e le applicazioni esterne (OTT).

Edge computing

distribuzione di piccoli data center dotati di capacità di elaborazioni che siano il più possibile vicini all'*edge* (cioè al "margine" della rete dove i dati vengono prodotti) → garantire la latenza ultra low per i servizi IoT.

The 5G Threat Landscape



Fonte: 5G Americas, "The Evolution of Security in 5G", ottobre 2018

SICUREZZA E 5G : GLI ASPETTI POSITIVI

FALLE E SISTEMI DI SICUREZZA

i sistemi di rete mobile sono sempre stati soggetti a possibili attacchi informatici

il **5G**

porta con sé tutte le **criticità** e le **vulnerabilità** cui sono soggetti i sistemi basati sugli **standard precedenti**

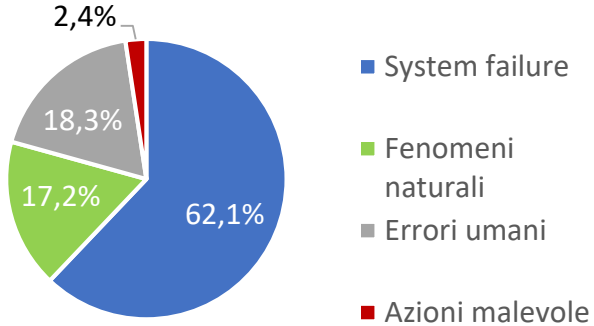
ha delle **possibilità di difesa** capaci di **innalzare** il livello di **sicurezza** complessivo a uno **stadio superiore** rispetto a tutti gli **standard precedenti**

GLI ATTACCHI

il **Rapporto Enisa** indica che appena **il 2,4% (su 169)** dei problemi riscontrati sulle reti di telecomunicazioni europee nel 2017 sono riconducibili a **incidenti di sicurezza causati** da attacchi di **hacker**.

Hardware failure, software bugs ed errati aggiornamenti software e gli errori umani siano la causa dominante degli incidenti riportati con impatto sul maggior numero di connessioni.

Incidenti significativi nella sicurezza degli operatori tlc, per tipologia (2017)



Fonte: Enisa, report agosto 2018, su dati NRA Stati membri

I casi di Germania (BNetzA) e UK (NCSC e HC-SEC) e le possibili misure per minimizzare rischi

GERMANIA

Requisiti BNetzA (marzo 2019)

- Impossibilità per gli operatori di utilizzare componentistica di un singolo vendor
- Necessità di utilizzare per le operazioni di infrastrutturazione e manutenzione **solo personale qualificato.**
- Rapporto fiduciario in caso di **subappalto**
- Fornitori di sistemi devono conformarsi alla **regolamentazione** su **sicurezza nazionale**, **segretezza** delle comunicazioni e **data protection**.
- **Monitoraggio** costante del traffico di rete rispetto ad anomalie
- Componenti **certificati** dal **Federal Office for Information Security** e testati regolarmente.
- Dimostrazione che hardware testato e codice sorgente siano realmente impiegati nei prodotti utilizzati.
- I requisiti verranno regolarmente **aggiornati**
- Misure sono valide per tutte le reti, tutti gli operatori e tutti i service providers.

REGNO UNITO

Governo prevede di:

- utilizzare la tecnologia di **diversi vendor**

- limitare l'approvvigionamento dei componenti provenienti da operatori **extra europei** alle parti **non-core** della rete.

Due entità: UK National Cybersecurity Center (**NCSC**) e lo Huawei Cybersecurity Evaluation Center (**HC-SEC**)

- cooperano con gli operatori di rete e con il vendor Huawei per:
  - → ridurre i rischi
  - → valutare la **sicurezza** sia degli **apparati** che delle **configurazioni** di rete.

L'HC-SEC ha un board **indipendente** ed ha pubblicato delle specifiche su come gli apparati di Huawei debbano essere sviluppati:

- →il divieto di sviluppare capacità di **intercettazione legali** con Huawei e Zte
- →divieto di creare connessioni **Vpn**
- →obbligo di effettuare le attività di **manutenzione** attraverso gli operatori di rete.

Possibili misure per minimizzare rischi

Di seguito una serie di misure proposte dal think tank tedesco Stiftung Neue Verantwortung

1. Standard e implementazione

a. Security **assessment** sui **processi** di **sviluppo** dei vendor e **certificazione** di sicurezza sui **prodotti It** (NESAS by GSMA e 3GPP).

b. Sviluppo di **schemi** di **certificazioni** obbligatori per le **apparecchiature di rete mobile** nel quadro del **Cybersecurity Act** europeo (basato su o complementare a GSMA e NESAS).

2. Configurazione

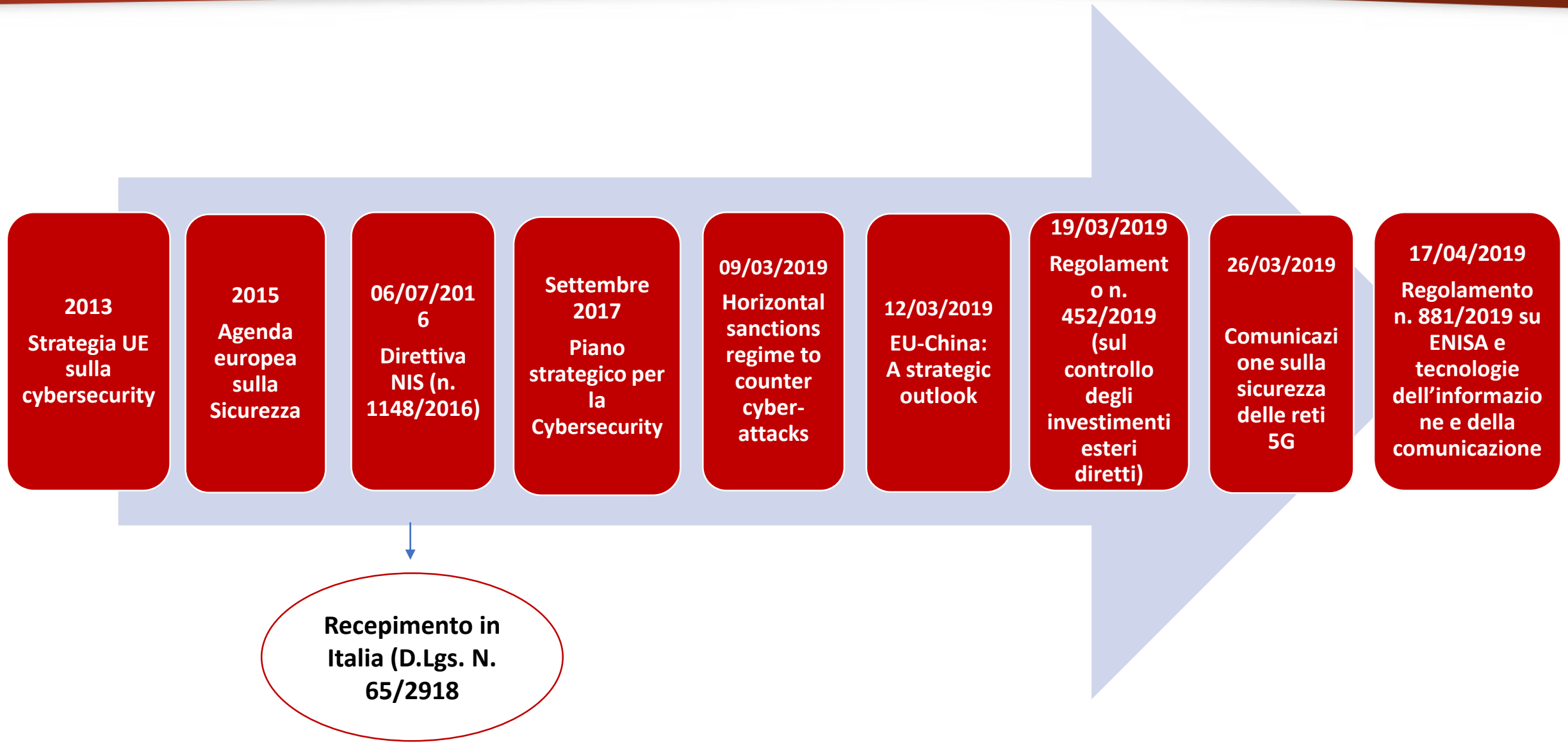
a. Sviluppo di **requisiti nazionali** relativi a configurazione di sicurezza su **apparecchiature** di **rete** mobile tra **operatori** e **agenzie nazionali** per la sicurezza.

3. Procedure e manutenzione

a. Sviluppo di **requisiti nazionali** relativi a **configurazione** di **sicurezza** di **reti mobili** (es. requisiti per i processi di sviluppo software o manutenzione da remoto).

b. Risk analysis continuativa e "**mitigation**" tra **operatore**, **vendor** e le **agenzie** di sicurezza nazionale.

Il framework europeo sulla sicurezza



Il Cybersecurity Act

Cybersecurity Act (Regolamento n. 881/2019 del 17 aprile 2019):

- ✓ ha fissato gli obiettivi, i compiti e gli aspetti organizzativi relativi all'**ENISA**
- ✓ ha fissato un quadro per l'introduzione di **sistemi europei di certificazione della cybersecurity** al fine di garantire un livello adeguato di cybersecurity dei prodotti TIC, servizi TIC e processi TIC nell'Unione ed evitare la frammentazione del mercato interno per quanto riguarda i sistemi di certificazione della cybersecurity nell'Unione
- ✓ ha fissato un'ampia gamma di obiettivi di sicurezza ed individuato diversi livelli di affidabilità dei prodotti, servizi e processi TIC (di base, sostanziale ed elevato)
- ✓ ha prescritto la designazione, da parte degli Stati membri, di una o più autorità nazionali di certificazione della cybersecurity nel proprio territorio oppure, con l'accordo di un altro Stato membro, la designazione di una o più autorità nazionali di certificazione della cybersecurity stabilite in tale altro Stato membro affinché siano responsabili dei compiti di vigilanza nello Stato membro designante
- ✓ ha istituito il **Gruppo europeo per la certificazione della cybersecurity**, composto da rappresentanti delle autorità nazionali di certificazione della cybersecurity o da rappresentanti di altre autorità nazionali competenti, con compiti di assistenza, proposta, collaborazione e consulenza nei rapporti con la Commissione ed ENISA

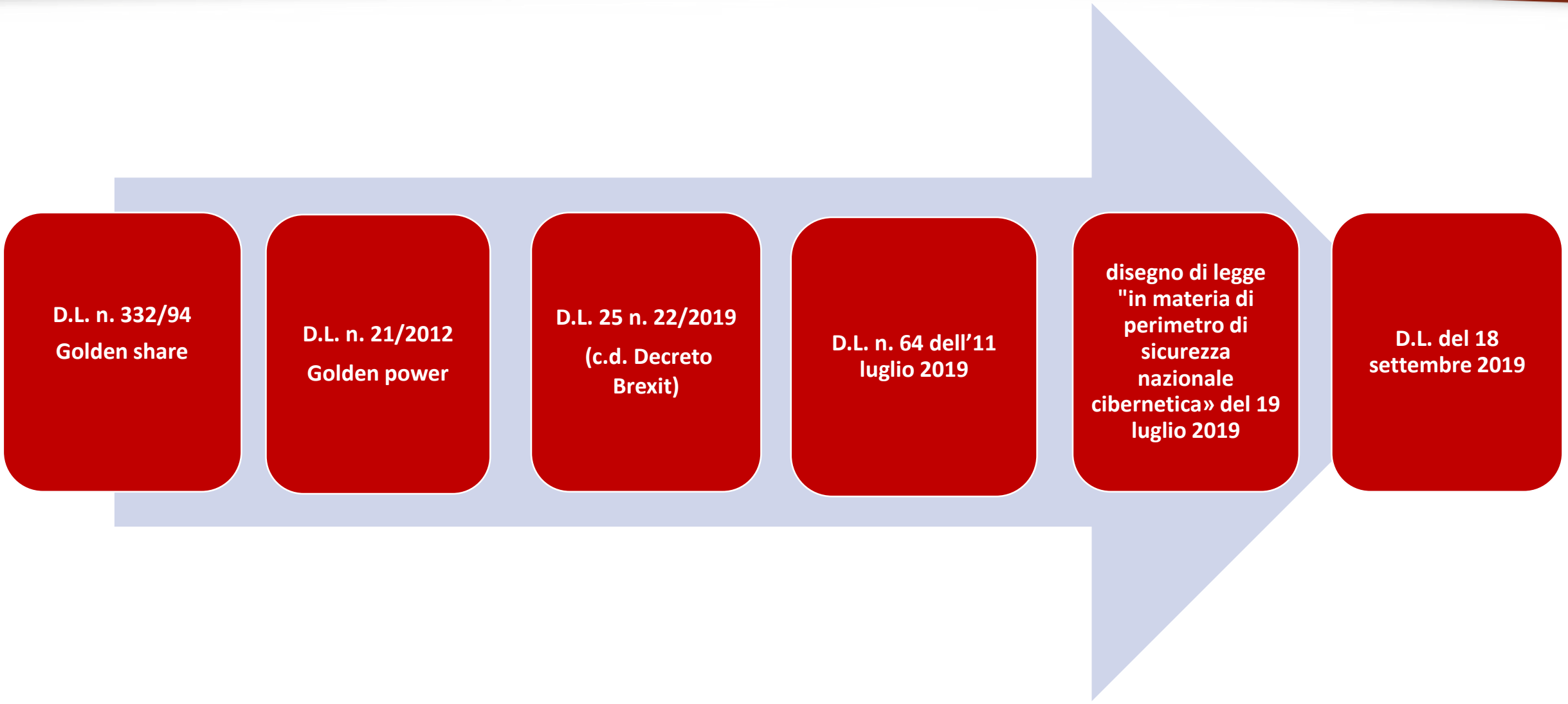
La Raccomandazione n. 2019/534 sulla cybersecurity delle reti 5G (26 marzo 2019)

- ✓ La Commissione ha evidenziato i rischi di cybersecurity nelle reti 5G e presentato **orientamenti s**ulle opportune misure di analisi e gestione dei rischi a livello nazionale, sullo sviluppo di una valutazione dei rischi coordinata a livello europeo e sulla definizione di un processo per lo sviluppo di un insieme di strumenti comuni volti a garantire la migliore gestione dei rischi.

- ✓ Da considerare **fattori tecnici e fattori ulteriori e diversi** (requisiti normativi o di altro tipo imposti ai fornitori di apparecchiature per le tecnologie dell'informazione e della comunicazione, il modello di governance esistente nel Paese analizzato, il rischio generale di influenza da parte di un paese terzo, l'assenza di accordi di cooperazione sulla sicurezza etc.)

- ✓ **Roadmap**: 1) completamento, entro il 10 ottobre 2019, da parte degli Stati membri, con il sostegno della Commissione e dell'ENISA, di una revisione congiunta dell'esposizione a livello di Unione ai rischi relativi alle infrastrutture alla base dell'ecosistema digitale, in particolare delle reti 5G; 2) sulla base di tali migliori pratiche nazionali, condivisione, entro il 31 dicembre 2019, di un insieme di possibili misure di gestione dei rischi adeguate, efficaci e proporzionate al fine di attenuare i rischi di cybersecurity individuati a livello nazionale e di Unione, che orienterà la Commissione nello sviluppo di requisiti minimi comuni a ulteriore garanzia di un elevato livello di cybersecurity delle reti 5G in tutta l'Unione (tale **insieme di strumenti** dovrebbe comprendere **un inventario** dei tipi di rischi di sicurezza e una serie di possibili **misure di attenuazione**).

Dalla golden share al golden power. La sicurezza delle reti 5G



Conclusioni e spunti di policy 1/3

Il **decreto 64 dell'11 luglio 2019**, sebbene non convertito, sollecita riflessioni su alcuni importanti aspetti in esso contenuti:

1. **LO STRUMENTO NORMATIVO UTILIZZATO.** Applicazione più difficile nel caso del processo di verifica degli apparati, che di fatto è dilatato nel tempo.
   - è preferibile la predisposizione di un **protocollo di certificazione** che si applica **continuativamente**, da parte di un ente certificatore – verosimilmente il **CVCN** del MiSE
   - preferibile **coinvolgimento** dei **vendor** e degli stessi **operatori di rete** – con procedure pragmatiche e neutrali rispetto alla concorrenza
   - garantire sicurezza, rapidità di esecuzione e apertura mercato

2. **LA LIMITAZIONE NEI CONFRONTI DI PAESI EXTRA EUROPEI**. La scelta, evidentemente riconducibile a considerazioni di carattere geopolitico, rischia **di non risultare efficace in termini di sicurezza**, **non essendo a priori escludibile una minaccia** a opera delle altre imprese (o di loro fornitori/clienti).

3. **LA POSSIBILE DILATAZIONE TEMPORALE**. Prevista dal decreto legge non convertito dal precedente Governo, con un'estensione da 15 a 45 giorni.
   - da una parte la disponibilità di un maggior arco temporale dovrebbe consentire una **maggiore ponderazione** da parte dell'Esecutivo
   - dall'altra **rischia di frenare** la dinamicità **imprenditoriale** assolutamente imprescindibile nella realizzazione delle reti 5G

4. **LE POSSIBILI SANZIONI**. Meritano approfondite riflessioni
   - per l'ammontare (fino al doppio delle operazioni) e per il potere attribuito al Governo di ingiungere all'impresa acquirente e all'eventuale controparte il **ripristino**, a proprie spese, della situazione **precedente**
   - in considerazione del potenziale **effetto negativo sugli investimenti** e sull'**attrattività** del sistema Paese verso l'estero

Conclusioni e spunti di policy 2/3

Il **D.L. approvato dal CdM** il 18 settembre 2019 appare disinnescare alcune potenziali problematiche che avrebbe introdotto il decreto legge di luglio, anche se permangono alcune preoccupazioni:

- considerato l'orizzonte attuativo previsto dal decreto (entro 10 mesi dalla data di entrata in vigore), si palesa il rischio di creare un clima di **generale incertezza** in grado di impattare negativamente sugli investimenti e lo sviluppo delle reti 5G
- è fondamentale **assicurare il rispetto dei termini previsti** dal decreto per l'adozione dei decreti e del regolamento che definiranno termini e procedure
- va assicurata la piena operatività del **CVCN** con la massima urgenza
- in generale va minimizzato il rischio di una **dilatazione delle tempistiche**

Conclusioni e spunti di policy 3/3

IN CONCLUSIONE, 3 CRITERI DA TENERE PRESENTI:

1. **BILANCIAMENTO TRA SICUREZZA E COMPETITIVITÀ**. La sicurezza nazionale va perseguita e garantita, sapendo che non potrà mai essere garantita un'imperforabilità delle reti al 100%, coniugandola con la crescita economica del Paese e servizi sempre più evoluti offerti alle imprese e ai cittadini.

2. **TEMPISTICHE**
   - garantire certezza sul ritorno degli investimenti e sugli ulteriori investimenti da effettuare per tutti gli attori coinvolti nella realizzazione delle reti 5G

3. **NORMATIVA ARMONIZZATA**. È forte la necessità che, almeno a livello europeo, si arrivi a una **normativa unica o a forme di certificazione unificate**.
   - es. **NESAS** (sviluppato congiuntamente dal 3GPP e dalla GSMA proprio per superare le criticità dovute ad una moltiplicazione e sovrapposizione di requisiti di sicurezza dei singoli Stati)
   - **coinvolgimento** di operatori di rete, vendor e istituzioni per la definizione di un **protocollo di certificazione.**