

Antenne 5G come radar: la nuova arma contro i droni

Pubblicato il 23/11/2026

Ericsson sta sviluppando una nuova **applicazione per le reti mobili che permette alle antenne 5G,** oltre a trasmettere comunicazioni, di rilevare e **tracciare i droni sfruttando la riflessione delle onde radio.** Il sistema funziona anche quando i velivoli senza pilota non sono connessi alla rete: l'azienda dichiara di aver individuato piccoli velivoli a distanze di diversi chilometri e prevede progetti pilota già nel 2027, con una diffusione su scala più ampia a partire dal 2028.

Per i governi la prospettiva è allettante: **riutilizzare infrastrutture già presenti sul territorio per rafforzare la sorveglianza di aeroporti, porti, centrali elettriche e installazioni militari.** Proprio qui, però, emerge il nodo politico e industriale: le reti sono di proprietà o gestite da operatori civili. Nonostante l'interesse per la sicurezza nazionale, affidabilità, copertura reale, costi e responsabilità operative non hanno ancora ricevuto una validazione pubblica indipendente su scala nazionale.

Che cos’è l’ISAC e cosa dicono i test del 2026

Il principio alla base di questa tecnologia si chiama **Integrated Sensing and Communication (ISAC)** e consiste nell’utilizzare i riflessi delle onde radio per ricavare informazioni sulla presenza e sul movimento degli oggetti. Grazie a più punti di osservazione, è possibile ricostruire le traiettorie anche senza ricevere alcun segnale diretto dal drone.

Non basta però una singola antenna per improvvisarsi radar: servono apparati compatibili, geometrie favorevoli, sincronizzazione e capacità di calcolo. Inoltre, rilevare un oggetto non significa riconoscerlo, classificarlo correttamente o stabilire se abbia l’autorizzazione al volo.

Le sperimentazioni condotte nel 2026 aiutano a distinguere ciò che è tecnicamente possibile da ciò che resta ancora da dimostrare:

- **Febbraio (Plano, Stati Uniti):** presso la sede americana, Ericsson ha mostrato il rilevamento di oggetti passivi tramite apparecchiature **massive-MIMO**.
- **Luglio (Arlington, Stati Uniti):** in collaborazione con AT&T, all’esterno dell’AT&T Stadium, sono stati tracciati più droni in volo tra i 300 e i 400 piedi (circa **91–122 metri**) utilizzando diversi siti radio sincronizzati.
- **Settembre (Helsinki e porto di Vuosaari, Finlandia):** insieme a Erillisverkot, operatore di rete per le autorità pubbliche, sono stati svolti test in ambito urbano e portuale.
- **Ottobre (Cracovia, Polonia):** il rilevamento radio è stato integrato con sensori acustici e con la piattaforma **PUSZCZYK** di Asseco.

False allarmi e perdite di traccia spostano il costo dell’incertezza sugli operatori della sicurezza. Radar, telecamere termiche e sensori acustici restituiscono dati differenti e il valore dell’ISAC risiede nell’aggiungere osservazioni distribuite a questi strumenti, non nel sostituirli. Nell’esperimento polacco, dati radio, acustici e software sono stati messi insieme, ma osservare i segnali in uno stesso ambiente non dimostra di per sé che siano associati correttamente allo stesso bersaglio. L’intelligenza artificiale può supportare l’analisi, purché le classificazioni poggino su misure verificabili: la decisione finale spetta comunque alle autorità competenti.

La questione economica e i limiti del modello di business

Sul piano economico si annida un secondo equivoco. Il partner polacco **Play**, per esempio, ha indicato oltre **13.500 stazioni radio** e più di **13,5 milioni di abbonati mobili**. Sono numeri importanti per il traffico dati, ma non misurano l'area effettivamente presidiabile dal nuovo sistema: a Cracovia il sensore ha impiegato lo spettro industriale, mentre la rete 5G di Play ha svolto la funzione di collegamento di trasporto. Una rete commerciale può quindi contribuire al servizio senza che tutte le sue antenne siano in grado di rilevare i droni.

L'obiettivo di Ericsson è riutilizzare tralicci, apparati, connessioni e frequenze esistenti, ma la sostenibilità economica dipenderà da adeguamenti tecnici e normativi: sostituzione di unità radio incompatibili, **edge computing**, consumi energetici, manutenzione, cybersicurezza e certificazioni. Stimare la capacità della rete partendo da una portata media ipotetica non offrirebbe né una copertura credibile né un preventivo affidabile.

Le **progettualità pilota dedicate al sensing** previste da Ericsson sono una cosa; reti completamente riconfigurate sono ben altro. Per un operatore si apre un potenziale mercato, ma va chiarito chi garantisca le misure, tuteli i dati e risponda in caso di malfunzionamenti. Un'autorità pubblica potrebbe ricevere coordinate senza avere il controllo diretto dei nodi che le generano, mentre quegli stessi collegamenti sostengono servizi essenziali per la collettività, e la dispersione dei siti non elimina le criticità comuni legate a gestione, sincronizzazione, trasmissione e calcolo.

Il 6G non scioglie il nodo

Il passaggio al **6G** non risolve automaticamente la questione. A novembre 2023 l'Unione internazionale delle telecomunicazioni ha inserito il sensing tra i sei casi d'uso per **IMT-2030**. Il **3GPP** ha definito i requisiti nella **Release 19** e prosegue gli studi radio nella **Release 20**, mentre la **Release 21** include specifiche ancora in corso di definizione.

Nel 2026 l’**ETSI** ha richiamato l’attenzione su diversi nodi ancora aperti: a febbraio ha individuato **17 criticità architetturali**, a marzo **19 profili legati a sicurezza, privacy e sostenibilità** (di cui **15** incentrati su sicurezza e riservatezza) e il **5 novembre** ha indicato **5 sfide e 6 possibili soluzioni** per integrare calcolo e sensing. Il 6G potrà coordinare più siti, ma frequenze più alte e reti più dense non assicurano maggiore copertura, perché restano ostacoli, attenuazione e vincoli geometrici.

Il quadro europeo e le diverse velocità nazionali

Nel contesto europeo, la direttiva **NIS2** del 2022 stabilisce gli obblighi di cybersicurezza per i soggetti inclusi nel perimetro, comprese le attività di comunicazione elettronica; la direttiva sulla resilienza delle infrastrutture critiche aggiunge ulteriori responsabilità nei settori interessati. Il Codice europeo delle comunicazioni elettroniche disciplina aspetti centrali di reti e spettro, mentre le norme sulla protezione dei dati intervengono quando le informazioni raccolte hanno natura personale.

Nessuna di queste disposizioni, presa singolarmente, autorizza una sorveglianza generalizzata. Questo aspetto incide sulle gare e sui progetti: una soluzione tecnicamente funzionante può restare inutilizzabile per uno specifico scopo se non è chiaro quale autorità la attivi, come vengano gestite le osservazioni e a quali condizioni vi accedano le forze di sicurezza.

Contesto	Quadro normativo e iniziative	Stato operativo e criticità principali
Italia	D.lgs. 138/2024 (in vigore dal 16 ottobre 2024) di recepimento NIS2, con poteri assegnati all’Agenzia per la cybersicurezza nazionale.	Non risulta avviato un programma ISAC nazionale. Il coordinamento tra proprietario della rete, autorità di sicurezza, fornitore dati e soggetto abilitato all’azione non si risolve con una scelta puramente informatica.

Contesto	Quadro normativo e iniziative	Stato operativo e criticità principali
Francia	Aggiornamento delle allocazioni di spettro da parte di Arcep (luglio 2026, inclusa la banda 3,4–3,8 GHz); linee guida CNIL (giugno 2025) su telecamere a bordo di droni per sicurezza pubblica.	I diritti d’uso per comunicazioni mobili non equivalgono ad autorizzazioni generalizzate per il sensing; l’abbinamento di dati radio a immagini identificabili può modificare il regime giuridico dei dati.
Germania	Normativa di recepimento NIS2 in vigore dal 6 dicembre 2025.	L’introduzione del monitoraggio richiede un’ulteriore valutazione dei rischi affinché software, accessi, manutenzione e interfacce non compromettano i servizi critici già protetti.
Regno Unito	Oltre 200 milioni di sterline stanziati dal Ministero della Difesa nel 2026 per il contrasto ai droni; 5 milioni di sterline resi subito disponibili a settembre tramite il programma **Project PANOPTES**.	Domanda pubblica più visibile e attenzione al contrasto ai droni controllati tramite fibra ottica, dove l’intercettazione radio ha limiti e le riflessioni possono offrire un apporto aggiuntivo da valutare sui requisiti.

Conclusioni: alleanze e limiti fisici

Per la **NATO** e l’**Unione europea**, l’interesse condiviso non cancella la frammentazione tra Stati. Affinché i dati provenienti da una rete civile siano utili ai sistemi di comando, devono arrivare accompagnati da informazioni verificabili su origine, data e accuratezza: condividere una visualizzazione non basta a garantire un quadro operativo affidabile.

Restano infine i limiti fisici: neppure il 6G supera la difficoltà di osservare sott’acqua o nel sottosuolo, ambiti che richiedono strumenti acustici e geologici dedicati, con i dati correlati tramite le reti ma non generati dalle antenne mobili.