Elon Musk, attacco frontale alle telco Usa. Acquisite le frequenze per il 5G

Ha fatto rumore l'acquisizione da parte di **Elon Musk** delle frequenze in banda 800 MHz per una somma di 8 miliardi di dollari da un fondo d'investimento. Una mossa che rivela appieno l'obiettivo del miliardario di entrare a piedi uniti nell'arena del mobile negli Usa. Lo scrive *Les Echos* in un'analisi che analizza il nuovo quadro.

Starlink Mobile entra a gamba tesa nel mercato del mobile

Sì perché d'ora in poi **Starlink Mobile**, che finora si era tenuta come dire in disparte dedicandosi soltanto alle aree non coperte e alle zone rurali, potrà puntare direttamente sui ricchi mercati urbani.

Se in Europa, per ora, Starlink non dispone ancora di frequenze cosiddette mobili, in grado di penetrare all'interno di edifici, negli Usa le cose sono cambiate dopo l'annuncio della scorsa settimana. Si ricorda che la banda 800 MHz è fatta apposta per la navigazione indoor in zone densamente popolate, come le città.

Questa acquisizione fa il paio con l'operazione da 19,5 miliardi di dollari dello scorso anno, quando Starlink rilevò le frequenze dell'operatore **EchoStar**.

Telco Usa a picco in Borsa

L'annuncio dell'operazione sulla banda 800 MHz fatto giovedì scorso ha subito affossato i titoli delle telco americane, che

in borsa hanno ceduto rispettivamente il 7,3 % per **AT&T**, 6,6 % per **Verizon** e **T-Mobile Usa**, per una perdita cumulativa virtuale di 37 miliardi di dollari.

L'onda lunga delle perdite ha contagiato anche le telco europee. **Deutsche Telekom** (casa madre di **T-Mobile), Vodafone, Orange** e **Telefonica** hanno lasciato sul terreno rispettivamente l'8 %, il 4,5 %, il 3,4 % e il 3,3 %.

Starlink Mobile, attacco frontale alle telco Usa

L'acquisizione di licenze nella banda degli 800 MHz dal fondo statunitense **Grain Management** è destinata a scuotere gli operatori tradizionali: come annunciato quest'estate, Starlink Mobile sta lanciando un attacco frontale. L'azienda potrà trasmettere il segnale 5G a terra, penetrare negli edifici e garantire una copertura migliore delle aree urbane: tutti aspetti che mancavano alla sua attuale offerta mobile "direct-to-device", basata su 700 satelliti dedicati. Gli analisti di **Morgan Stanley** considerano l'operazione un chiaro segnale della volontà di SpaceX di acquisire ulteriori frequenze.

Una rete ancora ridotta

Sulla carta, tuttavia, gli operatori statunitensi avevano motivi per restare tranquilli. *"La banda degli 800 MHz consente di implementare il 5G, ma con velocità di trasmissione inferiori; quanto all'ampiezza di spettro acquisita – 14 MHz – non c'è da aspettarsi miracoli se confrontata con quella dei tre operatori già presenti sul mercato, che dispongono complessivamente di 1.000 MHz",* osserva **Jean-Baptiste Thépaut**, Principal presso Novaspace.

L'ampiezza dello spettro è paragonabile al diametro di un tubo: con una misura simile, Starlink Mobile non potrà gestire un numero elevato di abbonati simultaneamente, limitando di

conseguenza la velocità di trasmissione. *“Le sue ambizioni sono inoltre frenate dalle frequenze disponibili sul mercato. Le opportunità sono scarse, fatta eccezione per* ***Anterix****, che detiene 10 MHz nella banda dei 900 MHz, attualmente poco utilizzati”*, aggiunge l’analista. SpaceX ha già manifestato interesse per queste risorse. E c’è da giurarci che l’intenzione sarà quella di accrescere la sua dotazione frequenziale in futuro, non appena si presenterà l’occasione, magari anche rilevando di sana pianta un operatore tradizionale.

Starlink non dispone né di antenne né di torri mobili

Inoltre, l’autorità statunitense per le telecomunicazioni **(FCC)** imporrà ora a Starlink l’effettivo utilizzo delle nuove frequenze. Tuttavia, l’aspirante operatore mobile non dispone né di antenne 5G a terra né di torri di trasmissione. Secondo **Jean-Baptiste Thépaut**, interpellato da Les Echos, *“l’azienda potrebbe cercare di far riconoscere l’uso della tecnologia satellitare per rispettare le prime scadenze normative, guadagnando così tempo prezioso per implementare una vera e propria rete mobile terrestre”*.

Serve l’appoggio delle tower company

Implementare l’infrastruttura significa installare antenne sui tralicci delle cosiddette *“towerco”*, società il cui modello di business punta proprio a massimizzare il numero di locatari per sito… e che avrebbero quindi tutto l’interesse a ospitare le antenne 5G di Elon Musk. *“Gli operatori storici non ne hanno alcun interesse e potrebbero esercitare pressioni contrarie”*, osserva l’analista.

Un nuovo status

Quanto alla costruzione di torri proprietarie, sebbene non sia un'impresa spettacolare come il lancio di una costellazione spaziale, si tratta di un'operazione costosa, soprattutto su un territorio vasto come quello statunitense. Secondo gli analisti di **Bernstein**, per realizzare una rete mobile nazionale credibile negli Stati Uniti, **SpaceX** dovrebbe investire 70 miliardi di dollari e installare 57mila siti nell'arco di otto anni. A Wall Street, le società **American Tower, Crown Castle** e **SBA Communications** hanno registrato rialzi compresi tra il 6,7% e l'8,3%, spinte dalla prospettiva di nuovi ricavi da locazione.

Minaccia concreta: Starlink potrebbe partecipare alle prossime aste frequenze negli Usa

Sebbene restino ancora molti passi da compiere, la minaccia per gli operatori "tradizionali" è concreta. *"Questa acquisizione permetterà a SpaceX di entrare nel mercato delle telecomunicazioni terrestri e di acquisire un nuovo status"*, sottolinea l'analista. Elon Musk si siede così al tavolo degli operatori mobili tradizionali e potrebbe partecipare alle prossime aste per le frequenze organizzate dalla FCC.

Nuove aste in arrivo negli Usa

Il calendario potrebbe giocare a suo favore: il 29 ottobre, l'autorità di regolamentazione delle telecomunicazioni dovrà pronunciarsi sull'asta per un blocco di frequenze da 25 MHz, suddiviso tra le bande 1.675-1.695 MHz e 2.020-2.025 MHz. Una nuova opportunità per SpaceX di ampliare il proprio portafoglio di frequenze, anche se si preannuncia una forte concorrenza da parte di **Amazon Leo** e **AST SpaceMobile**.

Starlink sta di fatto diventando il quarto operatore mobile negli Usa

“Starlink sta diventando di fatto il quarto operatore mobile degli Stati Uniti; Elon Musk sta mettendo piede nel settore e ciò che conta è la mossa strategica. Non entra in questo mercato solo per una porzione così ridotta di spettro. D’ora in poi adotterà una strategia opportunistica sistematica di acquisizione di frequenze, o arriverà addirittura ad acquisire un operatore”, osserva **Stéphane Lelux**, CEO della società di consulenza Tactis.

Aggiunge inoltre che la porzione di spettro acquisita oggi ha anche una valenza commerciale, poiché *“Starlink potrà raggiungere gli attuali clienti della telefonia mobile senza necessità di aggiornamenti hardware”.* Si tratta di clienti potenzialmente attratti dalla *“potenza di marketing di Musk, che potrebbe integrare il suo chatbot Grok nei piani tariffari mobili”*, prosegue l’analista.

Infine, secondo l’esperto, *“un operatore già presente sul mercato potrebbe voler stipulare un accordo di roaming con Starlink”*, rappresentando questa l’unica soluzione per ritrovare slancio in un mercato ormai maturo. E per Elon Musk, significherebbe raggiungere una massa critica, *“come Orange e Free nel settore mobile”*.

The post Elon Musk, attacco frontale alle telco Usa. Acquisite le frequenze per il 5G appeared first on Key4biz.

https://www.key4biz.it/elon-musk-attacco-frontale-alle-telco-usa-acquisite-le-frequenze-per-il-5g/590912/

6G, 2,4 miliardi di connessioni globali entro il 2035 (un quarto in Europa)

Il primo miliardo di connessioni 6G entro il 2033 secondo GSMA

Le reti **6G** sono in arrivo. Se ne parla da molto tempo, sono stati eseguiti i primi test, ma entro il 2030 si attendono i lanci commerciali veri e propri. È quanto assicurato dagli studiosi della GSMA Intelligence, che si aspettano **50 milioni di connessioni mondiali in 6G già per il 2030**.

Dalla fine del decennio in poi inizierà ufficialmente la transizione delle telecomunicazioni mobili di nuova generazione, che vedrà coesistere 5G e 6G. Le stime della GSMA sono più che ottimiste, con un trend di crescita notevole delle connessioni 6G che passeranno rapidamente da 275 milioni nel 2031 a 740 milioni nel 2032.

Il primo miliardo di connessioni 6G si dovrebbe raggiungere già nel 2033, per poi raddoppiare nel 2034 e attestarsi quindi a 2,4 miliardi nel 2035.

Una cavalcata notevole su scala globale, quella attesa dai ricercatori britannici, trainata dalla domanda di rete e dalla crescita del **traffico dati**, che è **stimato passare dagli attuali 144 exabyte (EB) mensili ai 604 di fine 2035**.

AI primo driver del boom di

connessioni 6G

I principali driver sono al momento i video, ma presto la fonte principale di traffico sarà rappresentata dall'intelligenza artificiale (AI), seguita dalla realtà estesa (XR), che abiliterà sempre nuove applicazioni in termini di fotocamere, sensori e apparecchiature esterne collegate in wireles con smartphone o pc.

L'AI è destinata a influenzare lo sviluppo del **6G lungo due direttrici**. Da un lato, le reti dovranno supportare un numero crescente di applicazioni e dispositivi basati sull'AI; dall'altro, la stessa intelligenza artificiale dovrebbe diventare sempre più integrata nel funzionamento delle infrastrutture di rete.

Questa evoluzione potrebbe consentire una maggiore automazione di funzioni come **l'allocazione delle risorse, l'ottimizzazione delle reti e la gestione dei consumi energetici**.

Anche la **Next G Alliance** individua nelle cosiddette **reti AI-native**, cioè progettate fin dall'origine per integrare l'intelligenza artificiale, un elemento centrale della propria roadmap per il 6G. L'obiettivo è migliorare **robustezza, prestazioni ed efficienza delle reti**, mentre diventano sempre più complessi i tipi di traffico da gestire, le architetture di implementazione e gli scenari di utilizzo dello spettro radio.

L'alba di una nuova industria?

In questo modo si va a modificare direttamente la natura della domanda di rete, perché i device connessi creano, modificano e trametton contenuti continuamente, accelerando la crescita di capacità di uplink, il potenziale di latenza e il livello di affidabilità.

Più in generale, il **6G punta a una maggiore integrazione tra**

comunicazioni e capacità di calcolo, all'impiego di nuove tecnologie radio e nuove porzioni di spettro, alla connettività di una gamma più ampia di dispositivi e ambienti e a livelli più elevati di automazione delle reti.

Il valore del 6G potrebbe quindi andare **ben oltre un ulteriore aumento della velocità di download degli smartphone**. Per l'industria, la questione più importante sarà capire se queste nuove capacità riusciranno a tradursi in **nuovi servizi, maggiore efficienza delle reti e casi d'uso commercialmente sostenibili**, difficili da realizzare con le infrastrutture di telecomunicazione attuali.

Un traffico dati quattro volte superiore a quello attuale, servirà più spettro e reti automatizzate

Il traffico dati, inoltre, è destinato a crescere a un ritmo annuo di circa il 15% nel prossimo decennio, secondo quanto riportato dallo studio. In questo modo, **entro il 2035 le reti dovranno gestire un volume di traffico più di quattro volte superiore a quello attuale**. Per far fronte a questa domanda sarà necessaria una combinazione di maggiore efficienza delle reti, capacità aggiuntiva e nuove risorse di spettro.

Per quanto riguarda la quantità di spettro necessaria, l'analisi **Vision 2040 della GSMA** stima che, tra il 2035 e il 2040, potrebbero servire **2-2,5 GHz di spettro nelle bande medie (mid-band)** per soddisfare la domanda nelle aree ad alta densità di popolazione. Il fabbisogno potrebbe salire a **2,4-3,3 GHz** nei Paesi caratterizzati da una domanda più elevata.

A titolo di confronto, nella maggior parte dei Paesi oggi è destinato ai servizi mobili circa **1 GHz di spettro nelle bande medie**. L'analisi indica quindi la necessità di **1-2 GHz**

aggiuntivi di spettro mid-band, parallelamente a ulteriori miglioramenti dell'efficienza spettrale e a una maggiore densificazione delle reti.

L'Europa sembra già muoversi nella direzione di uno sfruttamento più efficiente della capacità di spettro comunitaria. Lo spettro radio potrebbe diventare, ad esempio, uno dei nuovi strumenti con cui l'Unione europea potrebbe finanziare la propria autonomia tecnologica. Secondo la proposta elaborata dal presidente dell'Eurogruppo e ministro greco **Kyriakos Pierrakakis**, si potrebbe creare di una sorta di **"Unione europea dello spettro"**, attraverso la quale una parte dei ricavi delle future assegnazioni nazionali delle frequenze 6G verrebbe destinata a investimenti comuni nelle tecnologie strategiche.

Oltre la metà delle connessioni in Nord America, un quarto in Europa

L'esplosione delle connessioni 6G non sarà comunque omogena e uniforme su scala planetaria, ma a velocità differenziate da continente a continente e soprattutto sarà concentrata in alcuni Paesi. Ad esempio, ci si aspetta che oltre la metà delle connessioni sarà attivata in Nord America entro il 2035, più di un terzo in Asia e circa un quarto in Europa.

Differenze anche notevoli, legate ad un diverso ritmo dei cicli tecnologici (3G>4G>5G>6G). Molti paesi sono ancora impegnati nella maturazione delle reti 4G, altri nel passaggio dal 4G al 5G, altri ancora nella diffusione capillare del 5G, una parte invece sfrutterà una buona copertura 5G per effettuare il primo salto nello standard 6G.

The post 6G, 2,4 miliardi di connessioni globali entro il 2035 (un quarto in Europa) appeared first on Key4biz.

https://www.key4biz.it/6g-24-miliardi-di-connessioni-globali-e

ntro-il-2035-un-quarto-in-europa/589407/

Inwit, conti in calo ma stime confermate. Galli: “Impegno a investire”

Nel secondo trimestre **Inwit** ha realizzato ricavi pari a 267 milioni, in flessione dello 0,8%; l’Ebitda è stato pari a 240,7 milioni (-2,1%). L’Ebitda after leasing si è attestato su 190,9 milioni (-2,8%). L’utile netto è risultato di 79,3 milioni, in calo del 15,2 per cento.

Galli: “Inwit conferma la sua capacità industriale”

“Inwit – ha commentato il direttore generale **Diego Galli** – *conferma la propria capacità industriale, dimostrata dalla realizzazione di progetti complessi come il piano Italia 5G per l’eliminazione del digital divide in 500 kmq del territorio, e l’impegno a investire nello sviluppo strategico delle infrastrutture di telecomunicazione a supporto della crescita dell’industria e della digitalizzazione del Paese. I risultati del secondo trimestre rilfettono il contingente contesto industriale con contrazione degli utili e degli investimenti; i risultati sono in linea con la guidance che prevede il ritorno alla crescita del business nel 2027. In relazione alle controversie legali conseguenti alle disdette degli Msa (da parte di Tim e Fastweb + Vodafone ndr) la società ha presentato reclamo avverso le ordinanze del tribunale di Milano, convinti della fondatezza delle nostre*

ragioni”.

Inwit conferma la guidance 2026 e il medium-term baseline outlook.

Gli investimenti industriali, si legge nella nota sui conti, sono stati pari a 49,8 milioni, in calo del 22,7% rispetto allo stesso trimestre 2025. Il recurring free cash flow si è attestato a 123,9 milioni di euro, in diminuzione del 21,6% rispetto allo stesso periodo del 2025. L’indebitamento finanziario netto, pari a 5.453,3 milioni (inclusivo delle passività finanziarie IFRS16) risulta in aumento (+10,4%) rispetto al 30 giugno 2025, essenzialmente a sostegno degli investimenti e della remunerazione degli azionisti; in aumento (+8,5%) rispetto al primo trimestre 2026. La leva finanziaria, in termini di rapporto tra indebitamento netto ed Ebitda, è in aumento a 5,7volte rispetto al 5,0x del secondo trimestre 2025 per l’incremento dell’indebitamento finanziario netto; in aumento rispetto al 5,2x del primo trimestre 2026.

Resta l’incertezza nel mercato Tlc

Quanto all’evoluzione prevedibile della gestione per l’esercizio 2026 e outlook di medio-termine, lo scenario macroeconomico di riferimento è caratterizzato dal persistere di elementi di incertezza, quali ad esempio le aspettative sull’inflazione e i tassi d’interesse, che rimangono elevati. Nel breve termine, nel mercato italiano delle telecomunicazioni persistono significativi elementi di difficoltà, tra cui l’elevata competizione e la limitata generazione di cassa, con impatto sugli investimenti.

In questo contesto, tuttavia*, “si conferma il modello di business infrastrutturale di **Inwit**, che grazie alle sinergie derivanti dalla condivisione degli asset e alla solida esperienza industriale, garantisce la massima efficienza ai*

propri clienti creando valore per tutte le parti coinvolte“.

Stime per il 2026

La società ha riflesso queste condizioni di mercato nelle stime per il 2026 e per il medio termine, come già riportate anche nel Bilancio Integrato 2025. Nel 2026 si prevedono ricavi nel range 1.050-1.090 milioni di euro; Ebitda margin pari a circa il 90%; EbitdaaL margin pari a circa il 72%; recurring free cash flow nel range 550-590 milioni di euro; dividendo per azione almeno pari al valore dell’esercizio 2025 (confermato ad 0,55 euro per azione); leva finanziaria a 5,5 volte, confermando il target strutturale di leva finanziaria tra 5x e 6 volte.

Inwit, inoltre ritiene che l’outlook baseline di medio termine, in un contesto di limitata visibilità sull’evoluzione delle condizioni del mercato, si fondi su alcuni pilastri tra cui: crescita annuale dei ricavi “low single digit”; continua espansione del margine EbitdaaL, capex annuali (incluso acquisto di terreni) pari a circa euro 200 milioni; dividendo per azione almeno pari a 0,55 euro.

Potenziali upside esclusi

Questo outlook, precisa la nota, non include i potenziali upside relativi al ristabilirsi di una relazione costruttiva con gli anchor, all’oggettivo bisogno di densificazione richiesto sia dalla continua crescita del traffico dati in mobilità, che dalla necessità di completare e densificare la copertura indoor e outdoor e dall’opportunità di espandersi lungo la filiera delle infrastrutture digitali.

Inwit: conferma impegno a

collaborare con clienti in quadro di certezza

Inwit conferma, il proprio impegno a sostenere l'evoluzione delle reti mobili e a collaborare con i propri clienti in un quadro di certezza, trasparenza e stabilità, perseguendo, con rigorosa logica industriale, soluzioni di valore che garantiscano efficienza e benefici condivisi per tutte le parti. E' quanto si legge nella nota sui conti del secondo trimestre.

I principali clienti di **Inwit**, Tim e Fastweb + Vodafone, hanno disdettato gli accordi Msa, decisione a cui è seguita una controversia legale con la towerco.

Inwit: deposita i 2 reclami in tribunale contro decisioni a favore di Tim e Fastweb

Negli ultimi mesi, si è assistito ad un incremento della conflittualità con gli anchor tenants formalizzato nelle disdette degli Msa ricevute a marzo 2026, finalizzate a ottenere *"una squilibrata e ingiustificata rinegoziazione dei contratti Msa, validi ed efficaci, a giudizio della società, fino al 2038".* Lo ricorda Inwit a proposito della controversia giudiziaria aperta con i suoi due principali clienti Tim e Fastweb dopo le disdette degli Msa.

Reclami cautelari

"A seguito del rigetto da parte del tribunale di Milano delle istanze cautelari promosse dalla società in via d'urgenza, ex art. 700 del codice di procedure civile, contro le disdette presentata da Tim e Fastweb, Inwit – afferma la società confermando le notizie dei giorni scorsi – *ha provveduto a*

depositare, rispettivamente il 27 luglio 2026 e 28 luglio 2026, due distinti reclami cautelari avverso tali ordinanze”.

Novità su Google, per aggiungere Key4Biz tra le tue fonti preferite, clicca qui

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/inwit-conti-in-calo-ma-stime-confermate-galli-impegno-a-investire/583061/

5G standalone, WINDTRE Business testa con successo la rete di emergenza allo stadio Maradona per il concerto di Geolier

- Test realizzato da WINDTRE Business e ASL Napoli 1 Centro, con la supervisione scientifica dell’Università di Napoli Federico II, durante il concerto di Geolier

allo Stadio Maradona con circa 50.000 spettatori provenienti da tutta Italia.
- La soluzione basata su 5G Standalone e Network Slicing ha garantito continuità delle comunicazioni voce e dati tra ambulanza e centrale operativa anche in condizioni di elevata congestione della rete.
- I risultati confermano l'efficacia del 5G nel supportare servizi sanitari mission-critical, aprendo nuove prospettive per le comunicazioni di emergenza e la sanità digitale.

Una rete 5G dedicata all'emergenza allo stadio Maradona, durante il concerto di Geolier. Il network slicing e le reti 5G standalone cominciano a fare sul serio, dimostrando le loro potenzialità sul campo durante un evento di massa con migliaia di persone connesse contemporaneamente in un breve lasso di tempo.

Un importante passo avanti nell'applicazione delle tecnologie 5G a supporto della sanità e delle comunicazioni di emergenza è stato compiuto da **WINDTRE Business, ASL Napoli 1 Centro** e **Università di Napoli Federico II**, che hanno realizzato una sperimentazione sul campo durante il concerto di Geolier allo Stadio Maradona uno degli eventi musicali più partecipati dell'anno.

Il network slicing e il 5G standalone cominciano dunque ad entrare nel vivo, con casi d'uso sempre più diffusi e indicativi delle potenzialità di questa tecnologia che apre la strada a una miriade di applicazioni dedicate.

Sperimentazione chiusa con successo: connesse ambulanze e centrale operativa

L'obiettivo della sperimentazione era valutare la capacità delle comunicazioni di emergenza di mantenere elevati livelli

di affidabilità in uno scenario particolarmente sfidante, caratterizzato dalla presenza di circa 50mila spettatori e da un intenso utilizzo della rete mobile. In queste condizioni, assimilabili a quelle che possono verificarsi durante grandi eventi pubblici o situazioni straordinarie, è stata testata una soluzione basata su 5G Standalone e network slicing, sviluppata per garantire la continuità delle comunicazioni tra le ambulanze e la centrale operativa. Il test prevedeva la simulazione di comunicazioni voce e trasmissioni dati tra un mezzo di soccorso e la centrale operativa dell'ASL Napoli 1. I risultati hanno evidenziato la piena continuità dei collegamenti, la stabilità del servizio anche in presenza di elevati livelli di congestione della rete e l'efficacia delle funzionalità del 5G nel supportare applicazioni a elevata criticità operativa.

Validazione sul campo del network slicing

L'attività rappresenta un'importante validazione sul campo delle potenzialità del network slicing, una tecnologia che consente di creare porzioni virtuali dedicate della rete mobile, riservando capacità e priorità ai servizi essenziali. In contesti caratterizzati da un forte affollamento e da volumi di traffico elevati, questa architettura permette di garantire prestazioni affidabili ai servizi di emergenza, contribuendo a rafforzare la resilienza delle comunicazioni sanitarie. La supervisione scientifica dell'**Università di Napoli Federico** II ha consentito di valutare in modo rigoroso le prestazioni della soluzione in un ambiente reale e particolarmente complesso, fornendo un importante contributo alla ricerca e allo sviluppo di applicazioni innovative per la sanità digitale e la gestione delle emergenze.

Michele Lucantonio (WINDTRE Business): “Confermato ruolo strategico del 5G standalone in ambito sanitario”

“Questa sperimentazione conferma il ruolo strategico del 5G Standalone come abilitatore di servizi innovativi ad elevato valore sociale”, dice **Michele Lucantonio**, PA & Utilities Direct Sales Director. *“I risultati ottenuti dimostrano come il network slicing sia in grado di assicurare continuità e affidabilità alle comunicazioni critiche anche in condizioni di massima congestione della rete, aprendo nuove prospettive per l’evoluzione dei servizi di emergenza e per la digitalizzazione del sistema sanitario”.*

Fulvio Paone (Asl Napoli 1 Centro): “Sperimentazione primo passo per comunicazioni più affidabili”

Fulvio Paone, Direttore U.O.C. Informatizzazione e Transizione Digitale della ASL Napoli 1 Centro, ha detto: *“La trasformazione digitale della sanità passa anche attraverso tecnologie capaci di supportare i servizi di emergenza nei contesti più complessi. I risultati di questa sperimentazione confermano il valore del 5G e del network slicing nel garantire prestazioni elevate anche in condizioni di forte congestione della rete. La sperimentazione rappresenta un primo passo per rafforzare e rendere sempre più sicure ed affidabili le comunicazioni tra il campo e la centrale operativa, soprattutto in situazioni emergenziali complesse, contribuendo a migliorare il coordinamento dei soccorsi e l’efficacia degli interventi a beneficio dei cittadini.”*

Nicola Pasquino (Università Federico II): “Una corsia preferenziale in una autostrada intasata”

“Immaginiamo uno stadio con migliaia di persone connesse nello stesso momento: far passare una comunicazione di emergenza in queste condizioni è come aprire una corsia preferenziale in un’autostrada intasata. È esattamente ciò che consente il network slicing, riservando risorse dedicate ai servizi critici anche sotto carico massimo. La possibilità di misurare in modo rigoroso le prestazioni del 5G Standalone durante un evento reale così sfidante ci ha permesso di validare sul campo l’affidabilità di questa tecnologia a supporto dei soccorsi. Un esempio concreto di come la collaborazione tra università, operatori e istituzioni sanitarie possa tradurre l’innovazione in benefici reali per la sicurezza dei cittadini” ha detto **Nicola Pasquino**, Professore di Misure Elettriche ed Elettroniche dell’Università di Napoli Federico II.

La sperimentazione conferma come le reti mobili di nuova generazione possano diventare un elemento sempre più centrale nell’evoluzione dei servizi di pubblica utilità, contribuendo a rendere più efficaci, tempestive e affidabili le comunicazioni a supporto della sicurezza dei cittadini e delle attività di soccorso.

Domande Frequenti

- Che cos’è il Network Slicing testato da WINDTRE Business a Napoli? È una tecnologia avanzata delle reti 5G Standalone che consente di *“affettare”* virtualmente la rete mobile, creando corsie preferenziali protette dedicate esclusivamente a servizi essenziali o di

emergenza. In questo modo, la linea dei soccorsi non subisce rallentamenti anche se lo stadio è affollato.

- Qual è il vantaggio pratico del 5G applicato alle ambulanze? Come confermato dal test con l'ASL Napoli 1 Centro, permette a un'ambulanza di trasmettere in tempo reale e senza alcuna interruzione dati clinici, parametri vitali del paziente e flussi voce verso la centrale operativa, ottimizzando la tempestività dei soccorsi medici prima dell'arrivo in ospedale.
- Chi ha certificato la validità scientifica di questa sperimentazione? La supervisione scientifica e la misurazione rigorosa delle prestazioni di rete in tempo reale sono state curate dal team del Professor Nicola Pasquino, docente di Misure Elettriche ed Elettroniche presso l'Università degli Studi di Napoli Federico II.

Novità su Google, per aggiungere Key4Biz tra le tue fonti preferite, clicca qui

Leggi le altre notizie sull'home page di Key4biz

https://www.key4biz.it/5g-standalone-windtre-business-testa-con-successo-la-rete-di-emergenza-allo-stadio-maradona-per-il-concerto-di-geolier/579728/

La Linea 1 entra nell’era della connettività: Napoli accende il 4G e il 5G in metropolitana

Napoli compie un nuovo passo verso la trasformazione digitale. Da oggi la copertura mobile 4G e 5G è disponibile lungo l’intero percorso della Linea 1 della metropolitana, consentendo ai passeggeri di restare connessi senza interruzioni anche nelle gallerie e nelle stazioni sotterranee.

L’attivazione del servizio è stata celebrata martedì 30 giugno con una videochiamata effettuata dalla stazione Municipio dall’assessore comunale alla Transizione Digitale e Smart City, **Valerio Di Pietro**. A seguire si è svolto il convegno “Connessi al futuro”, promosso da **Cellnex** con il patrocinio del **Comune di Napoli**, in collaborazione con **ANM** e organizzato da *Key4Biz*.

L’intervento rappresenta molto più di un semplice miglioramento della copertura telefonica. La nuova infrastruttura digitale costituisce infatti la base tecnologica sulla quale potranno svilupparsi nuovi servizi per la mobilità, la sicurezza, il turismo e la gestione intelligente della città.

La connettività come primo tassello della smart city

Per l’assessore **Valerio Di Pietro** l’attivazione del servizio segna un cambio di paradigma.

“Questa mattina abbiamo fatto una ottima prova dimostrativa di questa connessione 4G e 5G. Fare una videochiamata fino a qualche giorno fa era impensabile. Si tratta di un tassello importante nel percorso di digitalizzazione, che consente agli utenti di poter fruire meglio del trasporto metropolitano per motivi di svago, lavoro e turismo. Avere connettività per quella mezz’ora che stai in banchina e in treno è importante – dice l’assessore – *Importante anche per ragioni di sicurezza e*

questioni di emergenza. Oggi all'interno della Linea 1 è possibile".

Si tratta quindi di un assaggio importante per i cittadini ma anche per l'amministrazione di Napoli e per tutta la rete. "*Perché si consente di usare la connettività e nell'immaginare una smart city del futuro è l'infrastruttura più importante per aggiungere in futuro altri sistemi hardware. Primo passo per una Napoli smart city del futuro e marcare un cambio di passo sostanziale per queste tematiche".*

L'infrastruttura invisibile che

abilita i servizi

Il ruolo dell'infrastruttura è stato al centro dell'intervento di **Federico Protto**, presidente e amministratore delegato di **Cellnex Italia**, che ha evidenziato come il valore del progetto stia proprio nella sua capacità di rendere la tecnologia "*invisibile*" agli utenti. *"Quello che noi abbiamo abilitato è una tecnologia. Ieri sono entrato in metropolitana, non ho visto le tecnologie ma in compenso le tecnologie ci sono eccome e il 4G e il 5G è ottimo, c'erano 150 persone in banchina e fruivano tutte di una connettività ottima. Tutto ciò permette un'esperienza senza interruzioni da quando siamo fuori a quando entriamo in banchina e anche sul treno. E sul treno la copertura è anche migliore, essendoci una copertura dedicata".*

Protto (Cellnex Italia): "Nelle nostre città italiane copertura in metropolitana meglio di Londra"

Il tutto considerato che la copertura nei tunnel della metropolitana è complessa e I'impatto visivo dei DAS (Distributed Antenna System) è stato minimo: *"E' un impianto multi operatore, neutrale, noi siamo il neutral host aperto a tutti gli operatori* – aggiunge Protto – *Napoli è una città a forte vocazione turistica: i turisti si aspettano questa copertura, così come i cittadini. Lasciamenti dire con una punta di orgoglio che nelle principali città italiane abbiamo questo tipo di copertura, mentre in una città come Londra non c'è la copertura in metropolitana, quindi è un orgoglio italiano che le nostre grandi città siano coperte".*

Napoli si pone così all'avanguardia anche relativamente ad altre aree del digitale come il supercomputer, il gemello digitale e la prima smart road in Italia realizzata in tangenziale. "*La base è la copertura 4G e 5G di alto livello,*

il prossimo passaggio per Cellnex sarà la Linea 6. Sicuramente il sistema di connettività è il sistema nervoso con cui possiamo abilitare tutti i servizi, sono orgoglioso che Napoli sia all'avanguardia".

Dal PNRR ai nuovi servizi digitali

Per **Marco Bellezza**, amministratore delegato di di Eutalia, in rappresentanza del Dipartimento per la Trasformazione Digitale, la conclusione del PNRR apre una nuova fase: quella della valorizzazione delle infrastrutture realizzate. *"Stamattina siamo arrivati a 9mila e passa scuole connesse, superando il target del PNRR* – dice Bellezza – *Nell'ambito del digitale il PNRR la connettività è stata una parte cospicua.*

Tanti operatori si sono impegnati a creare il substrato tecnologico per abilitare nuovi servizi. *I dati della Commissione europea mostrano che negli ultimi cinque anni l'Italia ha registrato un trend positivo nella digitalizzazione."*

ANM: Sicurezza, mobilità e nuovi servizi

Dal punto di vista di **Azienda Napoletana Mobilità (ANM)**, dell'azienda che gestisce il trasporto pubblico di Napoli, la disponibilità della connettività apre scenari completamente nuovi. **Francesco Favo**, Direttore Generale ANM: *"Noi siamo l'esercente, quindi sfruttiamo l'infrastruttura. Ad oggi l'infrastruttura è già attrezzata. Avere tutta la infrastruttura coperta dà vantaggi in termini di sicurezza* per la *sorveglianza. Oggi possiamo fare tutto. Il paradigma cambia. Adesso possiamo sapere dove si trovano i treni per la geolocalizzazione. Adesso avremo maggiori oneri di sicurezza e dobbiamo confrontarci. Un focus sulla cybersicurezza. Dovremo comunicare meglio con i cittadini. Questo tema sarà spostato anche sugli autobus e sulla sosta. Questo è un tema di smart city per migliorare la mobilità di Napoli".*

Un progetto nato nel 2019

Serena Riccio, Responsabile Area Infrastrutture di Trasporti, Comune di Napoli ANM, ha ripercorso il lungo iter che ha portato alla realizzazione dell'intervento. *"La Linea 1 della metropolitana è l'asse portante della mobilità di Napoli. Una linea così moderna non poteva non avere la connessione per percezione di sicurezza e sicurezza personale. L'iter è stato travagliato è partito nel 2019 ma serve una volontà politica. L'esecuzione è stata complessa. Anche la lavorazione è stata complessa, le finestre di lavoro sono state molto ridotte. Lavoro complesso ma alla fine ci siamo riusciti. Il futuro è la Linea 6".*

La rete digitale della città

Edoardo Fusco, Responsabile Area Infrastrutture di Trasporti del Comune di Napoli ha illustrato gli investimenti del Comune nelle infrastrutture digitali cittadine. *“Il Comune di Napoli ha investito 14 milioni di euro per il digitale. Tutti gli impianti semaforici sono dotati di sensori intelligenti per leggere i flussi veicolari. Il prossimo step a questo punto è usare il 5G. Abbiamo attrezzato le gallerie con sistemi di videosorveglianza. Tutti questi interventi si collegano alla necessità di una presenza sempre più completa del 5G”.*

Gli operatori: la collaborazione è la chiave

Nel secondo panel gli operatori telefonici hanno ribadito che lo sviluppo delle reti richiede infrastrutture condivise e collaborazione tra pubblico e privato. **Luciano Ausiello**, South Deployment & Maintenance Operations Director di WindTre: *"L'esperienza della Linea 1 della metropolitana di Napoli dimostra concretamente che la collaborazione tra operatori e soggetti infrastrutturali non è più una semplice opportunità, ma una condizione necessaria per accelerare lo sviluppo della connettività nel nostro Paese*".

"La condivisione di infrastrutture e investimenti consente di ottimizzare le risorse, ridurre tempi e costi di realizzazione e portare servizi sempre più performanti nei territori già coperti, favorendone al tempo stesso l'estensione verso nuove aree strategiche e produttive. Le collaborazioni già avviate, anche con tower company come Cellnex, confermano l'efficacia di un modello fondato sulla cooperazione industriale e sulla neutralità delle infrastrutture, prosegue Ausiello. La vera sfida dei prossimi anni sarà rafforzare questa convergenza strategica nello sviluppo delle reti, lasciando alla competizione il compito di valorizzare innovazione, qualità dei servizi ed esperienza dei clienti. I risultati raggiunti finora sono importanti e testimoniano i benefici concreti di questo approccio, ma il potenziale di crescita resta ancora molto ampio. Continuare a fare sistema sarà determinante per rendere la connettività un fattore sempre più decisivo per la competitività, la sostenibilità e la trasformazione digitale dei territori", conclude il manager".

Domenico Ferro, Head of Architecture & Demand di TIM: *"Oggi il cittadino entra in metro e dà per scontata la connettività. Si abilitano tutti i servizi digitali che i cittadini si aspettano".*

Massimiliano Gasparroni, CTSO di Fastweb + Vodafone: *“Senza l’infrastruttura di base questi servizi non sono possibili. Nuovi servizi migliorano Napoli, proiettandola nel futuro”.*

Ersilia Manzo, CTO di Iliad: *“Quando la connettività entra nei contesti pubblici diventa un diritto essenziale. La metropolitana è stata una scommessa vinta”.*

Il modello Napoli

A chiudere i lavori è stato **Alessandro Prosdocimo**, di Cellnex Italia, che ha indicato nella collaborazione tra amministrazione pubblica, gestori della mobilità e operatori il vero valore del progetto. *“Cellnex ha scommesso sulla sinergia delle infrastrutture una decina di anni fa. Creare infrastrutture condivise permette di indirizzare gli investimenti e permette a una tower company di creare una rete condivisa, agli operatori di creare servizi e ai cittadini di fruire dei servizi digitali. Abbiamo voluto replicare qui a Napoli il modello Milano nella metropolitana. C’era la volontà di portare i servizi al cittadino. Esiste il partenariato pubblico-privato per realizzare infrastrutture che possono portare beneficio alla società e ai cittadini. Dovremmo spingere perché questo diventi una leva di sviluppo per il Paese”.*

Lo sguardo al futuro della mobilità

Nelle conclusioni dell’incontro è intervenuto anche **Alfonso Pecoraro Scanio**, presidente della Fondazione UniVerde, che ha richiamato il valore delle infrastrutture digitali come elemento sempre più strategico per coniugare innovazione, sostenibilità e qualità dei servizi pubblici, sottolineando come la trasformazione delle città passi dalla capacità di integrare tecnologie e mobilità.

A chiudere i lavori è stato l’assessore alle Infrastrutture e

Mobilità del Comune di Napoli, **Edoardo Cosenza**, che ha inserito il progetto della copertura 4G e 5G della metropolitana all'interno della più ampia strategia di sviluppo della città. *"Un grazie a tutto e tutti. La Linea 1 si apre e si vede la storia. Questa è l'unica città che ha lasciato l'impianto e le direttrici greco-romane. Siamo una città proiettata verso il futuro, pensiamo all'America's Cup. Tecnologia ovunque. Il sindaco Manfredi, che è un ingegnere come me, pensa alla tecnologia di queste barche che hanno a bordo tecnologie all'avanguardia. Partiamo da questa bellissima operazione di Cellnex, a Londra non c'è la stessa connettività. Noi avremo nel 2027 una connettività completa in 5G. La Linea 1 fa 140mila passeggeri al giorno, abbiamo tolto 120mila passaggi di automobile al giorno e in un anno siamo a +23% di passeggeri rispetto all'anno scorso".*

Novità su Google, per aggiungere Key4Biz tra le tue fonti preferite, clicca qui

Leggi le altre notizie sull'home page di Key4biz

https://www.key4biz.it/la-linea-1-entra-nellera-della-connettivita-napoli-accende-il-4g-e-il-5g-in-metropolitana/577938/

Il Comune di Napoli accende il 4G e il 5G sulla Linea 1 della metro. Il sindaco Manfredi: “La città sempre più tecnologica”

Napoli è sempre più digitale. Martedì 30 giugno, è stata ufficialmente *“accesa”* la copertura **4G** e **5G** lungo l’intera Linea 1 della metropolitana con una videochiamata, nella stazione *“Municipio”*, da parte di **Valerio Di Pietro**, Assessore alla Transizione Digitale e Smart City del Comune di Napoli. A seguire, si è tenuto il convegno *“Connessi al futuro”,* nella Sala della Giunta comunale a Palazzo San Giacomo con i principali attori del progetto. L’evento è stato promosso dalla tower company europea **Cellnex**, con il **patrocinio del Comune di Napoli** e in collaborazione con **ANM – Azienda Napoletana Mobilità**, ed è stato organizzato dal quotidiano **Key4Biz**.

[embedded content]

4G e 5G a bordo della Linea 1 della metropolitana: i vantaggi per la città, i cittadini e turisti

Il progetto 4G e 5G nella metropolitana Linea 1, realizzato da **Cellnex** (attraverso soluzioni **DAS** – Distributed Antenna Systems), in collaborazione con il **Comune di Napoli** e**ANM** – **Azienda Napoletana Mobilità** – abilita una connettività mobile stabile e ad alte prestazioni nelle 16 stazioni e in tutte le gallerie della Linea, contribuendo a migliorare sia la navigazione, le telefonate e le videochiamate di cittadini e

turisti sia a rafforzare il ruolo delle infrastrutture di TLC per lo sviluppo di servizi digitali nella città.

Obiettivo è estendere la connettività alla Linea 6

Nel realizzare il progetto, **Cellnex** ha predisposto ulteriore capacità infrastrutturale per ospitare più operatori, contribuendo alla razionalizzazione degli interventi di rete e alla diffusione di servizi mobili ad alte prestazioni. L'obiettivo è estendere prossimamente la connettività 4G e 5G anche sulla Linea 6.

Il Sindaco Manfredi: "Passo in avanti in una città sempre più tecnologica"

"*Il potenziamento della connettività lungo la Linea 1 della Metropolitana, una delle infrastrutture di mobilità più importanti del territorio cittadino, è un punto strategico per quest'Amministrazione. Non soltanto garantisce a cittadini e turisti la possibilità di navigare in 4G e 5G, in banchina e durante il viaggio, ampliando l'offerta di servizi, ma costituisce un notevole passo in avanti in una città che punta sempre di più sull'innovazione tecnologica*", così il **sindaco Gaetano Manfredi**.

Cosenza: "La Linea 1 ha superato 44,5 milioni di passeggeri"

"*Con la connessione 4G e 5G nelle stazioni della Linea 1 della metropolitana di Napoli* – ha detto **Edoardo Cosenza, assessore alle Infrastrutture, Mobilità e Protezione civile** del Comune di Napoli – *si amplia l'offerta di servizi agli utenti sempre*

più numerosi. Basti pensare che la Linea 1 ha superato i 44,5 milioni di passeggeri nell'ultimo bilancio consolidato. I dati più recenti evidenziano una crescita verticale della frequentazione, con circa 2 milioni di passeggeri in più rilevati nei soli primi mesi rispetto ai record dell'anno precedente. Ai tanti passeggeri occorre offrire un servizio sempre più efficiente ed efficace. L'obiettivo, nello specifico, è avere la piena connettività in tutte le stazioni e lungo le gallerie nella Linea 1, ma in seguito anche nella Linea 6, perché garantire una copertura del segnale cellulare stabile e performante nella rete di trasporti pubblici è uno dei fattori chiave per trasformare una città, e la sua rete di trasporti, in una città intelligente".

Di Pietro: "Oggi la connettività non è più un semplice accessorio"

"*L'attivazione della connettività 5G sulla Linea 1* – ha evidenziato l'assessore alla Transizione Digitale e Smart City del Comune di Napoli, **Valerio Di Pietro** – *rappresenta un ulteriore passo avanti nel percorso di innovazione dei servizi pubblici della nostra città. La qualità di una Smart City si misura anche dalla capacità di offrire servizi digitali avanzati nei luoghi che i cittadini vivono ogni giorno, a partire dal trasporto pubblico. Oggi la connettività non è più un elemento accessorio, ma una componente essenziale della vita quotidiana: cittadini, studenti, lavoratori e turisti utilizzano dispositivi sempre più evoluti e hanno bisogno di poter contare su connessioni veloci, stabili e affidabili anche durante gli spostamenti. Questo investimento si inserisce in una visione complessiva: migliorare costantemente la qualità del trasporto urbano e accompagnare la trasformazione della città attraverso infrastrutture sempre più moderne ed efficienti*".

Favo (ANM): “4G e 5G a 40 metri di profondità non era scontato”

“*Le stazioni e i tunnel della Linea 1 della Metropolitana di Napoli si sviluppano a profondità considerevoli, in alcuni casi fino a 40 metri sotto il livello stradale. Garantire ai nostri passeggeri una connessione mobile stabile e di qualità in queste condizioni rappresenta quindi una sfida tecnologica significativa. L’attivazione della copertura 4G e 5G a queste profondità non è un risultato scontato e costituisce un importante passo avanti nel percorso di innovazione e miglioramento continuo dei servizi offerti da ANM, contribuendo a rendere gli spostamenti più confortevoli, sicuri e connessi per cittadini e turisti che ogni giorno scelgono la metropolitana per muoversi in città*“, ha commentato **Francesco Favo Direttore Generale e Amministratore Delegato di ANM**.

Protto (Cellnex): “Passo concreto per una città sempre più connessa”

“*L’attivazione del 4G e 5G sulla Linea 1 della metropolitana di Napoli rappresenta un passo concreto verso un modello di città sempre più connessa, efficiente e inclusiva. Le infrastrutture digitali sono oggi un elemento abilitante fondamentale per migliorare la qualità della vita di cittadini e turisti e per sostenere lo sviluppo economico dei territori. Come Cellnex, siamo orgogliosi di aver contribuito a questo progetto attraverso un modello di infrastruttura condivisa e neutrale, capace di ottimizzare gli investimenti degli operatori e accelerare la diffusione di servizi mobili ad alte prestazioni anche in contesti complessi come le metropolitane. Napoli dimostra come la collaborazione tra pubblico e privato possa tradursi in risultati tangibili per la comunità e rappresenti un esempio virtuoso per altre grandi aree urbane.*

Continueremo a lavorare, insieme alle istituzioni e ai partner industriali, per estendere questi benefici e accompagnare la transizione digitale del Paese», ha commentato **Federico Protto, Presidente & CEO di Cellnex Italia.**

Novità su Google, per aggiungere Key4Biz tra le tue fonti preferite, clicca qui

Leggi le altre notizie sull'home page di Key4biz

https://www.key4biz.it/il-comune-di-napoli-accende-il-4g-e-il-5g-sulla-linea-1-della-metro-il-sindaco-manfredi-la-citta-sempre-piu-tecnologica/577902/

TLC, Zorzoni (AIIP): "Basta assistenzialismo regolatorio. Il rilancio passa da concorrenza, Cloud e reti

vere”

Una parte dell’industria italiana delle telecomunicazioni continua a fare i conti con investimenti difficili, reti da completare, PNRR agli sgoccioli, nuove regole europee e un mercato che rischia di essere raccontato sempre dalla stessa prospettiva: quella dei grandi operatori.

Ne abbiamo parlato con **Giovanni Zorzoni**, vicepresidente AIIP, per fare il punto su Piano Italia 1 Giga, Fondo Nazionale Connettività, 5G standalone, Digital Networks Act, Cloud, concorrenza e ruolo degli operatori territoriali.

Key4biz. ***I fondi del PNRR sono agli sgoccioli. Come è andata dal suo punto di vista con Italia 1 Giga e Piano Italia 5G?***

Giovanni Zorzoni. L’esito era largamente prevedibile e, purtroppo, su questo siamo stati facili profeti. Il tempo a disposizione era pochissimo, gli obiettivi molto ambiziosi e, in queste condizioni, l’unico soggetto con un vantaggio operativo reale era la società dell’ex rete TIM, oggi **FiberCop**. Non per superiorità metafisica, ma per una ragione molto concreta: dispone della rete storica di infrastrutture fisiche già presenti sul territorio, compresa una rete capillare di pali in legno o vetroresina nelle aree periferiche, cioè proprio quelle più difficili da coprire.

Key4biz. ***Perché la rete di pali è così importante?***

Giovanni Zorzoni. Il tema dei pali è centrale e troppo spesso viene trattato come un dettaglio tecnico. Non lo è affatto. Portare fibra in case sparse, frazioni, strade secondarie e civici lontani, potendo appendere i cavi su infrastrutture già esistenti, cambia completamente l’economia dell’intervento. Scavare costa, richiede permessi, cantieri, ripristini e coordinamento con gli enti locali. Usare una palificata già esistente costa molto meno e consente tempi più rapidi.

Key4biz. ***Cambia qualcosa in termini di copertura?***

Giovanni Zorzoni. Sì perché questo non significa che la rete aerea sia la soluzione migliore: una rete scavata bene, ordinata e manutenibile è in generale superiore a una rete costruita inseguendo una scadenza. Ma se si impongono tempi quasi impossibili da rispettare, si finisce per premiare chi può riutilizzare infrastrutture storiche e già ammortizzate, non necessariamente chi avrebbe progettato la rete migliore per i prossimi vent'anni. La lezione è semplice: la spesa pubblica deve generare infrastrutture robuste, non soltanto rendicontazioni ordinate.

Key4biz. ***Avete criticato il bando con i 733 milioni di euro del Fondo Nazionale Connettività per la copertura dei civici rimanenti rimasti fuori da Italia 1 Giga dopo la rinuncia di Open Fiber. Perché?***

Giovanni Zorzoni. Perché era formalmente aperto, ma sostanzialmente accessibile solo a chi aveva già un'infrastruttura nazionale capillare. Il risultato non ha sorpreso nessuno: FiberCop è stata l'unico operatore su tutti i lotti. Quando una gara pubblica produce un solo concorrente reale, il problema non è il mercato, ma come è stata costruita la gara.

Key4biz. ***In che senso?***

Giovanni Zorzoni. Il vantaggio decisivo è sempre lo stesso: le infrastrutture storiche dell'ex monopolista. FiberCop usa i suoi pali. Gli altri, per competere, devono scavare ex novo o affittare quelle infrastrutture dal concorrente. Uno parte con la strada pronta, gli altri devono chiedere il permesso di costruirla, pagando il pedaggio. Non è così che si costruisce un mercato plurale.

Key4biz. ***È necessario un decreto Telecomunicazioni, come richiesto dall'industria?***

Giovanni Zorzoni. Dipende da cosa si intende. Se “decreto Telecomunicazioni” significa l’ennesimo pacchetto di vantaggi selettivi per pochi grandi operatori, la risposta è no. Sconti, proroghe, frequenze gratuite, regole più comode e interventi presentati come politica industriale ma pensati per alleggerire singoli bilanci: sono misure che possono mascherare alcuni problemi nel breve termine, a costo di aggravarli già nel medio. Non rafforzano la competitività, ma distorcono il mercato e sussidiano inefficienze.

Key4biz*. Cosa serve invece per l’AIIP?*

Giovanni Zorzoni. Altra cosa sono gli strumenti che stimolano davvero la domanda e producono benefici per tutto il comparto. Da tempo attendiamo **voucher cloud e cybersecurity**, che aiuterebbero le imprese italiane, soprattutto PMI, a svecchiare infrastrutture ICT, sicurezza, gestione dei dati e servizi digitali. Quella è domanda buona: crea mercato, fa crescere competenze, rafforza il tessuto produttivo.

Lo stesso vale per i voucher destinati agli allacci delle famiglie, in particolare quelli onerosi. In molti casi il problema non è la mancanza astratta di tecnologia, ma il costo concreto dell’ultimo tratto. Se poi questo strumento accelera il passaggio dal rame alla fibra, dovrebbe essere una buona notizia, non un disturbo da gestire con prudenza.

C’è poi un settore molto importante per il digitale, l’agricoltura italiana. Masserie, aziende agricole, filiere rurali: lì servono connettività reale, cloud, sensoristica, controllo remoto, sicurezza, gestione affidabile e sicura dei processi già automatizzata. Un euro pubblico messo lì genera valore, molto più che quello destinato a ennesimi interventi *“ad hoc”* che beneficiano pochi grandi.

Key4biz. *Il 5G standalone è indietro in Italia. Come incentivarlo? La richiesta delle telco di un’allocazione non onerosa dello spettro in cambio di impegni di investimento è*

una soluzione adeguata per accelerare la copertura?

Giovanni Zorzoni. No. Il 5G standalone non si incentiva regalando spettro. È la solita scorciatoia: si prende un bene pubblico scarso, le frequenze, e lo si trasforma in sostegno indiretto ai bilanci degli operatori mobili. Dietro obiettivi nobili quanto generici – innovazione, competitività e transizione digitale – si rischia di invalidare, a vantaggio ancora di pochi grandi attori, consolidati principi di corretta gestione del patrimonio pubblico.

Il 5G standalone è indietro per un motivo semplice: gli operatori radiomobili non hanno voluto investirvi. I casi d'uso sono stati raccontati con troppa enfasi, ma la realtà è che il 5G è stato sovrastimato e oltremodo spinto, anche finanziariamente, dall'UE, con risultati gravemente insoddisfacenti. Prima doveva cambiare tutto, poi è arrivato il standalone, domani sarà il 6G. Intanto il mercato mobile, dopo la telefonia, ha prodotto solo Internet mobile. Utile, ma non è la rivoluzione permanente raccontata nei convegni.

Key4biz. ***Cosa bisognerebbe fare allora per incentivare il 5G?***

Giovanni Zorzoni. Se lo Stato vuole davvero incentivare il 5G, deve permettere a più soggetti di usarlo, non solo agli operatori radiomobili. Parlo del 5G privato su bande gratuite all'interno di sedime privato, come già si fa in Germania. Solo così vedremmo un proliferare di usi reali nei distretti produttivi, nei porti, nella logistica, in agricoltura, nella sanità. Non regalando spettro a chi ha già dimostrato di non saperlo sfruttare.

Quanto agli impegni di investimento in cambio di frequenze non onerose: le promesse costano poco. Se si discutono rinnovi o proroghe, servono obblighi misurabili, verificabili, territorialmente puntuali, con penali vere e decadenza dei diritti in caso di mancato rispetto. Altrimenti non è politica industriale, è credito regolatorio senza garanzie: solo una

totale regolamentazione di un pieno servizio bistream wholesale sul 5G potrebbe avere come contropartita equilibrata uno sconto sui rinnovi delle frequenze.

Key4biz. ***Il Digital Networks Act è in discussione a Bruxelles: quali sono le principali criticità dal punto di vista di AIIP?***

Giovanni Zorzoni. La prima è il cambio di filosofia: DNA non è una manutenzione tecnica, è un tentativo di spostare poteri dalle autorità nazionali alla Commissione Europea, un organo non eletto e non sfiduciabile. Si passa da un modello in cui **AGCOM** analizza i mercati e definisce rimedi, a uno più accentrato, rigido, insensibile alle differenze tra Paesi e territori.

Per noi è un punto enorme. Le reti non sono tutte uguali. L'Italia non è la Germania, la Lombardia non è la Calabria, un operatore territoriale non è un ex monopolista. Governare tutto da Bruxelles con un modello uniforme significa scrivere regole eleganti sulla carta e dannose nella pratica.

Key4biz. ***Qual è la seconda criticità?***

Giovanni Zorzoni. La seconda criticità è il consolidamento: per decenni l'Europa ha messo al centro la concorrenza. Nel DNA emergono parole ambigue: competitività europea, campioni continentali, semplificazione. Tradotto: meno operatori, più grandi, più vicini al potere politico e finanziario. Una prospettiva che ci preoccupa.

Poi ci sono spettro, switch-off del rame, net neutrality. Le frequenze non sono rendite a vita da prorogare. Il rame va spento, ma con tempi realistici, non date calate dirigisticamente da Bruxelles, e compatibilmente con le capacità di assorbimento del sistema paese, del delivery e della realizzazione degli impianti nell'unità di tempo. La sicurezza delle catene di fornitura deve essere pura cybersecurity, non geopolitica contro l'interesse degli Stati

Membri: i rapporti internazionali, e ancor più la sicurezza nazionale, sono riconosciuti dagli stessi trattati come ambiti di competenza primaria degli Stati membri! E la neutralità della rete va difesa, senza reintrodurre il "fair share" che è solo una tassa sulle piattaforme per ripianare i bilanci degli ex monopolisti, ma pretendendo che finalmente il GDPR non sia rispettato solo dalle aziende Europee.

Key4biz. ***Il mercato fisso rischia di restare bloccato tra rame, prezzi wholesale e migrazione alla fibra?***

Giovanni Zorzoni. Il mercato non rischia di restare fermo, anzi. La direzione di questo movimento, tuttavia, dipenderà dal senso che daremo a obiettivi in realtà tutt'altro che univoci.

Da sempre, per noi *"fibra ottica"* significa *"vera"* fibra ottica, fino a dentro casa, ma altri soggetti vi ricomprendevano invece reti in misto rame. Analogamente, lo *"switch-off"* per noi significa passaggio alla fibra ottica, ma già abbiamo sentito letture del termine più ambigue, funzionali a far rimanere i clienti sul rame, riducendo i costi, dismettendo solo i POP, le centrali, con un enfatico -65% come si apprende dal memo Fibercop "NetBook".

Key4biz. ***Cosa pensate della nuova politica di prezzo di FiberCop per l'accesso alla rete?***

Giovanni Zorzoni. E' un'altra novità dirompente, non soltanto per gli operatori al dettaglio, ma per le imprese e le famiglie italiane. Con i nuovi listini FiberCop, oggetto della Comunicazione AGCOM del 23 aprile 2026 e relativo *"avvio della verifica delle proposte di FiberCop per i servizi wholesale dei Mercati 1B e 2B"*, ai sensi della delibera 58/26/CONS. Dopo la qualifica di FiberCop come operatore wholesale-only – qualifica che per AIIP è erronea – vediamo proposte di aumento su servizi essenziali: componenti passive, costi di cessazione, kit, colocazione, servizi accessori. Non è una

questione marginale. Sono i costi su cui gli operatori costruiscono offerte retail, investimenti e migrazioni dei clienti verso la fibra.

Key4biz. ***Per FiberCop si tratta della logica conseguenza del passaggio al nuovo status di operatore wholesale only, con l'adeguamento graduale dei prezzi alla media europea.***

Giovanni Zorzoni. Il rischio è che il passaggio da prezzi orientati al costo a prezzi *"equi e ragionevoli"* diventi una deregulation di fatto. Per noi *"equo e ragionevole"* significa ancora dimostrabile, trasparente, coerente con i costi sottostanti. Ci sono costi di disattivazione (!) che sono aumentati dell'440% sulla vecchia rete in rame… parliamo di 50€ di disattivazione per eseguire uno shutdown di una porta su un cabinet stradale con un prezzo precedente di 10€ già esoso? Se il servizio diventa talmente caro da impedire l'uscita di un contratto o rispettare i costi del contratto già in essere con il cliente finale la libertà di scelta degli operatori diventa solo teorica. Questo si chiama lock-in economico. Punto.

Se le cosiddette fibre primarie diventano più costose perché le centrali vengono accorpate e le tratte si allungano, non siamo davanti a una maggiore prestazione richiesta dagli operatori. Siamo davanti a una scelta di rete di FiberCop scaricata sul mercato. Sono profili fortemente tecnici che difficilmente arrivano nel dibattito pubblico, ma se AGCOM non interverrà in modo deciso, a fine anno si scaricheranno sugli italiani aumenti finora impensabili nelle telecomunicazioni.

A questo si aggiunge il tema **CUP (Canone Unico Patrimoniale)**, che profila rischi esistenziali per moltissimi operatori territoriali: alcune interpretazioni rischiano di produrre richieste sproporzionate verso aziende che non controllano grandi infrastrutture fisiche, ma rivendono o integrano servizi di accesso di terzi. Si stanno producendo esiti manifestamente irragionevoli, e e sono quasi esauriti i

margini temporali per un intervento legislativo che riconduca il CUP nei parametri della proporzionalità e della non distorsività. Confidiamo che il Governo possa intervenire con un emendamento entro l'inizio di settembre, prima che si producano conseguenze occupazionali irreparabili.

Insomma, il mercato non è fermo, siamo anzi in una fase di transizione, in cui si prospettano però direzioni non necessariamente positive per il sistema paese.

Key4biz. ***Nel memo "NetBook" di FiberCop c'è un dato che secondo voi merita particolare attenzione?***

Giovanni Zorzoni. Sì, il dato più interessante è quello sul traffico medio per linea attiva. Va letto bene, perché FiberCop precisa che si tratta delle linee che terminano sui propri apparati, escludendo quindi quelle servite da infrastrutture di altri operatori. Non è il traffico complessivo di una regione, ma il traffico che resta dentro il perimetro tecnico di FiberCop. Ed è proprio qui che il dato diventa interessante (tra l'altro questo memo fa capire perché il CUP lo devono pagare gli operatori infrastrutturali e non gli operatori retail: dimostra chi "accende i cavi", e non ne è solo proprietario).

In diverse regioni del Nord, cioè nelle aree economicamente più forti del Paese, il traffico medio per linea risulta inferiore alla media nazionale: Piemonte, Friuli Venezia Giulia, Trentino Alto Adige, Liguria e Valle d'Aosta sono sotto il dato medio italiano. La Lombardia, che è il motore economico dello Stivale, è appena sopra. Al contrario, alcune regioni del Centro-Sud e delle isole, come Lazio, Campania, Calabria e Sicilia, risultano sopra media.

La lettura industriale, a mio avviso, è abbastanza chiara. Dove esiste più concorrenza infrastrutturale, quindi reti territoriali realizzate da operatori di AIIP, oltre a **Open Fiber** e **Fastweb**, una parte della clientela più evoluta e più

esigente potrebbe essere uscita dal perimetro FiberCop. Dove invece la concorrenza infrastrutturale è più debole, o dove storicamente la rete dell'ex monopolista è rimasta dominante anche grazie a importanti piani pubblici sulla FTTC, il traffico continua a concentrarsi maggiormente su quella rete.

Non è una prova contabile di perdita di clientela, per quello servono altri indicatori: ricavi, abbandoni, ARPU, nuove attivazioni. Ma è un segnale industriale da non sottovalutare. Se nelle aree più ricche e più competitive il traffico medio sulle linee FiberCop non cresce in modo proporzionale, la domanda è inevitabile: FiberCop sta trattenendo davvero la clientela più avanzata, o sta soprattutto conservando quella ancora legata alla sua infrastruttura storica?

Key4biz. ***TIM e Fastweb + Vodafone hanno avviato un percorso di RAN sharing sul mobile. Che ne pensate?***

Giovanni Zorzoni. Dipende dalle condizioni. La condivisione di infrastrutture mobili può avere senso nelle aree meno dense: riduce duplicazioni, accelera coperture, permette di usare meglio energia, siti e apparati. Nessuno qui vuole la religione dello spreco, con tre tralicci accanto soltanto per dimostrare che il mercato esiste. Ma il punto è un altro: quando la condivisione riguarda soggetti molto rilevanti e porzioni importanti del mercato, non può essere trattata come una semplice ottimizzazione tecnica.

Se due grandi blocchi industriali condividono porzioni significative della rete di accesso radio, allora bisogna parlare seriamente di vero wholesale mobile, non quello che abbiamo visto sinora: offerte commerciali complicate, fragili, negoziate caso per caso, che rendono la vita difficile agli operatori mobili virtuali e agli operatori territoriali. Parliamo del bistream dati su rete mobile: rinnovi di frequenze a prezzi calmierati e/o accordi di RAN sharing devono avere come imposizione il vero wholesale bistream dati della rete mobile e non certo su "*slicing*" a bassa velocità,

bensì sulla stessa slice che i grandi operatori mettono i propri clienti.

Altrimenti il rischio è sempre lo stesso: si chiama efficienza ciò che nella pratica diventa consolidamento. Si dice che si vogliono ridurre costi per investire, poi però il mercato a valle resta chiuso o semi-chiuso. AIIP non è contraria alla cooperazione infrastrutturale quando serve. È contraria alle cooperazioni chiuse che privatizzano il controllo del mercato. Se la rete mobile diventa più condivisa, l'accesso deve diventare più aperto. Le due cose devono stare insieme, altrimenti manca metà del ragionamento.

Key4biz. ***Il tema dei vendor cinesi e della cybersecurity è diventato centrale. Qual è la posizione di AIIP?***

Giovanni Zorzoni. La sicurezza è una cosa seria e non va trasformata, come si sta facendo da anni, in propaganda. La cybersecurity deve basarsi su criteri tecnici, oggettivi, verificabili: codice, processi, vulnerabilità, aggiornamenti, gestione delle chiavi, audit, supply chain, risposta agli incidenti. In AIIP sappiamo di cosa parliamo, perché molti di noi nel weekend fanno glitching su CPU di sistemi embedded, invece di andare a farsi una passeggiata. Se invece il criterio principale diventa la provenienza geografica del fornitore, allora siamo in un altro campo: geopolitica e sicurezza nazionale.

Sono temi legittimi, ma vanno chiamati con il loro nome, e sono temi che non possono essere accentrati nella Commissione Europea, dovendosi rispettare il principio di attribuzione sancito dai Trattati. Uno Stato membro potrebbe decidere, per ragioni geopolitiche, che certi fornitori devono essere esclusi o limitati, assumendosene la responsabilità di fronte ai propri cittadini, ma l'Unione Europea non può arrogarsi questo potere, che non le compete. Non si può scaricare tutto sugli operatori, magari piccoli e medi, che hanno comprato apparati legittimamente, li hanno installati, li gestiscono, e

poi si trovano davanti a obblighi di sostituzione costosi e spesso poco proporzionati.

Inoltre la filiera tecnologica globale è molto più intrecciata di quanto piaccia raccontare. Un apparato può essere assemblato in Cina, contenere componenti americane, software europeo, chip asiatici e pezzi di supply chain sparsi in mezzo mondo. Fare finta che la sicurezza si risolva con una bandierina sul passaporto del vendor costituisce una drammatica semplificazione. La Cina è la fabbrica del mondo e non è un caso che governo americano, imprenditoria della filiera del complesso militare-tecnologico e il massimo esponente della finanza americana siano andati di persona dal presidente cinese. Noi dovremmo chiudere con l'oriente quando il paese che si suppone più industrializzato va a chiedere aiuto alla Cina? C'è un cortocircuito in termini.

AIIP chiede un approccio oggettivo e responsabile: sicurezza tecnica vera, criteri trasparenti, proporzionalità, tempi sostenibili e, quando la scelta è geopolitica, copertura pubblica dei costi. Altrimenti si usa la cybersecurity come etichetta elegante per fare politica industriale a spese degli operatori.

Key4biz. ***Che ruolo possono avere gli operatori territoriali e indipendenti nel futuro delle Tlc italiane?***

Giovanni Zorzoni. Un ruolo da assoluti protagonisti. E non lo dico per orgoglio associativo, ma perché i numeri raccontano una storia molto più chiara di tante presentazioni patinate.

In un mercato delle telecomunicazioni che da anni fatica a trovare una traiettoria credibile, gli operatori indipendenti rappresentati da AIIP sono una delle poche componenti industriali che continua a crescere, investire, assumere e innovare. Parliamo di circa settanta imprese, attive su tutto il territorio nazionale, con un fatturato aggregato di circa 1,7 miliardi di euro: più del dieci per cento del mercato

italiano di riferimento. Non è una nicchia, non è folklore territoriale, non è il *“piccolo operatore”* da trattare con paternalismo. È un pezzo fondamentale dell’industria digitale italiana.

Gli associati AIIP sono imprese che costruiscono fibra, gestiscono reti, realizzano data center, offrono servizi cloud, cybersecurity, connettività business, soluzioni per pubbliche amministrazioni, distretti industriali, aree artigianali, territori turistici e case sparse. Sono aziende che hanno portato Internet dove i grandi operatori non arrivavano o arrivavano soltanto quando c’erano soldi pubblici, obblighi regolatori o convenienza immediata. Noi abbiamo fatto quello che in Italia viene sempre invocato e quasi mai premiato: investimenti privati, competenze tecniche, presidio del territorio, rischio d’impresa e infrastrutture vere.

Per questo credo che gli operatori AIIP siano oggi il vero Made in Italy digitale. Non perché usiamo una bella etichetta da convegno, ma perché siamo italiani nella proprietà, nelle competenze, negli investimenti, nel personale, nei territori serviti e nella responsabilità verso i clienti. Nel momento in cui tutti parlano di sovranità digitale, cloud nazionale, sicurezza delle infrastrutture e riduzione delle dipendenze da piattaforme extraeuropee, bisognerebbe avere il coraggio di guardare dove queste cose esistono già: nelle imprese indipendenti che da trent’anni fanno rete, fibra, cloud e servizi digitali senza aspettare che qualcuno disegni per loro un grande piano salvifico.

A Bruxelles, purtroppo, si continua spesso a misurare il valore industriale in base alla dimensione del logo, alla presenza di una rete mobile o alla capacità di sedersi ai tavoli giusti. È un errore enorme. Il futuro delle Tlc italiane non sarà salvato da un campione unico, né da tre super-operatori continentali costruiti a tavolino, ma da una pluralità di reti, imprese e competenze capaci di competere,

innovare e stare vicino ai clienti. La qualità non nasce dalla concentrazione; nasce dalla concorrenza vera, dalla responsabilità diretta e dalla capacità di rispondere ai territori.

La regolazione europea sembra ancora innamorata dell'economia di scala, ma continua a sottovalutare l'economia di densità, di prossimità e di specializzazione. Gli operatori indipendenti conoscono i territori, conoscono le imprese, sanno dove passa una dorsale, dove serve un collegamento ridondato, dove un distretto produttivo non può permettersi mezza giornata di fermo, dove un data center deve essere raggiungibile con fibra vera e non con promesse in formato PowerPoint, quella grande invenzione umana per trasformare il nulla in slide.

Quindi il nostro ruolo non è difensivo. Non chiediamo di essere protetti perché piccoli. Chiediamo che venga riconosciuto ciò che siamo già: una componente industriale solida, in crescita, italiana, indipendente e strategica. Se l'Italia vuole davvero avere un futuro digitale autonomo, competitivo e meno dipendente da soggetti esteri, deve partire da chi quel futuro lo sta già costruendo. E gli associati AIIP lo stanno facendo da anni, metro dopo metro di fibra, cliente dopo cliente, data center dopo data center.

Con questa intervista Key4Biz vuole continuare il dibattito sul rilancio delle Telecomunicazioni in Italia e in Europa, per cui benvengano altri contributi di autorevoli esperti e stakeholder.

Novità su Google, per aggiungere Key4Biz tra le tue fonti preferite, clicca qui

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/tlc-zorzoni-aiip-basta-assistenzialismo-regolatorio-il-rilancio-passa-da-concorrenza-cloud-e-reti-vere/573662/

5G, Germania e Spagna contro il bando Ue a Huawei e ZTE (Pechino potrebbe vendicarsi sull’AI)

Germania e Spagna si sono messi alla guida dell’opposizione nei confronti del piano della Commissione Ue di mettere al bando **Huawei** e **ZTE**, i fornitori cinesi di attrezzature di reti 5G considerati ad alto rischio cybersecurity. Lo scrive *Bloomberg*, aggiungendo che le autorità dei due paesi vogliono mantenere a livello nazionale il controllo delle reti. Madrid e Berlino dietro le quinte avrebbero espresso preoccupazioni sul fatto che il bando di tecnologie cinesi di **Huawei** e altri fornitori **(ZTE)** potrebbe portare al rischio di una rappresaglia da parte di Pechino.

I due paesi hanno inoltre messo in guardia sul fatto che il bando rischia di rendere più cari i piani europei per la realizzazione di un'infrastruttura di Intelligenza Artificiale.

Il piano Ue contro fornitori extra-ue ad alto rischio per le reti 5G

La Commissione Ue ha etichettato **Huawei** e **ZTE** come "*fornitori ad alto rischio*" per le reti di telecomunicazioni, e Bruxelles ha chiesto agli Stati membri di escludere le due aziende dalle infrastrutture di connettività.

C'è da dire che le decisioni sulle infrastrutture vengono prese a livello di governi nazionali, ma la Commissione Ue sta spingendo per un controllo più rigoroso attraverso una revisione della sua legge sulla cybersecurity.

Le modifiche amplierebbero le valutazioni di cybersicurezza per includere i rischi di influenza di Stati esteri e di dipendenza da fornitori specifici, e renderebbero le raccomandazioni della Commissione giuridicamente vincolanti in tutta l'UE. I governi europei si trovano nel mezzo di una lotta di potere tra Stati Uniti e Cina, in bilico tra i vantaggi degli scambi commerciali con la nazione asiatica e la necessità di esaminare attentamente le fonti estere di infrastrutture critiche.

Il cancelliere Merz si sta riavvicinando a Pechino

Il cancelliere tedesco **Friedrich Merz**, che in passato si era mostrato critico nei confronti di un'eccessiva dipendenza dalla Cina, ha detto quest'anno che cambierà registro spingendo per rafforzare i legami sino-tedeschi.

L’UE sta anche pianificando di proporre la revoca temporanea delle sanzioni contro un fornitore cinese di chip per rafforzare la catena di approvvigionamento del settore automobilistico.

Da anni, legislatori ed esperti di sicurezza in Europa e negli Stati Uniti esprimono preoccupazione per la possibilità che le aziende cinesi possano inserire backdoor nelle loro apparecchiature, consentendo l’accesso non autorizzato ai dati personali dei cittadini europei. Sia Huawei che ZTE hanno negato tali affermazioni e non ci sono mai state prove concrete in questo senso.

Angela Merkel e Deutsche Telekom aperti con fornitori cinesi

In passato, **Angela Merkel** aveva avuto un atteggiamento aperturista nei confronti delle aziende tecnologiche cinesi, in particolare con i fornitori di attrezzature di rete 5G. Lo stesso vale per **Deutsche Telekom**.

Secondo Huawei la proposta di escludere i fornitori cinesi in base al loro paese di origine *“viola i principi giuridici fondamentali di equità dell’UE”.*

La Commissione ha stimato che le compagnie di telefonia mobile dovranno spendere dai 3,4 ai 4,3 miliardi di euro in tre anni per sostituire la tecnologia e toglierla dalle reti dove si trova attualmente montata.

Berlino e Madrid al lavoro

Un portavoce del Ministero dell’Interno tedesco ha detto che le discussioni sulla legge sulla sicurezza informatica sono in corso, aggiungendo che le consultazioni tra i ministeri sono iniziate questa settimana.

Un rappresentante della Spagna ha detto che il Paese sostiene la revisione della legge e *"ritiene che gli Stati membri debbano continuare ad avere un'adeguata partecipazione al processo decisionale in merito alla presenza di determinati rischi strutturali in un Paese, un fornitore o un prodotto".*

Anche la Spagna è diventata negli ultimi anni una sostenitrice più attiva degli interessi cinesi nell'UE. Il Primo Ministro **Pedro Sánchez** si è recato a Pechino quattro volte in altrettanti anni per corteggiare gli investimenti cinesi in settori come i veicoli elettrici e le energie rinnovabili.

Anche la Germania si è unita a questo sforzo, nonostante i disaccordi all'interno della coalizione di governo e tra i diversi ministeri coinvolti nel processo, secondo quanto riferito da alcune fonti.

Mentre parte del governo concorda generalmente sulla necessità di ridurre la dipendenza dalla Cina, altri hanno definito l'idea una bomba politica, hanno aggiunto le fonti.

Il governo tedesco ha concordato nel 2024 di rimuovere i componenti Huawei e ZTE dalla rete mobile 5G principale entro la fine di quest'anno per motivi di sicurezza nazionale.

Mercoledì, il Ministro dell'Economia tedesco **Katherina Reiche** ha affermato che l'UE dovrebbe garantire che qualsiasi misura applicata al commercio con la Cina non danneggi le esportazioni del blocco verso il Paese.

"In quanto nazione esportatrice, abbiamo due interessi", ha dichiarato Reiche ai giornalisti durante una visita a Pechino. *"Dobbiamo contrastare la concorrenza sleale, ad esempio nel settore dell'acciaio e delle ferroleghe, con misure adeguate, garantendo al contempo che le nostre aziende possano continuare a esportare".*

Novità su Google, per aggiungere Key4Biz tra le tue fonti preferite, clicca qui

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/5g-germania-e-spagna-contro-il-bando-ue-a-huawei-e-zte-pechino-potrebbe-vendicarsi-sullai/573757/

Sicurezza delle reti 5G private: opportunità industriali e rischi sottovalutati

C’è un momento preciso in cui un impianto produttivo cessa di essere un ambiente fisicamente delimitato e diventa, di fatto, un operatore di telecomunicazioni. Accade quando l’azienda installa una rete 5G privata, un *campus network* autonomo, per connettere robot industriali, sistemi AGV (*Automated Guided Vehicle*), sensori IoT e stazioni operative. È un salto tecnologico che porta con sé una promessa concreta: latenza submillisecondo, banda garantita, isolamento logico dal 5G pubblico, controllo totale sullo spettro assegnato. Ma è anche un salto in un territorio di rischio che molte organizzazioni

non hanno ancora imparato a cartografare con rigore.

La diffusione delle reti 5G private negli ambienti industriali è uno dei fenomeni più rilevanti del ciclo attuale di trasformazione digitale. Le stime di mercato variano significativamente a seconda del perimetro di analisi: tra i 5 e gli 11 miliardi di dollari nel 2025 secondo le principali società di ricerca, con proiezioni convergenti verso i 22-28 miliardi entro il 2029-2030 (Research and Markets, 2025; Grand View Research, 2025). Il dato che più impressiona, però, non è il valore di mercato: è il divario tra la velocità di adozione e la maturità dei modelli di sicurezza che accompagnano questa adozione.

La domanda che le imprese si pongono raramente con la giusta profondità non è "come connettere meglio i nostri asset", ma "cosa cambia nella nostra superficie d'attacco quando introduciamo una rete 5G privata in un ambiente che ospita sistemi SCADA, PLC e HMI". La risposta è scomoda: cambia tutto, e in una direzione che la maggior parte dei responsabili della sicurezza OT non ha ancora del tutto esplorato.

La convergenza IT/OT: un problema noto con una forma radicalmente nuova

Il tema della convergenza IT/OT non è nuovo. Da anni si discute dei rischi derivanti dalla connessione tra reti informatiche tradizionali e sistemi di controllo industriale; le vulnerabilità strutturali dei sistemi SCADA e ICS sono ben documentate, anche in questa sede.

Ma il 5G privato introduce una dimensione inedita: una rete di comunicazione mobile, con la propria architettura di *core*, i propri protocolli di segnalazione e la propria logica di

gestione degli accessi, si inserisce fisicamente e logicamente all'interno dell'ambiente OT. Non si tratta più di un confine tra IT e OT mediato da un *firewall* perimetrale. Si tratta di una rete progettata per connettere tutto, che porta con sé gli stessi vettori di attacco propri delle infrastrutture di telecomunicazione.

Il rapporto PwC *Global Digital Trust Insights* 2026, condotto tra maggio e luglio 2025 su 3.887 *executive* in 72 paesi, fotografa con precisione questa criticità strutturale: il **41%** delle organizzazioni intervistate identifica come principale ostacolo alla sicurezza OT/IIoT la mancanza di segmentazione di rete tra ambienti OT/IIoT e IT. Il 47% cita la carenza di competenze specialistiche OT, e il 39% denuncia assenza di governance e responsabilità chiare. Non sono problemi tecnici irrisolvibili: sono ritardi culturali e organizzativi nell'affrontare la convergenza con gli strumenti appropriati.

A dare la misura finanziaria del problema contribuisce il *2025 OT Security Financial Risk Report* pubblicato da Dragos in collaborazione con il *Cyber Risk Intelligence Center* di Marsh McLennan (agosto 2025): in uno scenario estremo ma statisticamente plausibile (evento 1-su-250-anni), il rischio finanziario globale derivante da incidenti OT potrebbe raggiungere i **329,5 miliardi di dollari**, con 172,4 miliardi attribuibili alla sola interruzione d'esercizio. Anche in anni ordinari, il rischio medio annuo stimato supera i 31 miliardi di dollari. Il dato più significativo del *report*, basato su un decennio di dati assicurativi e di *breach*, è che le perdite indirette, spesso escluse dai modelli tradizionali, rappresentano fino al **70%** dell'impatto reale di un'intrusione OT.

Il 5G privato non risolve questa frammentazione: la amplifica. Introduce un *layer* supplementare, quello della rete mobile, che dialoga con entrambe le dimensioni, IT e OT, e che risponde a logiche di sicurezza proprie del mondo delle telecomunicazioni, non del mondo industriale. Il personale che

gestisce i sistemi SCADA raramente ha familiarità con protocolli come GTP o NAS. I *team* di *network security* aziendale conoscono scarsamente le architetture del 5G *core*. Il risultato è uno spazio interstiziale dove nessuno guarda con sufficiente attenzione.

Robert M. Lee, CEO di Dragos, ha sintetizzato questa discrasia in modo diretto: "circa il 95% di tutti i *budget* destinati alla *cybersecurity* va al lato IT, non al lato OT. Eppure è sul lato OT che si genera tutta la capacità di fatturato, tutto l'impatto sulla sicurezza fisica e sulla sicurezza nazionale" (*The Chemical Show*, maggio 2025). Sono parole che descrivono con precisione l'asimmetria in cui si trovano le organizzazioni industriali che adottano il 5G privato: il nuovo vettore di attacco appartiene al dominio *telco*-IT, ma il danno si materializza nel dominio OT.

Specificità di sicurezza del 5G privato rispetto al 5G pubblico

Comprendere perché il 5G privato presenta sfide di sicurezza distinte rispetto alle reti pubbliche è essenziale per impostare correttamente la valutazione del rischio.

In una rete 5G pubblica, l'operatore assume la responsabilità primaria della sicurezza del *core network*: aggiornamenti *software*, gestione dell'autenticazione, integrità della segnalazione. L'impresa è sostanzialmente un utilizzatore finale, con visibilità limitata su ciò che accade al di là dell'interfaccia radio. In un *campus network* privato, questa responsabilità si sposta interamente sull'organizzazione che lo gestisce. Il 5G *core*, composto da funzioni virtualizzate come AMF (*Access and Mobility Management Function*), SMF (*Session Management Function*) e UPF (*User Plane Function*), è *deployato* in sede o in un *cloud* privato aziendale. La sua sicurezza dipende dalle competenze interne o da quelle di un *system integrator* terzo, spesso senza che i requisiti di

sicurezza *telco* siano stati esplicitamente negoziati nel contratto.

Questa redistribuzione della responsabilità ha implicazioni dirette. La superficie d'attacco aumenta perché l'azienda gestisce ora componenti *telco* che in precedenza erano fuori dal proprio perimetro. Le architetture *cloud-native* delle funzioni 5G *core* introducono rischi legati a misconfigurazioni dei *container*, a vulnerabilità nelle interfacce *Service-Based Interfaces* (SBI) e a possibili movimenti laterali attraverso l'infrastruttura *cloud* condivisa. Il *network slicing*, presentato come la soluzione tecnologica per isolare logicamente i servizi, garantisce separazione a livello logico, ma non necessariamente a livello protocollare di basso livello, come si vedrà nel prossimo paragrafo.

Esistono poi vulnerabilità specifiche legate alle *deployment Non-Standalone* (NSA), le più diffuse negli ambienti industriali attualmente in fase di adozione. In queste architetture ibride, il *core network* LTE coesiste con la radio 5G, creando un paesaggio di sicurezza che eredita le debolezze di entrambe le generazioni e introduce complessità di correlazione degli indicatori di compromissione tra domini eterogenei. Come documenta ABI Research (settembre 2025), per le reti 5G *Non-Standalone* "il modello ibrido crea un panorama di sicurezza di complessità significativa, con la correlazione incrociata degli indicatori di minaccia come fattore critico per fronteggiare gli attacchi."

Il problema GTP: un protocollo progettato senza avversari

Il **GPRS Tunneling Protocol** (GTP) è il protocollo che trasporta il traffico dati degli utenti nelle reti mobili, incapsulandolo in *tunnel* tra il nodo radio (gNB) e le funzioni di *core*. Nella variante GTP-U gestisce il piano utente; nella variante GTP-C gestisce i messaggi di controllo tra le

funzioni di *core* nelle architetture NSA.

Il problema fondamentale di GTP è di natura storica: come molti protocolli di telecomunicazione, è stato progettato in un'epoca in cui le reti mobili erano ambienti fisicamente chiusi e l'autenticazione reciproca tra i nodi era considerata secondaria rispetto all'affidabilità della connessione. Il risultato è che GTP-C può essere abusato per manipolare i *bearer path*, i percorsi attraverso cui fluiscono i dati degli utenti, iniettando traffico non autorizzato nel piano utente (GTP-U) o causando interruzioni di sessione attraverso messaggi di controllo falsificati. Come documenta P1 Security nel febbraio 2026, "gli attaccanti che guadagnano accesso alla funzione di controllo possono creare messaggi che istanziano o modificano *tunnel* GTP, pur senza avere accesso diretto al protocollo GTP."

Un attaccante che accede a un nodo interno alla rete 5G privata può usare messaggi GTP-C per terminare sessioni attive di dispositivi connessi, con effetti immediati sulle operazioni: un AGV che perde connettività nel mezzo di un ciclo produttivo, un sensore di sicurezza che smette di trasmettere, un sistema di monitoraggio remoto che diventa cieco. In contesti industriali dove il costo del *downtime* supera i **260.000 dollari per ora** nei grandi stabilimenti manifatturieri e raggiunge i **2,3 milioni di dollari per ora** nel comparto *automotive* (Siemens, *True Cost of Downtime* 2024), questi scenari non sono esercizi teorici.

La ricerca più recente ha chiarito un punto critico che riguarda anche il *network slicing*. Come analizzato in dettaglio su *Cyber Defense Magazine* (novembre 2025): "protocolli come GTP-U e PFCP (*Packet Forwarding Control Protocol*) operano a un livello inferiore rispetto alla separazione logica tra *slice*, all'interno dell'infrastruttura condivisa della *User Plane Function* (UPF). Un *exploit* su questi protocolli non rispetta i confini logici delle *slice* perché colpisce la risorsa fisica condivisa." La promessa di

isolamento offerta dal *network slicing* è, in assenza di controlli di sicurezza specifici aggiuntivi, una garanzia solo parziale.

Per le reti 5G *Standalone* (SA), l'architettura *Service-Based* ha sostituito GTP-C con interfacce HTTP/2 per la comunicazione tra le funzioni di *core*. Questo riduce alcune delle vulnerabilità di segnalazione ereditate da GTP-C, ma apre nuove superfici di attacco: le SBI sono esposte ad *API fuzzing*, a vulnerabilità di validazione degli *input* e a possibili escalation di privilegio attraverso la logica di orchestrazione condivisa. GTP-U rimane in uso anche nelle architetture SA per il piano dati.

Vulnerabilità NAS e il piano di segnalazione come vettore d'attacco

Il **Non-Access Stratum** (NAS) è il protocollo che gestisce la mobilità e la gestione della sessione tra il dispositivo (UE) e il *core network*, attraverso le funzioni AMF e SMF. È il livello dove avvengono autenticazione, cifratura e negoziazione degli algoritmi di sicurezza.

In architetture 5G NSA, i messaggi NAS vengono scambiati in chiaro durante la fase di *attach* iniziale, prima che la cifratura sia negoziata. Questa finestra espone informazioni sulla configurazione del dispositivo e sull'identità temporanea dell'utente (TMSI). Un attaccante può iniettare messaggi RRC falsificati a livello di *base station* per causare *denial-of-service* sul singolo terminale, sfruttando il fatto che il messaggio *RRC Connection Request* viene trasmesso in chiaro e contiene il TMSI dell'utente.

I cosiddetti *downgrade attack*, che forzano il dispositivo a retrocedere verso 4G o 3G perdendo le protezioni aggiuntive del 5G *Standalone*, rappresentano un rischio concreto nelle *deployment* industriali ibride. Quando la copertura 5G non è

disponibile, il terminale effettua automaticamente il *fallback* verso la rete LTE, perdendo funzionalità di sicurezza come SUCI (*Subscription Concealed Identifier*) e l'autenticazione estesa. "Gli attaccanti possono sfruttare questa vulnerabilità attraverso *downgrade attack* che forzano o ingannano i dispositivi 5G a usare reti 4G, con conseguente perdita prevedibile di protezione" (TechTarget, 2025).

Nel contesto industriale, i dispositivi connessi alla rete 5G privata includono sensori, PLC con moduli cellulari, telecamere di supervisione e HMI mobili. Molti di questi dispositivi non sono soggetti allo stesso ciclo di aggiornamento del *firmware* riservato agli *endpoint* IT tradizionali, e i loro *stack* di comunicazione cellulare possono presentare vulnerabilità note non *patchate*. La superficie di attacco via NAS si estende quindi ben oltre la rete mobile in senso stretto: un dispositivo OT compromesso attraverso il vettore cellulare diventa un punto di accesso all'interno del segmento di controllo industriale.

Le analisi *cross-protocollari* di P1 Security (febbraio 2026) hanno evidenziato come gli attaccanti che guadagnano accesso alle funzioni AMF o SMF del *core* possano manipolare messaggi NAS per alterare la gestione della mobilità, triggerare *drop* di sessione, o ottenere informazioni sull'identità e la posizione dei dispositivi connessi. In ambienti dove la posizione di un AGV o di una macchina a controllo numerico è un dato operativo critico, la compromissione del piano di segnalazione ha implicazioni che vanno oltre la sicurezza informatica per toccare la *safety* fisica.

Il rischio di *lateral movement* verso sistemi SCADA

L'architettura di un *campus network* 5G privato crea, per sua natura, ponti tra domini che in precedenza erano separati. Il *core* 5G è tipicamente *deployato* su infrastruttura *server* in

sede o *cloud* privato aziendale, che condivide risorse di rete con i sistemi IT aziendali. La UPF, la funzione che instrada il traffico degli utenti, è configurata per inviare i pacchetti verso le destinazioni appropriate, che possono includere sia *server cloud* sia sistemi OT locali.

Il rischio di *lateral movement* si concretizza quando un attaccante che ha compromesso un nodo della rete 5G, o un dispositivo connesso, riesce a raggiungere sistemi SCADA, DCS (*Distributed Control System*) o PLC che non erano direttamente esposti sulla rete IT. Il percorso tipico sfrutta la fiducia implicita che l'architettura ripone nel traffico proveniente dalla UPF: una volta dentro il *tunnel* GTP, il traffico è considerato legittimo dalla rete di destinazione, e la sua instradazione dipende dalla configurazione delle *route*. Se la segmentazione tra il segmento 5G e il segmento OT non è implementata con rigore (con *firewall* industriali, VLAN separate, *deep packet inspection* del traffico applicativo), il *tunnel* GTP diventa una via diretta verso i sistemi di controllo.

In questo scenario, i protocolli industriali *legacy* come Modbus, DNP3, IEC 104 e BACnet, che per definizione non includono autenticazione né cifratura, diventano il *target* terminale di un attacco che ha percorso un tragitto attraverso un vettore di telecomunicazione moderno. Un'azienda può aver investito considerevoli risorse nella sicurezza perimetrale della propria rete SCADA, ma aver lasciato aperto un accesso laterale attraverso l'infrastruttura 5G introdotta nell'impianto nell'ultimo anno.

La ricerca condotta nell'ambito del framework SWICS (Lenz et al., arXiv aprile 2026), il primo *testbed* virtuale per sistemi di controllo industriale che interconnette componenti ICS attraverso 5G in un ambiente di simulazione a eventi discreti, ha confermato che in condizioni di canale degradato o sotto attacco di *jamming*, i sistemi ICS connessi via 5G mostrano una suscettibilità agli attacchi significativamente superiore

rispetto a quelli su rete cablata. In particolare, la variabilità del canale radio rende inaffidabile il rilevamento di anomalie basato su *pattern* di comunicazione: i modelli addestrati su dati 5G in condizioni ottimali falliscono nel rilevamento quando il canale si degrada, aprendo finestre di invisibilità che un attaccante può sfruttare deliberatamente tramite tecniche di *jamming* selettivo.

Quando un'infrastruttura *cloud* ospita il *core* 5G virtualizzato, si aggiunge un ulteriore vettore: le vulnerabilità dell'infrastruttura *cloud* stessa possono diventare punti di accesso per movimenti laterali che, attraverso la UPF, raggiungono la rete OT. Come evidenziato nel *white paper* di OneLayer dedicato alle reti cellulari private, "quando il *core* cellulare è eseguito nel *cloud*, qualsiasi vulnerabilità sfruttabile dell'infrastruttura *cloud* può esporre la rete ospitata a *lateral movement*."

NIS2 e la governance delle reti 5G private industriali

In questo contesto di rischio emergente, il quadro normativo europeo e italiano offre strumenti di risposta, ma anche interrogativi aperti sulla loro applicazione concreta alle reti 5G private.

La Direttiva NIS2 (UE 2022/2555), recepita in Italia con il D.Lgs. 138/2024 entrato in vigore il 16 ottobre 2024, estende gli obblighi di sicurezza informatica a 18 settori critici, inclusi manifattura strategica, infrastrutture digitali, energia e trasporti.

L'Italia ha proceduto all'attuazione per fasi: dopo la registrazione obbligatoria dei soggetti NIS entro febbraio 2025 e la pubblicazione degli obblighi di base con la Determinazione ACN 164179/2025 (aprile 2025), il quadro operativo è stato consolidato a fine dicembre 2025 con due

ulteriori determinazioni del Direttore Generale dell'ACN, la 379887/2025 (che disciplina il Portale NIS) e la 379907/2025 (che definisce le misure di sicurezza di base e gli incidenti significativi di base), applicabile dal 15 gennaio 2026. Come abbiamo analizzato in dettaglio sugli adempimenti NIS2, la mappa delle scadenze è ora precisa e non lascia spazio a rinvii.

Dal gennaio 2026 è pertanto operativo l'obbligo di notifica degli incidenti significativi allo CSIRT Italia, con pre-notifica entro 24 ore dalla rilevazione. Entro ottobre 2026, i soggetti NIS dovranno aver adottato le misure di sicurezza definite dalla Determinazione ACN 164179/2025: **37 misure** per i soggetti importanti (87 requisiti complessivi) e **43 misure** per i soggetti essenziali (116 requisiti). Entro aprile 2026, l'ACN dovrà adottare il modello di categorizzazione delle attività e dei servizi e gli obblighi a lungo termine, ulteriore evoluzione rispetto agli obblighi di base già operativi.

Calate in un contesto 5G privato, le prescrizioni NIS2 richiedono una traduzione tecnica non banale. La **segmentazione di rete** deve ora includere il piano di controllo 5G e il piano dati GTP-U, non solo le tradizionali VLAN IT/OT. La **gestione delle vulnerabilità** deve estendersi ai componenti *software* delle funzioni virtualizzate del *core* (AMF, SMF, UPF), ai *firmware* dei dispositivi UE industriali e alle dipendenze *software* della piattaforma *cloud* su cui il *core* può essere ospitato. Il **monitoraggio continuo** deve saper interpretare il traffico di segnalazione NAS e GTP, protocolli che i SIEM aziendali tradizionali non analizzano senza strumenti specializzati.

Sul versante della *supply chain*, la NIS2 impone mappatura e classificazione dei fornitori ICT rilevanti, con clausole contrattuali esplicite su gestione degli incidenti, obblighi di notifica e diritto di *audit*. Nel caso delle reti 5G private, questa catena include i *vendor* del *core network*

(Ericsson, Nokia e altri), i fornitori di *hardware* radio (gNB), i *system integrator* che hanno realizzato la *deployment* e i fornitori *cloud* su cui è eventualmente ospitato il *core* virtualizzato. Ogni anello è potenzialmente un punto di ingresso.

Una questione normativa aperta riguarda la qualificazione della rete 5G privata industriale all'interno del perimetro NIS2 di un'organizzazione: la rete stessa è infrastruttura digitale soggetta agli obblighi, o è semplicemente un componente dell'infrastruttura produttiva? La risposta dipenderà dal settore di appartenenza dell'organizzazione e dalla classificazione come soggetto essenziale o importante, ma in ogni caso il rischio *cyber* derivante dalla rete 5G privata deve essere incluso nella valutazione del rischio complessiva che la NIS2 richiede.

Verso un modello di sicurezza integrato per il campus 5G

La soluzione non risiede in un singolo strumento tecnologico, ma in un cambio di prospettiva sull'architettura di rischio. Un *campus network* 5G industriale deve essere governato con un modello che integri tre livelli di competenza oggi troppo spesso separati: sicurezza delle telecomunicazioni (con conoscenza dei protocolli 5G), sicurezza IT (con capacità di *network security*, SIEM, *identity management*) e sicurezza OT (con comprensione dei sistemi industriali e delle loro specificità operative).

Il principio **Zero Trust**, applicato all'accesso dei dispositivi UE alla rete 5G privata, richiede che ogni dispositivo sia autenticato individualmente prima di ottenere accesso alle risorse OT, indipendentemente dalla posizione fisica nell'impianto. L'identità del SIM e del dispositivo deve essere verificata continuamente, non solo al momento dell'*attach* iniziale. L'uso di SUCI (*Subscription Concealed*

Identifier) al posto del SUPI non cifrato riduce il rischio di *tracking* e intercettazione dell'identità durante la fase di *attach*.

La **microsegmentazione del piano dati**, implementata a livello di UPF tramite *policy* PFCP, consente di isolare il traffico tra gruppi di dispositivi anche all'interno dello stesso *slice*, limitando la propagazione di un eventuale *lateral movement*. Questa segmentazione deve essere progettata esplicitamente, non affidata alla configurazione di *default* del *vendor*.

Il **monitoraggio del piano di segnalazione**, attraverso strumenti capaci di analizzare messaggi NAS e GTP-C, è indispensabile per rilevare anomalie non visibili a un tradizionale IDS/IPS. La letteratura recente (*MDPI Future Internet*, ottobre 2025) indica come strategie raccomandate "cifratura avanzata, autenticazione a più fattori, sistemi di *intrusion detection* e *audit* di sicurezza periodici per mitigare rischi emergenti ed evolutivi."

La gestione del rischio di *downgrade*, ovvero la ricaduta automatica su 4G o 3G in assenza di copertura 5G, deve essere valutata esplicitamente per ogni categoria di dispositivo. Per i dispositivi che accedono a sistemi OT critici, la *policy* preferibile può essere l'interdizione della connessione in assenza di 5G, piuttosto che la tolleranza di un *fallback* che degrada le protezioni di autenticazione.

Il rischio di *jamming* selettivo dell'interfaccia radio, documentato dal *testbed* SWICS (2026) come vettore per rendere inefficaci i sistemi di rilevamento anomalie, va infine incluso esplicitamente nei modelli di minaccia delle reti 5G private industriali, al pari degli attacchi protocollari sul *core*.

Conclusioni: la falsa sicurezza dell’isolamento privato

Il termine “privato” nel contesto delle reti 5G private porta con sé una connotazione di isolamento e controllo che rischia di diventare una trappola cognitiva. Una rete è privata nel senso che è dedicata a un singolo operatore, ma non è immune per natura dagli attacchi, né da quelli che provengono dall’esterno attraverso i dispositivi connessi, né da quelli interni che sfruttano le vulnerabilità protocollari del *core*.

Le industrie manifatturiere, energetiche e logistiche che stanno adottando *campus network* 5G si trovano a gestire una superficie d’attacco ibrida di tipo nuovo, dove la convergenza IT/OT si arricchisce di una terza dimensione, quella *telco*, per la quale non sempre esistono competenze interne, standard di riferimento condivisi o strumenti di difesa già consolidati. Il *report* PwC 2026 conferma che solo il **25%** delle organizzazioni manifatturiere spende significativamente di più in misure di sicurezza proattive rispetto a quelle reattive: uno squilibrio che, nell’era dei *campus network* 5G, diventa ancora più pericoloso.

Ignorare questa specificità, o trattare il 5G privato come una semplice evoluzione del Wi-Fi industriale, è un errore che le organizzazioni critiche non possono permettersi. La NIS2, con gli obblighi ora operativi in Italia, offre una cornice normativa che spinge verso un approccio strutturato, ma la *compliance* non è sinonimo di sicurezza.

Il vero lavoro consiste nell’adattare il modello di gestione del rischio alla specificità tecnica di un’infrastruttura che parla simultaneamente i linguaggi del 3GPP, dell’IEC 62443 e dell’ISO/IEC 27001, e nel farlo prima che un attaccante trovi nel *campus network* il percorso verso il sistema SCADA che controlla la produzione.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/reti-5g-private/

Fastweb porta il 5G a bordo di Luna Rossa all’America’s Cup. Rete dedicata nel Golfo di Cagliari

Fastweb è Official Sponsor e Technical Partner del team italiano Luna Rossa in vista della 38esima edizione di America’s Cup, la più prestigiosa competizione velica al mondo che – per la prima volta nei suoi 176 anni di storia – si disputerà in Italia, a Napoli, nel 2027.

5G, Rete dedicata nel Golfo di Aranci

In qualità di Technical Sponsor, Fastweb realizzerà una copertura 5G dedicata nell’area del Golfo di Cagliari e in quella del Golfo di Napoli utilizzando la tecnologia 5G *“slicing”,* una delle caratteristiche principali del 5G Standalone (5G SA), che consente di fornire copertura e prestazioni personalizzate, adattandosi con efficacia a contesti operativi articolati. Il capoluogo sardo, infatti, ospita il quartier generale del team ed è sede della prima regata preliminare, mentre Napoli sarà la venue ufficiale della 38^ America’s Cup.

Luna Rossa, dati di bordo trasmessi in sede a terra in real time

La copertura permetterà a Luna Rossa di trasmettere agli uffici a terra informazioni preziose in tempo quasi reale: i dati telemetrici durante le regate e i video durante gli allenamenti. In questo modo si velocizzeranno ulteriormente le operazioni a bordo, contribuendo a fornire un vantaggio aggiuntivo a tutto l'equipaggio. La tecnologia garantirà bassa latenza e alta capacità della trasmissione per tutta l'area interessata.

Luna Rossa, rete dedicata nel Golfo di Cagliari

Il progetto verrà implementato nel Golfo di Cagliari entro maggio 2026 per la prima regata preliminare, mentre entro l'estate, la rete verrà realizzata anche nell'area relativa al Golfo di Napoli che verrà utilizzata durante la 38esima edizione dell'America's Cup.

"*Siamo molto contenti di avere Fastweb come technical partner per la 38^ America's Cup* – ha detto **Gilberto Nobili**, Technology and Operations Manager di Luna Rossa – *Si tratta di un'azienda italiana leader nel settore delle telecomunicazioni e averla a fianco ci permetterà di ottimizzare la trasmissione dei dati e le comunicazioni tra la barca e i nostri uffici tecnici. Sapere di poter contare su una rete affidabile e potente e sul know-how di un brand leader come Fastweb è di fondamentale importanza in una sfida complessa e altamente tecnologica come l'America's Cup*".

"*La partecipazione a uno dei progetti sportivi più ambiziosi mai realizzati in Italia nasce da una visione condivisa: esprimere l'eccellenza mettendo a disposizione tecnologie di rete avanzate come il 5G dedicato e know-how* – ha dichiarato

Max Gasparroni, Chief Technology & Security Officer di Fastweb + Vodafone – *Nell'ambito di questa collaborazione forniremo a Luna Rossa strumenti all'avanguardia per l'analisi delle performance, la comunicazione in tempo reale e l'ottimizzazione di ogni fase della navigazione, contribuendo a creare un ecosistema in cui tecnologia, sport e intelligenza umana si integrano per raggiungere nuovi livelli di prestazione. Una partnership che conferma il nostro impegno verso l'innovazione e la transizione digitale del Paese*".

Leggi le altre notizie sull'home page di Key4biz

https://www.key4biz.it/fastweb-porta-il-5g-a-bordo-di-luna-rossa-allamericas-cup-rete-dedicata-nel-golfo-di-cagliari/570857/