



Dalle HF in AM alle reti digitali: l'evoluzione delle radio militari, tra tecnologia e realtà operativa

Pubblicato il 25/01/2026

Oggi, come ieri, la radio resta uno dei canali centrali attraverso cui passano decisioni e coordinamento: la tecnologia evolve, ma la sostanza non cambia, perché sul campo il collegamento è la condizione che rende possibile **manovra e comando**.

Fino a tutti gli anni '90 questa verità si vedeva in modo netto nelle scelte operative: sulle lunghe distanze si ricorreva spesso a **HF in AM/SSB**, mentre la **FM** era lo strumento più naturale per le comunicazioni a corto raggio. Non era una questione di "vecchio" o "nuovo", ma di **propagazione, orografia, potenze disponibili** e, soprattutto, di **affidabilità** in condizioni non sempre ideali.

In quel periodo le reti erano più "semplici" nella struttura, ma richiedevano competenze solide. L'HF, con i suoi limiti (rumore, fading, variabilità legata all'ora e alle condizioni ionosferiche), permetteva di coprire distanze che la VHF/FM non poteva garantire. La FM, al contrario, offriva

qualità audio superiore e una gestione più immediata, ma restava vincolata alla linea di vista e quindi a un impiego principalmente tattico, locale. In mezzo c'erano **procedure, disciplina radio e buone pratiche** che spesso facevano la differenza tra un collegamento che regge e uno che "salta" sul più bello.

In termini pratici, dal **secondo dopoguerra fino agli anni '90 l'evoluzione delle comunicazioni radio militari è stata più incrementale che rivoluzionaria**. Sono migliorati affidabilità, robustezza, potenze e standardizzazione, ma **la logica di fondo è rimasta la stessa: HF** per il lungo raggio, **VHF/FM** per il tattico, con una forte centralità dell'esperienza dell'operatore.

La vera discontinuità arriva con la **digitalizzazione** e la gestione "di rete", che cambia non solo gli apparati, ma anche il modo di concepire il **C2**.



Negli anni '80 l'Esercito Italiano impiegava anche apparati analogici di produzione nazionale, come l'ER 95-A/I (RV3) in configurazione veicolare, pienamente inseriti nelle reti tattiche di reparto prima dell'introduzione dei sistemi digitalizzati di nuova generazione - Foto Radiosurplus Elettronica

La sicurezza come "optional"

La sicurezza delle comunicazioni, storicamente, **non è nata come requisito automatico**, ma come un problema da gestire.

Già nella **Prima guerra mondiale**, quando la radio e il telefono da campo iniziano a essere usati su larga scala, la protezione del traffico è affidata quasi esclusivamente a **codici, cifrari manuali e disciplina procedurale**. La tecnologia trasmette; la sicurezza è demandata

all'uomo.

Durante la **Seconda guerra mondiale** il quadro migliora, ma non cambia nella sostanza. Sistemi di cifratura più evoluti fanno la loro comparsa, ma restano **complessi, ingombranti e limitati a specifici livelli di comando**. Nella maggior parte dei casi la sicurezza continua a poggiare su procedure, rotazione dei codici, brevità dei messaggi e capacità degli operatori di non “dire più del necessario”.

Questo approccio rimane sostanzialmente valido anche nel dopoguerra e per tutta la Guerra Fredda. Fino agli anni '90, in molte configurazioni operative la cifratura **non era nativa** o non sempre disponibile: moduli dedicati e strumenti di caricamento delle chiavi, a seconda delle dotazioni e delle missioni, potevano esserci oppure no.

La radio funzionava comunque, ma **la sicurezza non era garantita di default**.

Di conseguenza, la protezione del traffico non dipendeva soltanto dall'hardware. Pesavano moltissimo **procedure COMSEC**, gestione rigorosa delle chiavi, disciplina nell'impiego e coordinamento tra le stazioni della rete. Un errore umano, una procedura saltata o una sincronizzazione imperfetta potevano annullare qualsiasi vantaggio tecnologico.

In altri termini, la tecnologia contava, eccome, ma contava almeno altrettanto **come** veniva impiegata. Una lezione che, a distanza di decenni, resta sorprendentemente attuale.



Negli anni '80 e '90 la cifratura non era sempre nativa: in ambito NATO si impiegavano moduli COMSEC esterni come il KY-57 VINSON (in foto), utilizzato anche dall'Esercito Italiano in specifici contesti operativi - Fonte Crypto Museum

Il cambio di passo: i sistemi digitali

Verso l'inizio del secolo, con l'introduzione dei primi sistemi digitali tattici e con la progressiva diffusione della famiglia **SINCGARS**, il cambiamento non è stato soltanto tecnologico, ma soprattutto **metodologico**.

Il **frequency hopping**, una gestione più strutturata delle reti e una maggiore attenzione alla **protezione** hanno imposto nuovi standard operativi, modificando il modo stesso di pianificare e condurre le comunicazioni tattiche. La radio non era più solo un mezzo "da accendere", ma un sistema da configurare, sincronizzare e gestire all'interno di una rete.

Allo stesso tempo, però, si è iniziato ad appoggiare una parte sempre più grande del **C2** su architetture complesse: **reti dati, relay, SATCOM, sistemi di comando e controllo integrati**.

Il risultato è stato un'enorme crescita di capacità, ma anche una crescente dipendenza da infrastrutture.



Le SINCGARS impiegate dall'Esercito Italiano tra la fine degli anni '90 e i primi 2000 erano basate sulla famiglia AN/PRC-119 e sulle corrispondenti versioni veicolari VRC. Nelle dotazioni venivano identificate con codici come "635" o "637", che indicavano la configurazione operativa dell'asset. In foto, una "635" in allestimento veicolare/di posto comando, con moduli affiancati e cifratura esterna: non una radio diversa, ma una configurazione più completa dello stesso sistema, adattata al contesto operativo - Foto by flickr

Verso il futuro con uno sguardo al passato

È qui che, negli ultimi anni, molti eserciti sono tornati a guardare con pragmatismo a ciò che non dipende dallo spazio e da catene tecnologiche “lunghe”. Negli scenari moderni, soprattutto ad alta intensità, il **dominio elettromagnetico** non è più un contesto di sfondo, ma un vero terreno di confronto: **disturbi, jamming, degradazione del GPS, attacchi alle reti e perdita dei collegamenti** non sono più ipotesi remote, ma condizioni operative da mettere in conto fin dalla pianificazione.

Questo campo di battaglia viene spesso ricondotto al **dominio cyber**, perché oggi una parte rilevante delle comunicazioni dipende da **reti digitali**, protocolli, software e gestione delle chiavi. Sul terreno, però, l'effetto operativo nasce dall'intersezione tra **spettro elettromagnetico e guerra elettronica**, cioè dal contesto fisico in cui quei sistemi funzionano e vengono contestati.

Le comunicazioni moderne non sono solo “radio” né solo “reti”: sono **sistemi digitali che viaggiano sullo spettro**, e possono essere colpiti sia sul piano fisico, disturbi, jamming, spoofing, che su quello logico, degradazione dei servizi, compromissione dei nodi, alterazione dei flussi informativi.

È in questa zona di sovrapposizione che la perdita di un collegamento, anche senza un singolo colpo sparato, può produrre effetti immediati sul **comando e controllo**.

Quando la connettività digitale si degrada o si interrompe, riemerge una realtà che chi ha operato trent'anni fa conosce bene: serve una capacità di comunicazione **essenziale, resistente e replicabile**, anche nelle condizioni peggiori. In questo contesto l'**HF**, con procedure aggiornate e tecnologie più moderne, continua a rappresentare uno dei pilastri del **fallback reale**: non un ritorno al passato, ma una risposta concreta alla fragilità delle architetture più complesse.

In trent'anni, dunque, non sono cambiati soltanto gli apparati. È cambiato il modo di costruire le reti, la gestione della sicurezza, la filosofia del **C2**, la consapevolezza del rischio elettromagnetico e, più in generale, il modo di combattere.

Oggi si parla molto di multi-dominio, ma sul terreno questo si traduce in una cosa concreta: saper **passare con lucidità da sistemi avanzati a procedure essenziali**, quando serve, senza perdere il filo del comando.



Nell'immagine: AN/PRC-163 (handheld), AN/PRC-167 (manpack) e Web UI su dispositivo rugged. Radio tattiche multibanda di nuova generazione della famiglia Falcon IV, oggi riferimento in ambito NATO: sistemi software-defined progettati per integrare voce, dati e cifratura nativa all'interno delle reti di comando e controllo - Copyright L3Harris Technologies

Non perdere la Diretta di Mercoledì 28 ottobre

Ne parleremo **mercoledì 28 alle ore 21 in live** sui nostri canali [YouTube](#) e [Facebook](#) con due super ospiti: **Danilo Amelotti**, Incursore del 9^o Col Moschin in congedo, e con **Nello Di Savio**, radiofonista Forze Speciali in Congedo e Capo Cellula J6 della leggendaria Task Force 45.

In questa diretta analizzeremo:

- **Come si comunicava negli anni '90:** apparati, procedure, disciplina radio e limiti reali
- **Affidabilità vs modernità:** dall'analogico al digitale, pro e contro
- **Sicurezza:** intercettazione, triangolazione, cifratura e il valore del silenzio radio
- **Integrazione:** dal “parlare” al lavorare in rete (unità, supporti, comando)
- **Resilienza:** cosa succede quando la tecnologia non c'è o non puoi usarla
- **Aneddoti dal campo:** episodi (anche ironici) che spiegano meglio di mille slide la comunicazione militare

Raccontremo cosa è cambiato davvero sul campo in 30 anni: **non solo apparati, ma procedure, sicurezza e modo di combattere.**

Vi aspettiamo con le vostre domande !

[Diretta Youtube](#)



BRIGATAFOLGORE.NET è in diretta Mercoledì 28 gennaio Diretta Youtube e Facebook alle ore 21:00