Guerra elettronica e comunicazioni radio

Autor(en): **Di Martino, Basilio**

Objekttyp: **Article**

Zeitschrift: **Rivista militare della Svizzera italiana**

Band (Jahr): **59 (1987)**

Heft 2

PDF erstellt am: **21.06.2024**

Persistenter Link: https://doi.org/10.5169/seals-246834

Guerra elettronica e comunicazioni radio

(da «Rivista militare dell'esercito italiano»)

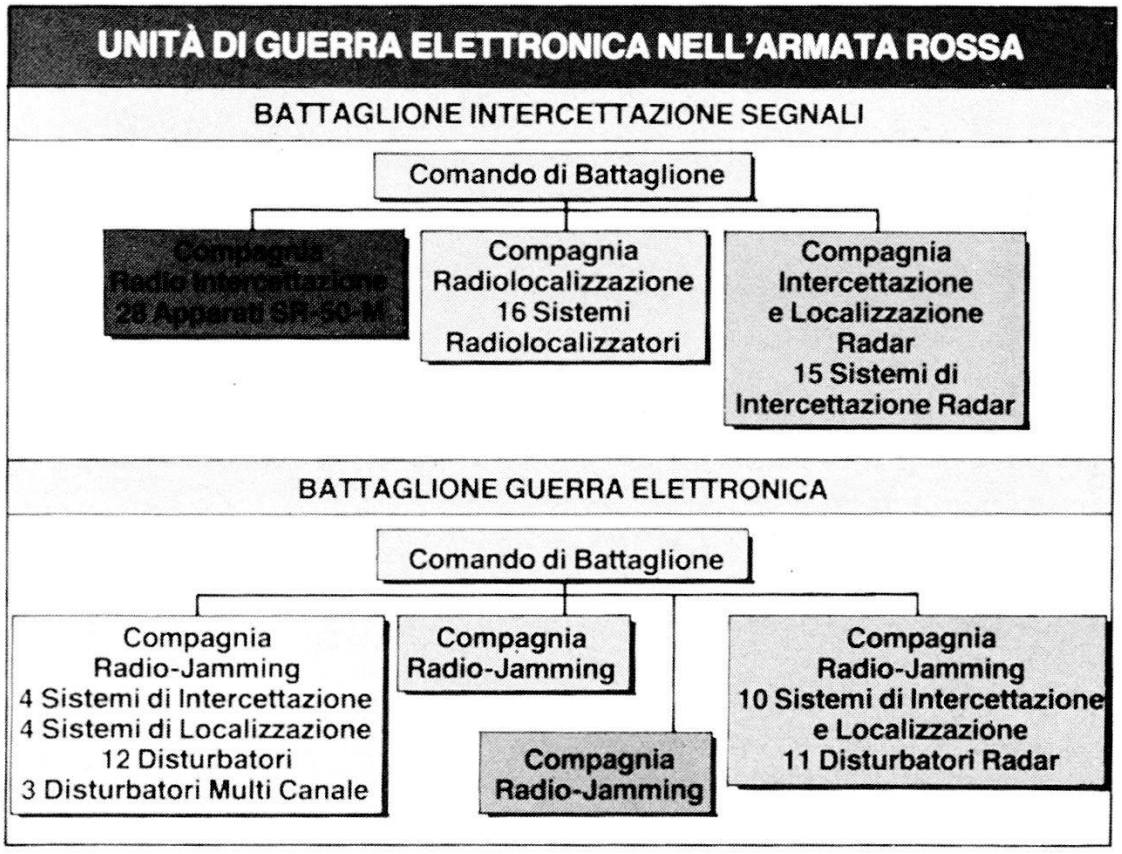
È universalmente riconosciuto che le comunicazioni rappresentano un fattore essenziale per il successo di qualsiasi operazione militare. Rispetto alle tecniche via cavo, la radio costituisce il sistema di collegamento più immediato e flessibile, insostituibile quando sia necessario collegare fra loro forze operanti nei tre elementi: aria, acqua, terra. Sfortunatamene non appena un segnale radio inizia a propagandarsi nell'etere l'informazione ad esso affidata diventa disponibile a chiunque riesca ad intercettarlo. Questo può così sfruttare il contenuto informativo del messaggio per acquisire un vantaggio sul campo di battaglia, prevenendo le mosse della parte avversa. L'utente indesiderato può anche sfruttare la sua capacità di intromettersi nel canale di comunicazione per interromperlo del tutto, impedendo alle unità avversarie di comunicare gettandole nel caos. Quest'azione di disturbo, correntemente indicata con il termine inglese *jamming*, può essere eseguita facilmente irradiando un segnale a radiofrequenza, modulato con del rumore, sulla stessa frequenza del canale che si desidera interrompere. L' uso del *jamming* ha un ruolo fondamentale nella dottrina sovietica alla quale è visto come uno degli strumenti da impiegare sul campo di battaglia, in stretto coordinamento con le unità di artiglieria e lanciarazzi. Accanto all'uso del disturbo intenzionale per attaccare il sistema di comando e controllo della NATO, è previsto il ricorso a sistemi di ascolto elettronico non solo per analizzare il flusso delle comunicazioni, ma anche per localizzare posti comando, centri di fuoco ed unità, determinando il tipo e la forza di queste ultime. I sistemi di *jamming* e di ascolto usati dall'Armata Rossa, per quanto forse non troppo sofisticati per gli standard occidentali, si fanno certamente apprezzare per la loro robustezza ad

SISTEMI DI INTERCETTAZIONE E RADIOLOCALIZZAZIONE IN USO NELL'ARMATA ROSSA — **Tabella 1**

Apparato	Compito	Banda di frequenza	Antenna	Sensibilità
SR-53-V	Intercettazione	HF (3-30 Mhz)	Rombica	-105 dBm
SR-52-V	Intercettazione	VHF-UHF (30-300 Mhz)	Log-Periodica	-110 dBm
SR-51-V	Intercettazione	VHF-UHF (30-300 Mhz)	Frusta	-110 dBm
SR-50-M	Intercettazione	VHF-UHF (30-450 Mhz)	Frusta	-110 dBm
SR-20-V	Localizzazione	HF (3-25 Mhz)	Adcock	-90 dBm
SR-19-V	Localizzazione	VHF-UHF (30-300 Mhz)	Loop o Adcock	-90 dBm
SR-25-V	Localizzazione	VHF-UHF (30-300 Mhz)	Loop	-90 dBm

I sistemi di intercettazione e di radiolocalizzazione in uso nell'Armata Rossa consentono di scoprire tutte le bande di frequenza impiegate in campo tattico.

affidabilità e la loro pericolosità è accresciuta dal fatto di essere distribuiti capillarmente ed in gran numero.
Un quadro riassuntivo dei dispositivi di ascolto è riportato in tabella 1, mentre in figura 1 sono schematicamente tracciati gli organigrammi delle unità destinate ad impiegarli. Controbattere questa minaccia solo con un'analoga azione di disturbo e di sorveglianza non è sufficiente e può anzi essere controproducente. La dottrina difensiva della NATO si basa sulla flessibilità e sull'elasticità di impiego delle forze a disposizione, numericamente inferiori a quelle del potenziale avversario. Ciò presuppone un sistema di comunicazione altamente efficiente, in grado di assicurare in modo costante il collegamento tra i centri di comando e le unità sul terreno. Per contro un attaccante numericamente superiore non è altrettanto dipendente del sistema di comando e controllo. Almeno nelle fasi ini-



Le unità a livello battaglione dedicate alle operazioni di guerra elettronica sono presenti a livello di Armata e di Fronte (Gruppo di Armate) nell'esercito sovietico.

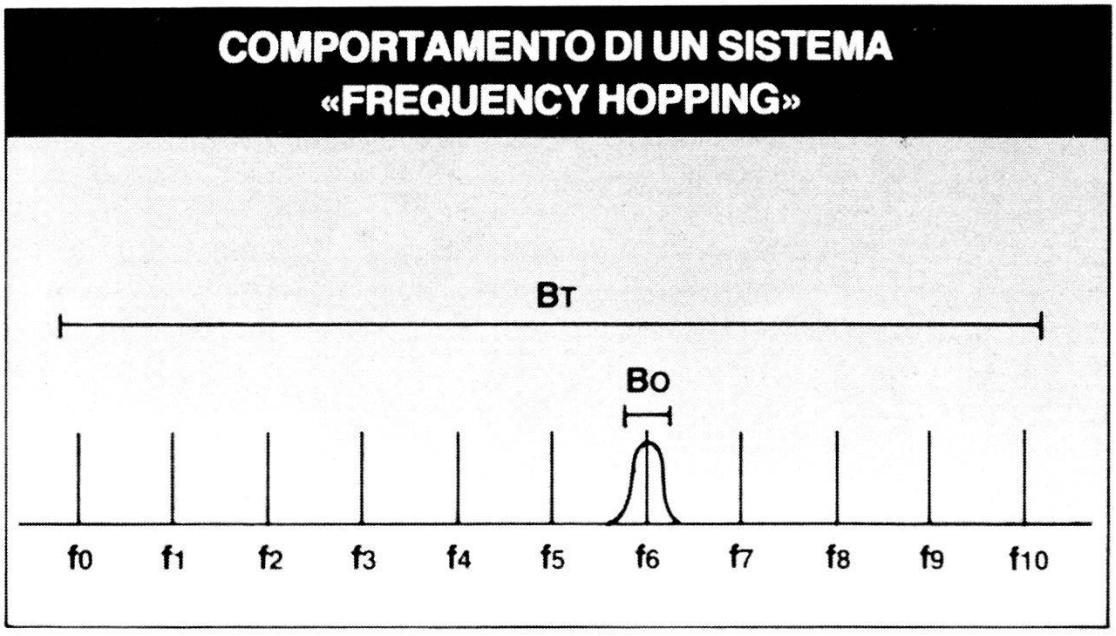
ziali dell'offensiva egli può infatti operare seguendo piani già predisposti e la sua superiorità gli consente di accettare un tasso di perdite più elevato. Oltre ad essere intrinsecamente meno vulnerabile, l'attaccante è agevolato anche dal fatto che il difensore sarà costretto a limitare la propria azione di disturbo per evitare di saturare lo spettro a radiofrequenza, sconvolgendo ulteriormente il suo sistema di comunicazioni.
La risposta alla minaccia elettronica va dunque cercata anche e soprattutto in tecniche di protezione che garantiscono la sicurezza dei canali di collegamento.
Un discorso analogo può essere fatto nel campo della difesa aerea. I velivoli intercettori operano infatti sotto il controllo di una rete radar, utilizzando a questo

Veicolo dell'esercito britannico equipaggiato con un moderno sistema per telecomunicazioni.

scopo canali radio dedicati. L' interruzione di queste comunicazioni avrebbe l'effetto di annullare le capacità del sistema di avvistamento aprendo vaste brecce nella difesa. Anche in questo caso la soluzione è da cercare nell'impiego di metodi e tecniche che assicurino l'integrità del flusso informativo. Questo articolo si propone di illustrare brevemente alcune soluzioni offerte dalla moderna tecnologia per la protezione delle comunicazioni dal distrubo intenzionale e dall'intercettazione.

Tecnica «Frequency Hopping»

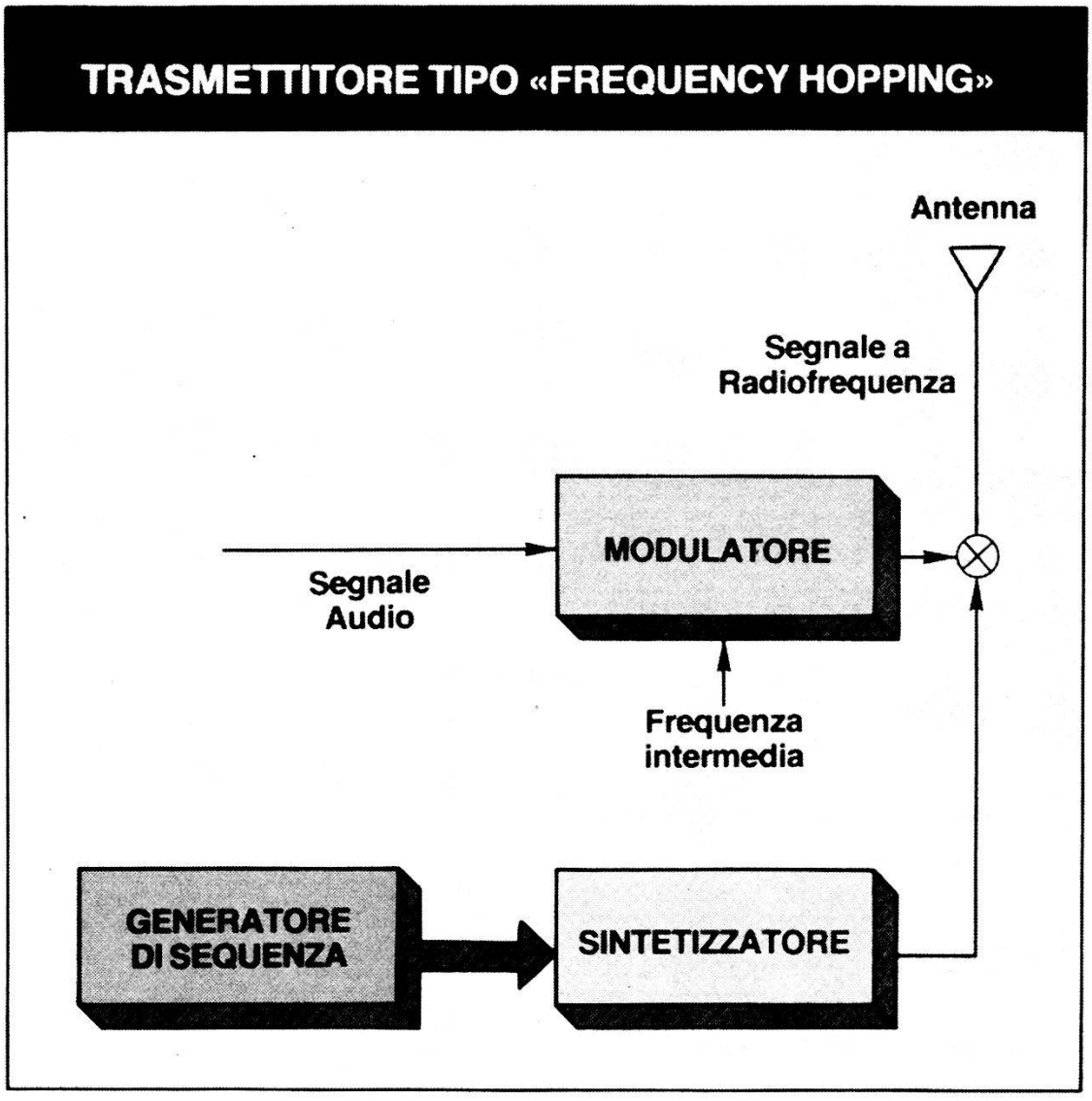
La tecnica detta dei salti di frequenza o, in inglese, *frequency hopping*, mira ad annullare l'azione di guerra elettronica dell'avversario variando più volte al secondo la frequenza di collegamento. L'informazione viene così trasmessa invece che su una sola frequenza portante su più frequenze portanti, ciascuna emessa per un certo intervallo di tempo seguendo una successione pseudo-casuale. A questo scopo un generatore di sequenza pseudo-casuale viene impiegato per controllare il sintetizzatore, a cui spetta generare la frequenza di trasmissione, negli



Comportamento di un ipotetico sistema *frequency hopping* in grado di saltare su 11 frequenze, indicate con i simboli F_0 ... F_{10} nell'unità di tempo. Bo è la larghezza del segnale, Bt la larghezza di band complessivamente impeganta nell'unità di tempo.

istanti dettati dalla velocità di salto prescelta. La sequenza viene determinata introducendo un opportuno codice nell'apparato. Ovviamente i terminali di una rete di comunicazione possono collegarsi fra loro solo occupando la stessa frequenza nello stesso istante di tempo e devono quindi essere in possesso dello stesso codice ed iniziare la sequenza di salto contemporaneamente.
Lo schema a blocchi di un trasmettitore del tipo *frequency hopping*, riportato in figura 2, evidenzia che l'apparato è in tutto simile ad un trasmettitore convenzionale se si esclude la presenza del generatore di sequenza che comanda il sintetizzatore. Istante per istante il sistema occupa una larghezza di banda che è dettata solo dalla modulazione impressa sulla portante. Nel caso più comune di comunicazioni in fonia vengono occupati solo pochi chilohertz intorno alla frequenza in uso. Quando però si osservi il comportamento di una radio *frequency hopping* in un periodo di tempo, appare evidente che vengono successivamente impegnate porzioni dello spettro a radiofrequenza distribuite su una banda di frequenza molto più ampia. La larghezza di banda totale del sistema viene dunque ad essere costituita da più bande elementari, occupate in istanti diversi (fig.3).
Da quanto detto si comprende che i parametri caratteristici di un sistema di questo tipo sono la velocità di salto e la larghezza di banda complessiva, intesa come numero di frequenze impegnate nell'unità di tempo. Questi due parametri dettano le caratteristiche di resistenza al disturbo ed all'intercettazione. Non esistono criteri universalmente riconosciuti per definire la velocità di salto. Si può tuttavia considerare lento un sistema in grado di effettuare fino a 200 salti/secondo e veloce uno capace di operare con una velocità superiore a 2000 salti/secondo. La velocità di salto rappresenta la principale difesa contro l'azione di disturbatori a banda stretta, comunemente indicati con la denominazione inglese *spot jammers*. Con questi dispositivi l'attaccante focalizza la sua attenzione su un numero molto limitato di frequenze fra loro vicine. Perché l'intervento di uno *spot jammers* sia efficace occorre che sia stata esattamente individuata la frequenza della trasmissione da disturbare. Dal momento che gli utenti di una rete operante in *frequency hopping* cambiano rapidamene e simultaneamente frequenza in modo pseudo-casuale, il disturbatore vede annullata la sua azione. Infatti, ignorando la logica della sequenza non è in grado di effettuare in tempo utile gli stessi cambiamenti di frequenza. Inoltre, anche quando uno *spot jammers* fosse in grado di reagire tanto rapidamente da intercettare il segnale trasmesso su una frequenza prima che il trasmettitore si sposti sulla successiva, il sistema non avrebbe modo di assegnare questo frammento di comunicazione ad una particolare rete,

proseguendo alla cieca la sua attenzione. Si realizza così anche un'efficace difesa contro i sistemi di ascolto e sorveglianza elettronica, che, in un etere affollato da trasmissioni con caratteristiche *frequency hopping*, avrebbe un compito estremamente gravoso dovendo analizzare i frammenti di segnale ricevuti, discrimare le



Schema a blocchi estremamente semplificato di un trasmettitore di tipo *frequency hopping*. Si noti come il sintetizzatore sia pilotato dal generatore di frequenza.

diverse trasmissioni e ricostruire le reti di appartenenza. La validità delle tecniche di salto di frequenza quali contromisure all'azione di *spot jammers* o comunque di sistemi di intercettazione, è dunque proporzionale alla velocità di salto ed anche al numero di reti attivate.
La sola agilità di frequenza non è sufficiente a contrastare l'azione di disturbatori a banda larga, noti anche come *barage jammers*, in grado di intervenire con continuità su un gran numero di frequenze. Per fronteggiare questa minaccia occorre che gli apparati radio non solo saltino di frequenza ma anche coprano con i loro salti una banda molto più ampia. In questo modo la potenza del disturbatore, per quanto grande, dovrebbe essere dispersa su un numero molto elevato di frequenze con la conseguenza che l'azione di disturbo sulla singola frequenza sarebbe meno efficace di quella di uno *spot jammers* di pari potenza. In termini più specifici si può dire che l'efficienza di un *barrage jammers* viene ad essere ridotta di un fattore pari al rapporto tra la larghezza di una banda totale occupata e la larghezza di banda istantanea del canale di comunicazione da disturbare. Non bisogna infine dimenticare che un disturabatore di questo tipo, oltre ad essere molto dispendioso in termini di potenza, non è in grado di distinguere tra un canale di comunicazione amico ed un nemico intervenendo inesorabilmene su entrambi. Una rete che operi saltando in frequenza è efficacemente protetta solo se i sistemi di guerra elettronica dell'avversario non sono in grado di seguirla nei suoi spostamenti. Questa eventualità sembra piuttosto remota perché, anche se si comincia a parlare di *spot jammers* con caratteristiche *frequency hopping*, passerà molto tempo prima che questi sistemi diventino realtà.
I problemi connessi con una capacità di intercettazione e di sintonizzazione in brevissimi tempi sono infatti ancora ben lontani dall'essere risolti. L'avversario potrebbe superare agevolmente queste difficoltà qualora entrasse in possesso dei codici di salto. Occorre dunque proteggere in modo adeguato quest'informazione, ma anche evitando di utilizzare sequenze operative in tempo di pace, ripiegando su frequenze particolari per le necessarie attività di sperimentazione e d'addestramento. Questi accorgimenti sono necessari per evitare che un'attività di ascolto elettronico protratta per un lungo periodo di tempo permetta di ricostruire la logica del generatore di sequenza pseudo-casuale. La gestione dei codici di salto va attentamente studiata anche perché un loro corretto uso consente di semplificare il problema dell'assegnazione delle frequenze. Nel caso di sistemi convenzionali, operanti a frequenza fissa, per evitare interferenze reciproche è necessario che una frequeza venga utilizzata da una rete soltanto e l'uso della stessa da parte di altre reti di comunicazione è possibile solo quando esiste una

sufficiente separazione geografica. L'impiego di codici diversi, e quindi di sequenze diverse, permette a più reti di coesistere senza distrurbarsi, evitando che la stessa frequenza venga occupata contemporaneamene da più utenti.
Perché questo avvenga è necessario che l'emissione di un trasmettitore rimanga confinata entro limiti ben definiti di tempo e di frequenza. Ciò è possibile utilizzando opportuni circuiti che provvedono a silenziare l'apparato durante i cambi di frequenza. Sistemi *frequency hopping* operanti nelle bande VHF, HF e recentemente anche UHF, hanno cominciato ad essere sviluppati da una decina di anni e sono ormai in produzione anche se in quantità relativamente limitata. Programmi di sviluppo e di approvvigionamento sono in corso in quasi tutti i paesi NATO, ed in altre nazioni quali Israele e Sud Africa. Apparati sud africani sono stati i primi ad essere impiegati in condizioni operative reali, sia dalle forze armate nazionali che dall'esercito argentino al quale erano stati forniti durante la campagna delle Falkland.

Tecnica «nullo d'antenna»

Questa tecnica sfrutta le caratteristiche del sistema d'antenna per respingere segnali indesiderati. Il principio ispiratore è molto semplice. È noto che la trasmissione irradiata da un'antenna omnidirezionale, che trasmette con pari potenza in tutte le direzioni, può essere intercettata molto più facilmente di quella originata da un sistema che utilizza un'antenna direttiva, in grado cioè di convogliare la maggior parte dell'energia a radio frequenza in una direzione ben definita. In questo caso, per operare efficacemente, il sistema di disturbo o di ascolto elettronico deve collocarsi lungo la direzione di massimo guadagno dell'antenna, che coincide con la direzione del collegamento. La tecnologia attuale consente di costruire una situazione di questo tipo quando diventi necessario. È possibile infatti sagomare il diagramma di irradiazione dell'antenna adattandolo alle circostanze, orientando la direzione di massimo guadagno verso l'altro terminale di collegamento e facendo in modo che i nulli del diagramma, vale a dire direzione nelle quali è minima sia la potenza irradiata che quella ricevuta, siano orientati nella direzione di provenienza della minaccia elettronica.
In presenza di un nullo un disturbatore vede sensibilmente ridotta l'efficacia della sua azione poiché è minima la quantità di energia da lui irradiata che viene catturata dall'antenna. Anche i dispositivi di ascolto elettronico perdono di efficacia dal momento che si trovano a disporre di livelli di segnale molto deboli e sicuramente inferiori a quelli irradiati da un'antenna omnidirezionale. Questi ri-

sultati possono essere ottenuti accoppiando a normali ricetrasmettitori dei dispositivi che, collegati all'uscita a radiofrequenza, provvedono a costruire un nullo del diagramma di irradiazione, orientandolo nella direzione del segnale disturbante eventualmente percepito, ed a trasmettere a piena potenza il segnale desiderato nella direzione di interesse. Sistemi di questo tipo consentono di avere un margine di 40 dB tra segnale desiderato e disturbo. Il principale inconveniente è rappresentato dalla necessità di disporre di più antenne. La cancellazione del disturbo è infatti realizzata prendendo più versioni dello stesso segnale, ricevute da diverse antenne, e sommandole sfruttando la relazione di fase e d'ampiezza. Queste operazioni devono essere fatte dal sistema in modo completamente auto-

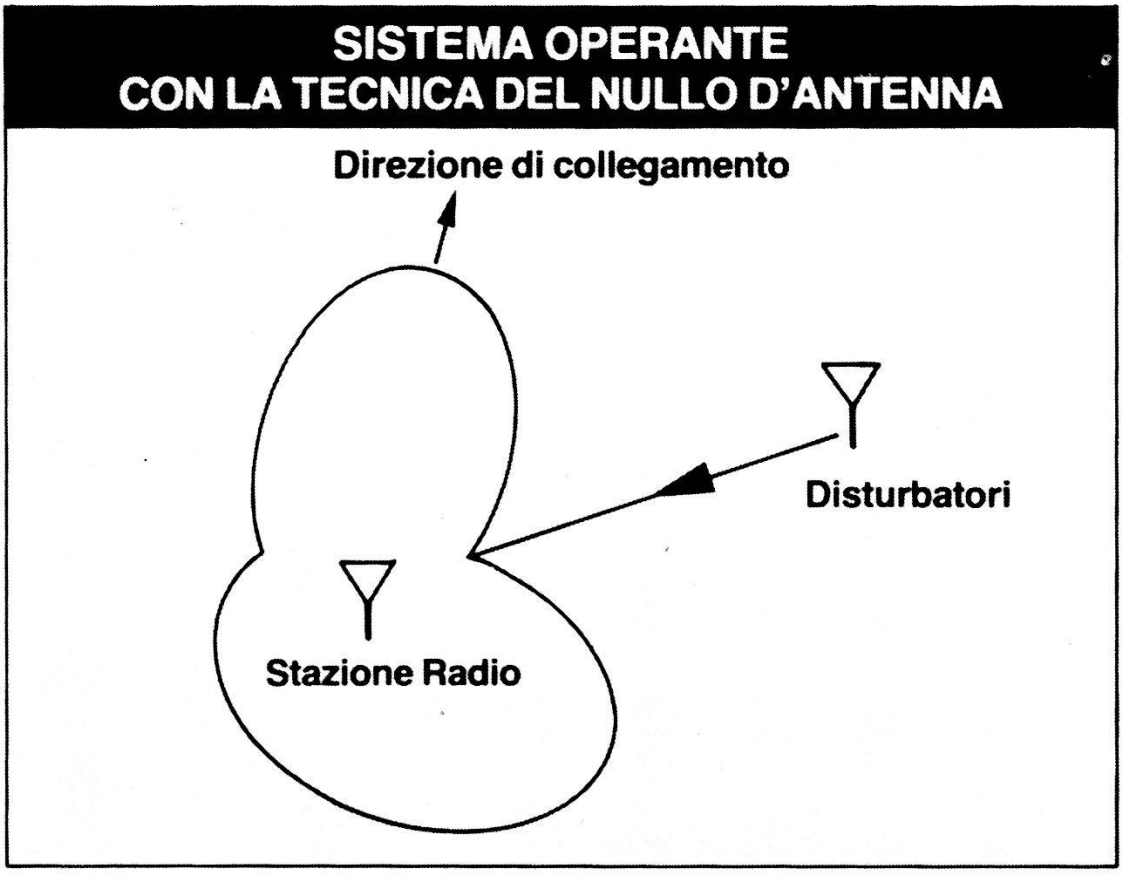


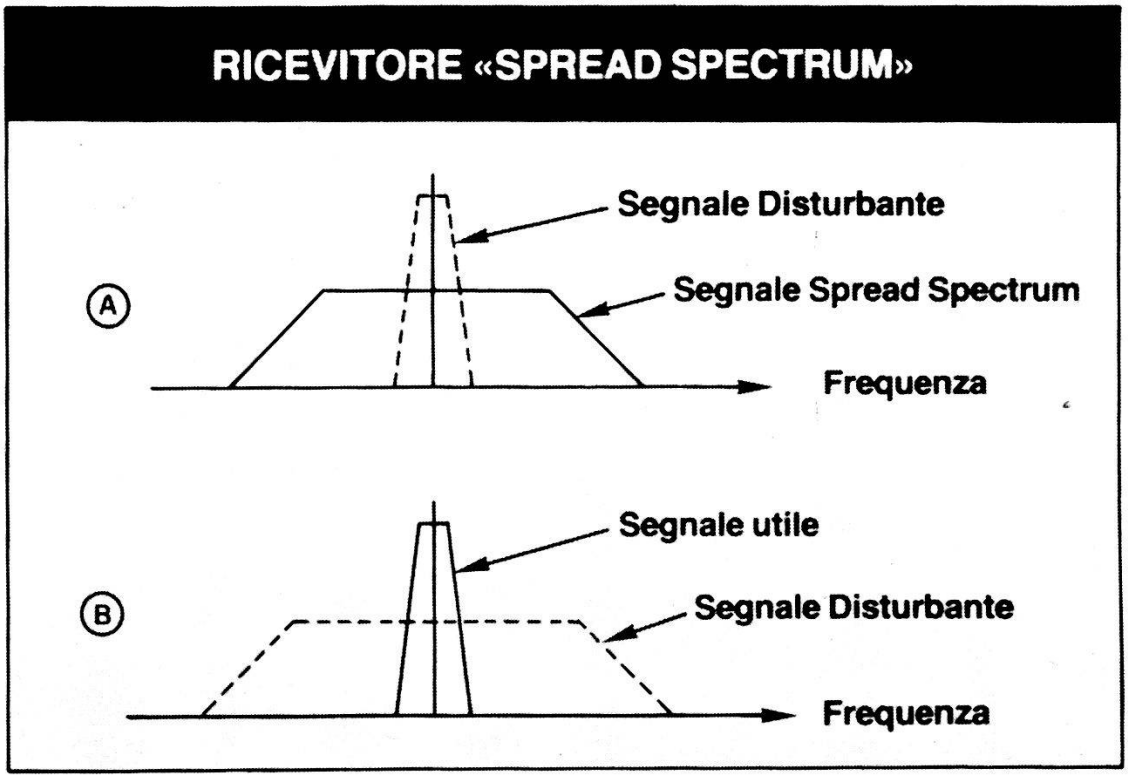
Diagramma di irradiazioni di un sistema operante con la tecnica del «nullo d'antenna». Le dimensioni del diagaramma, proporzionali al segnale ricevuto, evidenziano l'effetto riduttivo nei confronti del segnale distrubatore.

matico, così da avere i tempi di reazione estremamente ridotti. La tecnica del nullo d'antenna suscita un notevole interesse per la possibilità di operare in modo completamente passivo e per il costo di implementazione relativamente basso. La completa automazione e la capacità di operare usando un solo elemento d'antenna sono gli obiettivi delle ricerche in atto. Il loro raggiungimento consentirebbe di adottare questa tecnica anche per complessi mobili e di piccole dimensioni, permettendo inoltre di estenderne l'uso alla banda HF.

Tecnica «Spread spectrum»

Nel campo delle comunicazioni radio esiste tradizionalemente la tendenza a ridurre la larghezza di banda del segnale trasmesso in modo da poter utilizzare un maggior numero di canali. L'esigenza di resistere all'offesa elettronica ha invece paradossalmente portato alla diffusione di una tecnica di trasmissione che fa ricorso a segnali che occupano una larghezza di banda molto più ampia di quella del messaggio. Questa tecnica di espansione dello spettro, meglio nota come *spread spectrum*, ha trovato impiego tanto nel settore delle comunicazioni che nel settore della navigazione satellitare. Nei sistemi *spread spectrum* si ha la modulazione diretta della portante a radiofrequenza con una forma d'onda costruita sovrapponendo un messaggio in forma digitale ad una sequenza pseudocasuale di impulsi che può essere assimilata a del rumore elettronico. Questo processo digitale ha come risultato un segnale che occupa una banda di frequenza molto più ampia della banda che verrebbe normalmente occupata dall'informazione da trasmettere. L'incremento di banda è legato al rapporto tra la velocità di scorrimento della sequenza pseudo-causale e la velocità di scorrimento delle unità binarie che compongono l'informazione digitale. Il trasmettitore viene modulato con questo segnale composito, il cui livello, a causa dell'ampia distribuzione in frequenza, viene ad essere molto basso al punto di confondersi con il rumore elettronico normalmente presente nell'ambiente. Al terminale ricevente, per riottenere il messaggio originale, occorre rimuovere la componente pseudocausale. Quest'operazione viene eseguita generando nel ricevitore una sequenza che è la replica esatta di quella prodotta nel trasmettitore e che è con questa sincronizzata. Questa conseguenza viene poi sottratta dal segnale ricevuto mediante un processo di correlazione. In questo modo, rimuovendo la causa dell'espansione, si contrae lo spettro del segnale che diventa in tutto assimilabile ad un segnale convenzionale. In sintesi si può quindi dire che con la tecnica *spread spectrum* la potenza trasmessa viene distribuita su una larga porzione della gamma di fre-

quenza in uso e che in ricezione si ha invece un processo di comprensione. Dal punto di vista della guerra elettronica un sistema di comunicazioni che operi con modalità *spread spectrum* impone all'avversario il ricorso al disturbo a larga banda (*barrage jamming*) per avere qualche speranza di successo. Completamente inutile sarebbe infatti l'impiego dello *spot jamming* dal momento che un segnale interferente centrato sulla frequenza della portante verrebbe sottoposto nel ricevitore ad un processo opposto a quello del segnale desiderato, vedendo la sua potenza dispersa su un'ampia banda di frequenza.
La tecnica *spread spectrum* offre inoltre una protezione efficace contro i sistemi di ascolto elettronico: quando anche il messaggio venisse intercettato individuandolo nel rumore ambientale, sarebbe quasi impossibile estrarne il contenuto informativo senza disporre della corretta sequenza codificata. Infine, nonostante



Comportamento di un ricevitore *spread spectrum* in presenza di un segnale disturbatore a banda stretta. Disegno A: all'ingresso del ricevitore il segnale distrurbante ha un livello superiore allo *spread spectrum*. Disegno B: comprensione del segnale *spread spectrum* e dispersione del disturbo nel ricevitore.

venga occupata una banda piuttosto ampia, questa tecnica offre la possibilità di trasmettere più segnali della stessa frequenza, purché ogni segnale sia codificato con una sequenza diversa. La complessita strutturale e l'elevato costo di questi sistemi rappresentano dei fattori che ne ostacolano la diffusione, limitandone per il momento l'impiego ad applicazioni particolari. Tra queste figurano il sistema di navigazione satellitare GPS NAVSTAR ed il sistema tattico di comunicazioni JTIDS (Joint Information Distribution System). Proprio le difficoltà tecniche ed economiche incontrate dal JTIDS evidenziano come la tecnica *spread spectrum* non sia ancora matura per un'applicazione su vasta scala.

Conclusioni

I sistemi di comunicazione che sfruttano per il trasferimento dell'informazione la propagazione delle onde elettromagnetiche nello spazio libero sono esposti per loro natura all'azione di disturbo e di ascolto dell'avversario. Queste forme di guerra elettronica non possono essere trascurate soprattutto quando il potenziale avversario attribuisce a queste attività un ruolo fondamentale. Il fatto che durante la campagna delle Falkland le forze armate britanniche abbiano potuto usare senza seri inconvenienti reti di comunicazione non protette, non può essere considerato significativo. Le operazioni del maggio-giugno 1982 furono infatti caratterizzate da un limitato ricorso all'offensiva elettronica, il che contrasta con quanto verificatosi in altri recenti conflitti e soprattutto con quanto è ragionevole prevedere nel teatro europeo. La tecnologia mette a disposizione nuove risorse il cui impiego può consentire di contrastare tutte le forme di guerra elettronica. La capacità di operare con le tecniche dei salti di frequenza, del nullo d'antenna, dell'espansione di spettro è destinata a diventare un requisito irrinunciabile dei moderni sistemi di comunicazione tattici.

La scelta dell'una o dell'altra tecnica andrà fatta caso per caso, considerando i punti di forza ed i punti deboli di ciascuna. I sistemi a salto di frequenza ad esempio, che anche per il loro relativamente basso costo stanno incontrando il massimo favore, pur risultando molto resistenti al disturbo e all'intercettazione, possono essere localizzati da un sistema che sia in grado di controllare una o più frequenze. Il radiolocalizzatore dovrà soltanto attendere che il sistema dei suoi salti attraversi il suo campo di osservazione. Il messaggio risulterà incomprensibile ma il rilevamento dell'emittente sarà individuato con facilità. I sistemi *frequency hopping* si prestano dunque soprattutto all'installazione su veicoli e aeromobili, negli altri casi sarà invece opportuno ricorrere alle tecniche del nullo

d'antenna o dell'espansione di spettro. La necessità di disporre di più soluzioni ed il costo d'acquisto di questi sistemi spingono verso soluzioni modulari che consentono di modificare apparati già esistenti od in via di acquisizione permettendo inoltre di programmare il piano di approvigionamento su un periodo piuttosto lungo.

Cap Basilio Di Martino