DOCUMENTO TRATTO DA

WWW.AEREIMILITARI.ORG

Tecniche di attacco elettronico

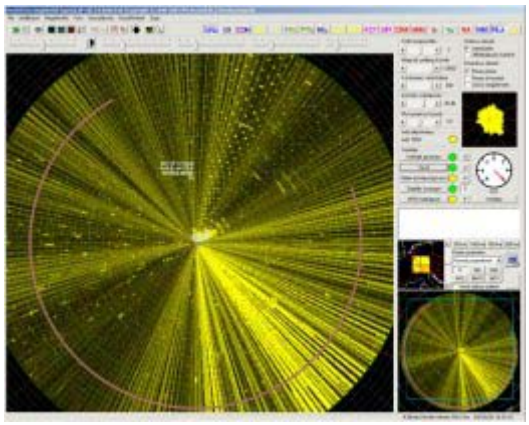
Una panoramica sulle principali tecniche d'attacco elettronico usate.

I radar costituiscono ancora lo strumento primario di rilevamento. Le loro prestazioni sono andate aumentando progressivamente e così la loro sofisticazione, soprattutto in termini di ECCM o, nella definizione attuale, EP (electronic protection). Ogni radar è caratterizzato da diversi parametri (lunghezza d'onda, frequenza di ripetizione degli impulsi, polarizzazione del segnale, velocità di rotazione dell'antenna, presenza di lobi secondari, modalità di scansione, forme d'onda, potenza media e di picco, ecc. ecc. per le definizioni…Cercate su wiki!). Anche le tecniche di disturbo più vecchie possono tornare utili perché sono ancora presenti in quantità sistemi superati ma insidiosi…

L'attacco elettronico utilizza il disturbo (noise), l'inganno (deception), la seduzione, la confusione. E' in grado di disturbare la corretta rilevazione dei parametri tipici di un bersaglio, cioè distanza, rotta, velocità.

Noise: il disturbo è la tecnica più facile da applicare. Sulla stessa frequenza del radar vittima si trasmette rumore di fondo ad elevata potenza in modo da coprire il segnale di ritorno. La potenza richiesta è proporzionale a quella di picco del radar e, quindi, molto alta. Impedisce principalmente la determinazione della distanza e può schermare molti aerei contemporaneamente. E' efficace quando il rapporto disturbo/segnale (jam-to-signal ratio) è maggiore o uguale a 1. Ogni tanto è necessario interrompere l'emissione (look-through), per "ascoltare" le frequenze in arrivo e verificare eventuali cambiamenti nei parametri. In caso affermativo il Jammer modifica all'istante l'emissione. I sistemi più sofisticati possono interrompere le emissioni in time-sharing (High speed chop) o con schemi (look over) di sicurezza,basati su dati elint. E' importante non attivare troppo presto i disturbatori: il rischio è il rilevamento passivo (beaconing) che, tra l'altro, consente di tracciare il disturbatore oltre il raggio di scoperta del radar. Poiché la potenza dell'eco radar del bersaglio varia inversamente alla quarta potenza della distanza e la potenza del jammer invece è inversa al quadrato della distanza, al diminuire di questa, la potenza dell'eco aumenta più rapidamente ed è richiesta sempre più potenza. Alla fine il rumore generato dal jammer non potrà più nascondere il bersaglio (JSR<1) ed il radar potrà vedere attraverso i disturbi (burn through). Anche così però, il disturbo diminuirà la portata massima del radar. Sfortunatamente, il Jamming colpisce indiscriminatamente amici e nemici.

SPT Spot noise: si focalizza tutta l'energia su una sola frequenza (narrow bandwidth). La procedura può essere altamente automatizzata (ASN Automatic spot noise), in modo che il disturbatore possa agganciarsi alla corretta frequenza al primo segnale ricevuto. Il disturbo, a seconda del segnale, può essere continuo (CN), a impulsi (PN), modulato (NSAM), ecc.



EPM (ECCM): il radar controbatte cambiando frequenza all'interno della banda (su spread spectrum). I moderni disturbatori possono seguire un cambio prevedibile di frequenza (pseudo-random, basato su algoritmi che consentono la replicabilità), perciò la variazione deve essere realmente casuale (truly random). Si possono adoperare più disturbatori ma senza garanzia di successo. Un'altra tecnica consente di cancellare l'interferenza (Polarization canceller), prendendo il segnale, modificando la sua ampiezza ed invertendone la polarità. Quando i due segnali, falso e reale, sono sommati, l'interferenza sparisce. Sfortunatamente esistono jammer "polarization agile"che cambiano rapidamente polarizzazione . Inoltre la cancellazione è inefficace contro disturbatori multipli. A questo si può ovviare con i "cancellatori di polarizzazione a monoimpulso"digitali…E il gioco continua.

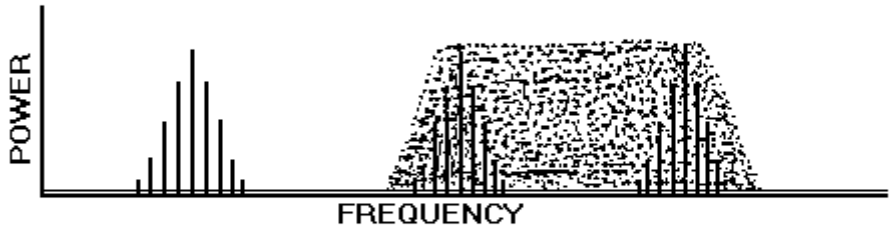
SWPT Swept spot jamming o Sweep jamming (pulse o cw): Se i radar sono numerosi, si può utilizzare il jamming di "spazzata". Tutta la potenza è spostata (swept) passando attraverso tutte le frequenze di una banda utilizzate dai radar, da una frequenza all'altra, con schemi sistematici in veloce successione (fast sequential). Il problema è che, in tal modo, non sono disturbate tutte contemporaneamente, e l'efficacia complessiva è limitata. Rende comunque tutte le frequenze periodicamente inutilizzabili. Una variante più sofisticata è l'SOJ Automatic frequency Set-On-Jamming che, in time-sharing, rileva, forma una lista prioritaria e disturba frequenze multiple simultaneamente.

EPM: molti radar possono cambiare banda o possono esserci più radar che operano su bande diverse. Una buona difesa consiste nel "guard band receiver", con una frequenza adiacente, che oscura il segnale quando il ricevitore mostra un disturbo. Inoltre lo stesso radar può inviare segnali spurii da un'antenna ausiliaria per mascherare il segnale reale con rumore casuale e rendere difficile la rilevazione della frequenza esatta e per sovraccaricare (overload) le difese del bersaglio. Anche l'accurata gestione delle emissioni, in una rete radar, con l'accensione o lo spegnimento in successione dei radar, complica l'opera di disturbo.

BAR Barrage noise e BSAM Barrage-Noise-Swept Amplitude Modulation : se i radar sono numerosi, di diverse caratteristiche, operano su molte frequenze e bande differenti, è il momento di impiegare i “jammer di sbarramento”. Si possono disturbare simultaneamente tutte le frequenze di una banda (broadband) con un solo disturbatore. Ma l’effetto può essere limitato perché tutta l’energia è dispersa su tutte le frequenze. (il raggio di “burn through” sarà maggiore). E più frequenze sono disturbate, meno efficace è il disturbo sulla singola frequenza. La potenza richiesta è altissima. Se, per fare un esempio, la potenza di picco dell’eco radar (alla distanza del bersaglio) è pari a 10Kw, il jammer dovrà impegnare 10Kw di potenza! Se i radar sono 10, dovrà inviare 100Kw! Qui non si fanno sconti. La potenza massima è il fattore dominante: ecco perché metodi simili sono definiti “di forza bruta”. I radar moderni sono pieni di sorprese spiacevoli per i velivoli “dedicati” al supporto elettronico: oltre all’agilità di frequenza, hanno filtri adattativi, ricevitori CFAR, circuiti di soppressione disturbi nei lobi laterali, compressione degli impulsi ecc. ecc. Non ultime, caratteristiche L.P.I.

Così i moderni disturbatori possono scansionare le bande al ritmo di molti GHz al secondo, misurare all’istante la frequenza ed i principali parametri, penetrare i codici degli impulsi emessi (anti-coded waveform), seguire automaticamente i salti di frequenza e riconoscere tutti i metodi difensivi adottati dai radar vittima. La conoscenza precisa del funzionamento del sistema nemico, permette di calibrare il disturbo anche contro il singolo radar (Base Jamming), senza interferire sulle frequenze vicine.

A. BARRAGE JAMMING AGAINST ONE EMITTER



B. BARRAGE JAMMING AGAINST TWO EMITTERS

C. BARRAGE JAMMING AGAINST THREE EMITTERS

Ma le grane non sono finite. Perché qualcuno ha avuto la bella idea di inserire in alcuni missili la possibilità HOJ (home-on-jam): autoguida sulla sorgente di disturbo. Il missile viene così attirato dalle potenti emissioni del disturbatore e, silenziosamente, lo attacca. E allora?

CAJ COOPERATIVE ANGLE JAMMING (mutual protection) : già in Vietnam si utilizzava il disturbo cooperativo di gruppi di aerei, in formazione a quadrato o a pentagono, per rendere più efficace il jamming contro i radar di puntamento e presentare un bersaglio diffuso. Qui la faccenda è diversa. Il gruppo di aerei (due o più) utilizza l'Angular Blinking.

CBN cooperatively blinked noise, BDN blinking doppler noise : i disturbatori sono accesi e spenti alternativamente in modo coordinato, all'interno della medesima "cella" angolare del radar vittima. Questo degrada la risoluzione angolare del radar di ricerca e crea falsi bersagli in un radar TWS, al punto di saturarlo e renderlo incapace di agganciare alcunché. In più, degrada la guida HOJ. Il missile puntato alla coppia di aerei, passerà tra di loro senza danno, perché quando nel suo settore il sensore vede 2 o più sorgenti si dirige sul

centro medio (centroid homing). Lo scherzetto deve essere fatto bene: se la frequenza di “blinking” è troppo alta il radar potrà calcolare i dati di posizione medi, se è troppo bassa il missile centrerà uno dei due disturbatori. Il Blinking jamming risulta efficace anche contro i “polarization canceller” per i motivi già visti.

RBM range bin masking o Cover Pulse jamming: efficace contro radar a bassa e media prf che rilevano la distanza. Il disturbo è temporizzato per cadere entro un intervallo che copre la distanza in cui si può trovare l’aereo.

VBM velocity bin masking o DN doppler noise o Straight-through Repeater : efficace contro radar ad alta prf che sfruttano la variazione di frequenza doppler dei bersagli. Ricevuto il segnale, variano la frequenza Doppler e la ritrasmettono indietro, rendendo il radar incapace di ricavare la distanza reale.

Con questi ultimi sistemi iniziamo già ad entrare nel settore dell’inganno elettronico, con tecniche molto più sofisticate. Prima di proseguire, qualche altra diavoleria difensiva adottata come protezione dai radar (EPM):

Hole-finding: dopo una serie di impulsi, il radar controlla il ricevitore per determinare la frequenza che ha il più basso livello di disturbo. Si sposta quindi sulla nuova frequenza.

Dwell time: il ricevitore del radar è regolato per accettare nuovi segnali solo dopo una sosta (dwell) prefissata, in base al tempo occorrente ai veri segnali per ritornare indietro. Così gli impulsi di disturbo vengono scartati.

Nota: l’agilità di frequenza avviene a ritmi vertiginosi, alcune migliaia di volte al secondo. Tanto che, praticamente, ogni impulso è diverso dagli altri.

Tecniche di inganno (Deception jammer)

L’ingannatore non mira a nascondere l’eco, ma fornisce false informazioni di direzione e distanza, spesso senza che l’operatore nemico se ne accorga. L’inganno usa metodi molto diversi per ottenere lo scopo. Rispetto ai disturbatori, la potenza richiesta è proporzionale a quella media (non a quella di picco) e al numero di bersagli generati. La potenza media si può ricavare tramite il Duty cycle (o Duty factor) e, senza scendere in noiose spiegazioni, diciamo che può essere molto bassa, decine o centinaia di volte meno. Problemi: generare movimenti e bersagli credibili, espansione dell’eco e rischio di rilevamento passivo.

FTG False target generator. I generatori di falsi bersagli sono impiegati, per esempio, contro radar TWS (track while scan) e possono saturare i computer di falsi ritorni, ritardati rispetto a quelli reali, dando l’illusione di un’enorme

quantità di bersagli. Si dividono in ingannatori non-coerenti (Transponder) e coerenti (Repeater).

Transponder: riceve gli impulsi, attende un certo tempo, corrispondente al raggio desiderato del falso bersaglio, e lo ritrasmette identico, producendo falsi echi a diverse distanze rispetto al bersaglio reale. Con questo sistema è difficile ottenere bersagli "credibili", così viene impiegato assieme al disturbo che degrada la rilevazione radar, impedendo di distinguere i falsi bersagli. Prendendo l'esempio precedente, se la potenza di picco dell'eco radar è di 10Kw, quella media può essere di solo 1Kw o magari di 100w! Impiegando la medesima potenza di emissione si potranno generare decine di bersagli. Se i radar sono 10, tutti con frequenze diverse, si potranno creare falsi bersagli per tutti, programmando echi diversi per ognuno. E questo è vitale! Perché altrimenti il nemico potrebbe eliminare i falsi echi per comparazione (de-ghosting). L'unico neo è la potenza di elaborazione, che contro 10 frequenze diverse, aumenta di 10 volte! Se i radar invece emettono tutti sulla stessa frequenza, le cose si mettono male: l'elaborazione aumenta in modo esponenziale, per dividere gli impulsi in arrivo (de-interleave). Ma, a parte il fatto che è raro trovare 10 radar uguali tutti a distanza ravvicinata, 10 radar sulla stessa frequenza sono un bersaglio fantastico per uno Spot jammer : si disturbano tutti in una volta sola!

EPM: Compressione degli impulsi (Pulse compression): rende i radar resistenti ai Transponder. La compressione degli impulsi migliora la risoluzione, aumenta la potenza media e riduce il clutter e/o il disturbo. Questo sistema è vulnerabile, però, ai Repeater con DRFM.

RPTR Repeater: produce un falso bersaglio più realistico rispetto al transponder grazie alla memoria all'interno del jammer. Riceve gli impulsi, li amplifica e, dopo un certo tempo, li rispedisce indietro. Genera frequenze doppler molto diverse sul radar. Errori di azimuth, raggio e numero di bersagli.

EPM: i veri bersagli presentano fluttuazioni del segnale (amplitude scintillation-angular glint), hanno accelerazioni realistiche , mentre i segnali prodotti dai transponder e dai repeater sono stabili. I radar "Leading-edge" ,combinati con agilità di frequenza e processori di segnale avanzati, sono in grado di rilevare le differenze.

DRFM Repeater : Digital radio frequency memory, Coherent Repeater Jamming: grazie all'uso di nuovi microprocessori, riceve l'impulso, ne conserva un campione digitale, lo sintetizza in un realistico, falso ritorno temporizzato e lo rispedisce. Cambia la distanza rilevata dal radar cambiando il ritardo nella

trasmissione degli impulsi , la velocità rilevata cambiando la variazione doppler del segnale trasmesso o l'angolo di tracking usando tecniche AM per trasmettere nei lobi laterali (sidelobe).

RSAM Repeater swept amplitude modulation: in alcuni vecchi radar si utilizzano due lobi paralleli, ed il computer confronta i segnali ricevuti passando da un lobo all'altro (switching), con una determinata "Lobing frequency". Se si conosce la frequenza di switch, si può programmare l'ingannatore in modo da inviare un segnale forte o debole quando il lobo è puntato lontano dall'aereo. Alla fine il computer elabora i due segnali dei lobi e, involontariamente, inserisce il falso segnale d'inganno. Questa tecnica degrada o interrompe l'aggancio. Non funziona contro i radar monopulse.

EPM: il modo migliore per evitare tutto ciò è il radar LORO (ve lo spiego dopo) che nega all'ingannatore ogni dato di Lobing. L'ingannatore può inviare gruppi di segnali non sincronizzati per disturbare i LORO ma l'effetto non è dei migliori.

NBRN Narrow-band repeater noise: in un radar Doppler degrada pesantemente l'aggancio del bersaglio. Questa tecnica provoca la formazione di falsi segnali che appaiono sia sopra che sotto la frequenza dell'eco reale. E' utilizzata anche la modulazione d'ampiezza. Il risultato è una uniforme distribuzione di "rumore" sulla banda, che maschera così il bersaglio.

MFR Multiple frequency repeater o FDT False Doppler target: ripetitore coerente con modulazione d'ampiezza che produce un segnale a numerose frequenze, equamente spaziate attorno alla frequenza dell'eco del bersaglio, ognuna con ampiezza più grande di quella dell'eco reale. Induce errori di distanza e calcolo del "range gate"(ve lo spiego dopo) dei radar Pulse Doppler o introduce falsi bersagli nei radar a impulsi in modalità ricerca. Può disturbare anche le operazioni di AGC (automatic gain control) dei radar.

RD Random Doppler: produce falsi bersagli Doppler e causa confusione durante la sequenza di ricerca ed acquisizione. Oltre al vero eco, invia falsi segnali più forti, la cui frequenza cambia casualmente per periodi di 20 millisecondi.

EPM: Double/short pulsing: tecnica difensiva utilizzata dai radar contro i Repeater ad impulsi, basata sul controllo del periodo di "pausa" dopo ogni impulso di disturbo.

Track breaker (interruttori di traccia)

Ve ne sono diversi, con diverse modalità di inganno. Quelli che tratteremo adesso sono i cosiddetti "Gate stealer". Sono impiegati contro radar di

tracciamento in modalità STT (singol target track) con prf basse e medie, ed attaccano i meccanismi automatici di inseguimento usando sofisticati Repeater. La tecnica è geniale.

RGPO Range gate pull off o RGWO Range gate walk off o RGS Range gate stealing:

Una volta individuato il bersaglio, il radar piazza “range gate” (“gate” si può tradurre in molti modi: cancello, portone…) ai suoi lati. Questi oscurano tutti i segnali originati da distanze fuori di uno stretto intervallo, incrementando il “Signal-to-noise ratio” e proteggendo il radar da impulsi di disturbo non sincronizzati. Il radar si concentra su un intervallo di distanze di poche centinaia di metri, che racchiudono la posizione del bersaglio, e non cerca più altri bersagli. Si ottiene il codiddetto “Lock-on”. Ma il “range gate” può essere catturato ed il radar “sedotto”. Dopo aver rilevato che un radar ha ottenuto il lock-on, il jammer si attiva:

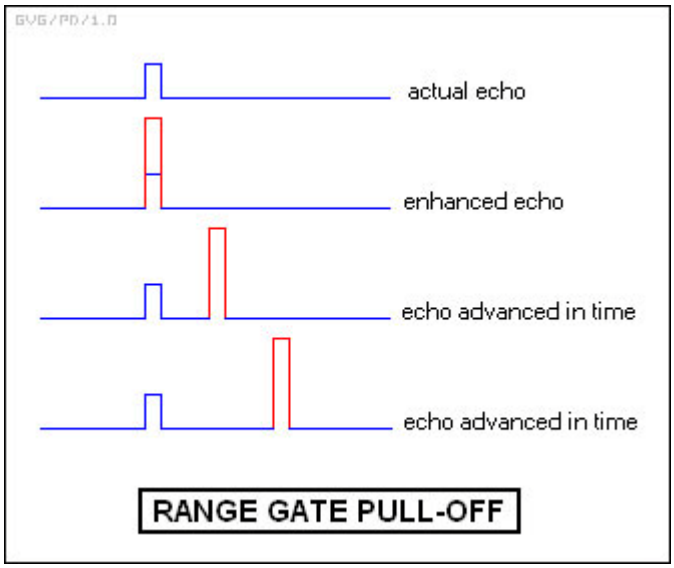
1. Un campione di impulso è amplificato e rispedito immediatamente indietro quando altri impulsi sono ricevuti. Sembra una pessima idea: il bersaglio appare più “evidente” sullo schermo radar. Invece, la trappola sta per scattare! La potenza viene incrementata e continua finchè la “replica” è molto più forte del vero eco. A questo punto il radar è costretto a ridurre automaticamente la sensibilità del ricevitore, per evitare un sovraccarico. E, ovviamente, il vero eco si perde nel rumore di fondo.

2. una seconda replica, più forte, viene trasmessa dopo la prima eco falsa, la cui potenza viene, invece, ridotta.

3. Il radar aggancia la replica che viene, rispetto ad ogni nuovo impulso, ritardata progressivamente. Il “range gate”segue la falsa eco, che sembra retrocedere. Questo continua finchè il “gate”si è spostato fuori dalla vera posizione dell’aereo.

4. L’ingannatore si spegne, lasciando il radar con il “range gate” vuoto (break-lock). Il radar è costretto a tornare in modalità ricerca, perdendo tempo. Se dovesse riacquisire il bersaglio, sarà sufficiente ripetere la procedura. L’RGPO crea falsi bersagli solo a distanze più elevate rispetto a quelle vere, perché i segnali sono inviati con ritardo. Se il radar ha una ripetizione degli impulsi costante, si può però facilmente prevedere l’impulso successivo e creare bersagli a distanze minori : RGPI Range Gate Pull-In.

L’inganno rende impossibile guidare un missile e funziona anche contro radar ad onda continua (CW). E il bello è che, se il missile è dotato di guida HOJ, nel momento in cui l’ingannatore si spegne…Anche il missile perde il bersaglio.



VGPO Velocity gate pull off o VGWO oVGS: i radar Doppler e Pulse doppler sono importanti perché consentono la rilevazione di bersagli a bassa quota dove, a causa del clutter indotto dal terreno, i radar tradizionali ad impulsi sono del tutto inefficaci. I radar Doppler hanno “velocity gate”che concentrano l’attenzione su bersagli con velocità radiali entro certi limiti, per esempio 100 m/sec. Con i radar Doppler, il trucco è simile. Si cattura il “velocity gate”in frequenza Doppler, si amplifica il segnale e si rispedisce indietro. Gradualmente si sposta le falsa frequenza doppler su o giù, spingendo lontano dall’aereo il “gate”. Alla fine si spegne il Repeater, lasciando il “gate” senza segnale, provocando il break. Ed il radar è costretto a ripetere la sequenza di acquisizione. Se serve si ripete. Funziona al meglio contro radar con Prf alte e radar CW.

EPM: i radar moderni sono in grado di riacquisire il bersaglio molto velocemente, utilizzando la Bandwith expansion.

Double pull: per aggirare l’ostacolo l’RGPO ed il VGPO spesso operano di concerto, oppure combinati con l’Inverse gain e l’SSW (poi ve li spiego) per interrompere anche l’Angle tracking. Spesso si trasmette anche rumore di fondo (Noise floor) per complicare la vita al radar.

Dwell walk: un’altra tecnica di inganno del “gate” : l’ingannatore rileva i parametri del gate (angle, range, velocity) e li ripete per un tempo limitato (dwell) così il radar si aggancia al segnale di disturbo. Lentamente il sistema varia i parametri per simulare un movimento di allontanamento dalla reale posizione. Quando la distanza ottenuta supera di 10 volte il “gate”, l’inganno si disattiva, lasciando il radar senza bersaglio.

EPM: il radar può utilizzare “gate” addizionali (Guard gating), oppure può ritardare ogni impulso in modo diverso (Jitter) in base ad una sequenza casuale. Il sistema d’inganno non può, così, capire quando arriverà l’impulso

successivo e risponde in ritardo, non potendo così generare bersagli più vicini. Anche i falsi bersagli più lontani possono essere, però, eliminati controllando l'intensità dei segnali (signal strenght) che, come abbiamo visto, è più alta (è proprio l'RGPO che, all'inizio, ha inviato un impulso più forte).

La tecnica del "Leading edge track"e l'agilità di frequenza, rallentano ulteriormente i tempi di risposta dell'ingannatore. Che può rispondere solo aumentando la potenza, così tanto da catturare i circuiti di "automatic gain control"o inviando impulsi di disturbo abbastanza lunghi da coprire l'intero "jitter period".

VGPO+RSAM : nell'ultima parte del programma VGPO, si applica l'RSAM. Poiché il "velocity gate"è già spostato, l'inganno angolare è facilitato.

CGS Chirp Gate Stealer: simile al VGPO ma la deviazione è 20 volte superiore. Si usa contro radar che adottano la "pulse compression"(Chirp). Il radar interpreta i cambi di frequenza del CGS in variazioni della distanza. Così facendo il CGS allontana il radar dal vero bersaglio, e poi si disattiva.

Per aiutare nella comprensione dell'argomento (oggettivamente difficile), segnalo questo sito:

http://www.geocities.com/jasonlemons/radar/topic1.htm Guardatevi anche le parti 2 e 3.

EPM: una nota aggiuntiva chiarificatrice a proposito del "Leading edge track". Il radar controlla l'intensità dell'eco, osservando se "brilla" in modo eccessivo. Se la risposta è affermativa, il radar traccia il "leading edge" dell'eco reale (il primo impulso ricevuto), ignorando l'impulso ritardato più forte. Il "leading edge" di un impulso è la parte ascendente dell'onda, prima del picco massimo di potenza. Un'altra buona contromisura è il "burn-through"(stesso nome, perchè è in relazione col precedente). Abbassando la PRF, le pause sono incrementate, ed il segnale di ritorno è più forte, al prezzo di minore precisione.

Angle deception: inganno che induce errori di inseguimento angolare.

I radar, oltre al fascio principale (main beam), hanno anche indesiderati lobi laterali (sidelobe) che emettono e ricevono energia, con minore efficienza. Questi lobi possono essere rilevati dai sistemi RWR (radar warning receiver) e disturbati.

Sidelobe Jamming: il disturbatore si attiva quando aggancia uno dei lobi laterali più lontani da quello principale (off boresight) ed invia un forte impulso.

Il radar interpreta il segnale come proveniente dal lobo principale. L'effetto risultante è che il segnale sembra provenire da ogni lato: invece di un bersaglio sullo schermo, si vedrà un cerchio attorno al centro.

EPM: si può aggiungere al radar un ricevitore omnidirezionale. Se questo, improvvisamente, rileva un impulso più forte di quello previsto nello specifico settore, probabilmente è attivo un "sidelobe jammer".

Alcuni radar di vecchio tipo utilizzano la modulazione d'ampiezza del segnale e muovono il fascio attorno alla posizione del bersaglio. Due esempi sono gli "Height-finding", che muovono il fascio su e giù, e quelli a scansione conica (ConScan). La scansione conica è un modo semplice per ottenere precisi rilevamenti angolari (frazioni di grado!) anche se il fascio è ampio. Il fascio ruota attorno all'asse di simmetria del radar, leggermente fuori asse di alcuni gradi (forma un cono). Quando il bersaglio è rilevato, l'antenna si ferma ed il fascio ruota attorno all'ultima posizione. La scansione conica si è imposta per la semplice processazione dei segnali adatta all'elettronica a valvole. Se il bersaglio giace nel cono, la rotazione modula il segnale, che sarà più forte se il bersaglio è vicino all'asse, e costante in ampiezza se si trova al centro. Così una variazione indicherà un disallineamento. La direzione del bersaglio si trova attraverso la fase della modulazione. Il segnale può essere a impulsi o CW (onda continua), il primo è più potente ma facilmente disturbabile. In ogni caso il sistema, se si conosce la velocità di rotazione, è attaccabile con successo. Molti missili aria-aria sono guidati con questo sistema. Gli RWR possono rilevare questi radar per la fluttuazione ciclica dell'intensità.

IG Inverse gain jamming o Inverse amplitude modulation: inganno che interrompe l'inseguimento angolare del bersaglio attaccando il meccanismo di scansione conica dell'antenna (il radar misura ancora correttamente la distanza). Se trasmettiamo un segnale modulato (variato) in ampiezza, con una frequenza pari a quella di rotazione dell'antenna, si crea un errore angolare. Si trasmettono forti copie del segnale quando questo è debole , nulle o debolissime se è forte (Inverse gain). Il disturbo si somma all'eco reale, così il radar crederà di aver agganciato il bersaglio quando in realtà è fuori tiro o penserà di trovarsi nel punto sbagliato quando in realtà è puntato correttamente.

EPM: l' Inverse gain jamming misura i parametri del fascio rotante. Ma non c'è nessun bisogno che il fascio radar ruoti quando trasmette il segnale! E'sufficiente che ruoti il ricevitore, eliminando così la fluttuazione ciclica del segnale. Un modo è usare due antenne, una con un fascio fisso per trasmettere e l'altra con fascio rotante per la ricezione. Questo sistema è denominato CSORO (Conical Scan on Receive Only) o LORO (Lobe On Receive Only). Il jammer perde tutte le informazioni utili. Radar di questo tipo, inoltre, rilevano la modulazione d'ampiezza del disturbo e la cancellano prima di processare il segnale.

SSW Swept square wave: i radar LORO non sono esenti da jamming. Sono efficaci nel negare al disturbatore ogni dato sulla frequenza di scansione (quanto velocemente ruota il fascio?) e la fase (quando è sul bersaglio?). Ma il disturbatore può ipotizzare la presenza di un radar LORO e variare l'Inverse gain attraverso una serie di probabili frequenze di scansione, in un ciclo ripetitivo, cercando di rompere l'aggancio. Questa tecnica è denominata SSW (Swept Square Wave). Non è però efficace al 100%.

Tecniche avanzate

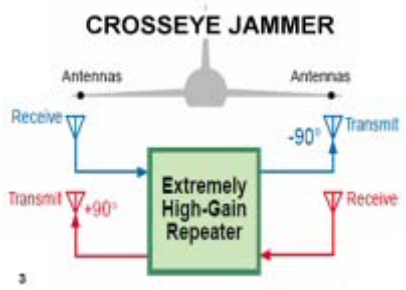
Molti dei metodi di disturbo trattati sono stati sviluppati tra gli anni'50 e '70. Verso la fine degli anni'70 ha fatto la sua comparsa un nuovo, pericoloso, sistema di guida. Il Monopulse.

Monopulse (simultaneous lobing): nei radar a monoimpulso le informazioni sulla localizzazione angolare del bersaglio sono ottenute per comparazione dei segnali ricevuti in due o più fasci simultanei, distinguendosi da tecniche come il lobe switching o il conical scan dove i fasci sono generati in sequenza. Con questo sistema è possibile ottenere con un singolo impulso (monopulse) una rilevazione angolare bidimensionale (azimut e quota). Un comparatore monoimpulso analizza le differenze di fase tra i segnali in arrivo per generare segnali di guida. Se il bersaglio si trova al centro, l'eco arriverà simultaneamente in ogni ricevitore. Altrimenti il segnale entrerà prima nel ricevitore più vicino e poi nell'altro, provocando una variazione di fase, proporzionale all'errore angolare. Di solito si utilizzano quattro ricevitori, due per ogni asse, per migliorare la precisione e fornire migliore risoluzione Doppler. Il sistema può essere utilizzato con radar a impulsi e ad onda contina (CW). E' eccellente negli attacchi contro bersagli a bassissima quota, che rileva eliminando il "clutter" del terreno. Ed è estremamente difficile da disturbare perché insensibile ad inganni angolari provenienti da una sola sorgente. Eppure…Altre trappole sono in agguato.

TB Terrain Bouncing (anche Sea Bouncing): guardando il tramonto sul mare, la superficie dell'acqua è un ottimo riflettore della luce (onda elettromagnetica). Lo stesso avviene con le onde radar. Una superficie può essere considerata "piatta", rispetto alle onde elettromagnetiche, finchè le irregolarità rimangono corte rispetto alla lunghezza d'onda. Il terreno umido per la pioggia o la brina, il ghiaccio, oggetti larghi e piatti , si comportano come specchi radar. Questa modalità viene utilizzata da aerei a bassissima quota. Si utilizza un ripetitore che cattura il segnale radar, lo amplifica e lo ritrasmette facendolo rimbalzare sul terreno con un certo angolo di fronte all'aereo. Il sensore dovrà scegliere tra un'eco debole e un'immagine luminosissima. Questo "hot spot"nel punto dove il segnale è rimbalzato, provocherà o un break-lock o guiderà il missile contro il punto sul terreno.

Difetti della tecnica: la riflessione (scattering) terrestre non è prevedibile esattamente ed inoltre provoca un effetto depolarizzante.

X-EYE Cross-Eye jamming: una delle contromisure più sofisticate mai concepite. Il jammer contiene un'antenna ricevente e una trasmittente in entrambe le estremità alari e un repeater interno all'aereo. I segnali sono ricevuti simultaneamente dalle estremità. Il modulo sull'ala sinistra riceve il segnale radar, lo passa al repeater che ne sposta in avanti la fase e lo passa all'ala destra per essere ritrasmesso indietro al radar. Contemporaneamente, il modulo sull'ala destra riceve il medesimo segnale radar, lo passa al repeater che ne sposta indietro la fase e lo passa al modulo nell'ala sinistra per essere trasmesso indietro al radar. Manipolando la fase (ritardo) dei due segnali di ritorno, il cross-eye distorce la forma dell'eco di ritorno (wavefront), e, quindi, la direzione percepita, creando una distorsione angolare. I due segnali in controfase (180° phase shift) si sommano nel ricevitore radar, producendo un segnale nullo, proprio dove dovrebbe esserci un picco. Il missile cerca di riallinearsi al fronte distorto (credendolo reale), e vira spostandosi lateralmente rispetto all'aereo. L'intero processo dura una manciata di secondi e porta ad errori anche di Km. La potenza in gioco è alta, perché deve coprire l'eco reale. Il sistema funziona ancor meglio utilizzando un'esca rimorchiata (Towed decoy) dotata di repeater.



Nel caso precedente la potenza dei due segnali è identica e cambia solo la fase. E' possibile, però, (necessario in alcuni casi) variare anche in modo coordinato la potenza (amplitude modulation) dei due segnali in controfase. Si attiva solo uno dei repeater. Il sensore monopulse inizia a tracciarlo. A questo punto si attiva il secondo repeater in controfase, la cui potenza cresce fino a raggiungere quella del primo. Il sensore inizierà a spostarsi. Il primo lobo laterale si centrerà sul primo ripetitore. A questo punto la potenza del primo decresce lentamente fino a zero, mentre il secondo la mantiene inalterata. Il punto di mira si sposta ancora. Se, dopo un ciclo completo, la prima fonte è improvvisamente accesa e la seconda spenta, il seeker continuerà a tracciare col suo primo lobo laterale. Ed il ciclo ricomincia, spostando la mira sul secondo lobo laterale, poi sul terzo e così via. La risultante è un continuo spostamento del sensore con incremento costante di errore angolare.

EPM : in questo caso, le migliori contro-contromisure sono il leading edge track o l'uso di "multiple range track". Per evitare, in parte, le possibili difese, spesso il Cross-eye è abbinato a tecniche come l'RGPO.

I segnali radar sono polarizzati, ed una particolare polarizzazione può facilitare, per esempio, la scoperta di bersagli a bassa quota. La polarizzazione può essere di molti tipi: lineare orizzontale (HOR) o verticale (VER), circolare (CP), ellittica, swept (SX), doppia (DOUBLE CROSS), ecc.

X-POL Cross-polarization jamming o PECM Polarization-exchange cross modulation: ripetitore che prende il segnale, lo ruota di 90°, e lo ritrasmette indietro. Ottimo contro missili a guida semiattiva monoimpulso. Causa errori angolari nei radar di puntamento e mette in difficoltà i sistemi ECCM, irradiando un segnale polarizzato "ortogonale" rispetto a quello polarizzato del radar vittima. Richiede alta potenza, pena la scoperta del bersaglio.

EPM: Orthogonal Polarization ECCM. Il radar vittima continua a trasmettere il segnale con la polarizzazione precedente, ma traccia passivamente la polarizzazione ortogonale del Jammer, usandolo come radiofaro. Oppure può ricorrere alla Variable Polarization: variando la polarizzazione può migliorare il segnale nel ricevitore (ma alcuni Jammer possono seguire la variazione!). Può anche sfruttare il fatto che il segnale di disturbo polarizzato proveniente da un solo Jammer (single lobe) è differente da quello prodotto da un vero eco, e cancellarlo mediante filtri appositi (Cross polarization screen).

Altri metodi di disturbo e possibili contromisure.

I prossimi metodi di disturbo sfruttano le debolezze insite in alcuni radar, a livello di elaborazione dati. Sono efficaci, perciò, solo se si conosce in anticipo il livello di sofisticazione dei sistemi da attaccare. Nella fase di elaborazione del segnale di ritorno, vengono effettuate numerosissime operazioni. Una interferenza intenzionale può degradarne il risultato.

Nel radar, un ricevitore a supereterodina usa un oscillatore locale (LO) per convertire una frequenza d'ingresso in una "frequenza intermedia". Questo avviene in un mixer che genera le somme e le differenze nei segnali ricevuti. L'uscita del mixer è filtrata e passata all'amplificatore di frequenze intermedie. La frequenza dell'LO è sopra la prevista frequenza a cui è sintonizzato il ricevitore, di una quantità uguale alla frequenza intermedia, o, per meglio dire, la "frequenza intermedia è uguale alla differenza tra la frequenza a cui il ricevitore è sintonizzato e la frequenza dell'oscillatore locale". Es.: un ricevitore è sintonizzato a 800 khz. Se la frequenza di LO è di 1250 Khz , la frequenza intermedia sarà di 450 Khz. Dov'è il problema? Il problema è che esiste anche una frequenza speculare (Image frequency), in questo caso a 1700 Khz (1250+450), in relazione con le precedenti, e che, conseguentemente, può essere erroneamente accettata e processata come reale dal ricevitore.

IF Image Frequency Jamming : si emette un segnale sull'"Image frequency" di un radar monopulse. Il ricevitore è sintonizzato su di una frequenza adatta a ricevere lo "skin return" del bersaglio. La frequenza intermedia è uguale alla differenza tra la frequenza dell'oscillatore locale e quella dell'eco. Se un segnale che somiglia all'eco, viene ricevuto sull'Image frequency, con sufficiente potenza da superare il filtro, sarà amplificato anch'esso e processato col vero eco. Solo che, essendo invertito in fase, darà valori opposti nel sistema di tracking e muoverà il radar lontano dal bersaglio invece che verso di esso.

EPM: inefficace se il ricevitore radar è dotato di "image rejection" che attenua il segnale dell' image frequencies. Ma il sistema monopulse può anche utilizzare passivamente il segnale dell'Image Jammer per tracciare il bersaglio, procedura indicata come " Image-enhanced mixing".

Delta Jamming: si trasmettono due segnali in radiofrequenza, le cui frequenze sono separate in modo tale da causare falsi segnali di frequenze intermedie nell'amplificatore del radar. Provoca errori angolari nei radar monoimpulso.

Uno dei tanti filtri incorporati nei radar, si occupa di attenuare i segnali fuori della banda di interesse del ricevitore, sintonizzato per ricevere l'eco. Un segnale lontano da questo settore verrà rigettato completamente. L'attenuazione aumenta fino ad un massimo in prossimità del cosiddetto "filter's skirt". Qui, le frequenze, sopra e sotto quella prevista, sono ancora nel "range" del ricevitore e la risposta di fase del filtro è indefinita.

Filter Skirt Modulation: un segnale molto forte fuori della banda ma in prossimità delle "Skirt frequency" , verrà rigettato solo in parte dal filtro. La fase verrà sconvolta causando malfunzionamenti nei circuiti di inseguimento del radar. Il rapporto J/S (disturbo/segnale) deve essere molto elevato, per superare il rigetto del filtro e coprire il vero ritorno.

Glint enhance jamming: Abbiamo già detto che un vero bersaglio, illuminato da un radar, non presenta una traccia costante. A causa della riflessione delle onde radar sui vari punti del velivolo, il segnale presenta variazioni di potenza, riflessi e bagliori (scintillation-glint) improvvisi. Un effetto simile si può ottenere con un disturbo trasmesso alternativamente da differenti antenne, passando da una all'altra in sequenza o in modo casuale.

NCDB Noise Countdown Blink e BCDB Barrage Countdown Blink

Inganno angolare dei radar d'inseguimento, che fanno uso di AGC (Automatic Gain Control). Un segnale di disturbo o inganno del tipo On-Off viene trasmesso con una frequenza e un duty cycle tali da portare sempre fuori livello l'AGC. È così chiamato perché in origine, per calcolare il periodo di variazione del duty cycle, si usava un contatore e si effettuava un conto alla rovescia. Per capire come funziona bisogna richiamare il funzionamento di un AGC. Il segnale di interesse, nel "range gate", è confrontato con un valore di riferimento. Se risulta troppo alto, si genera un segnale di errore per ridurre il guadagno sulla IF (frequenza intermedia), se è più basso si incrementa. L'AGC compensa così le fluttuazioni d'ampiezza dell'eco dovute a scintillazione, variazione di dimensioni apparenti del bersaglio, ecc. Nei radar ConScan o Lobe-switching vanno utilizzate precauzioni per limitare l'AGC allo stretto indispensabile onde evitare magari la cancellazione del segnale per eccesso di correzione. Per esempio se la scansione è a 100hz, l'AGC si limita a 10 hz , opera cioè a bassa frequenza attorno al valore principale del segnale. Se un segnale di disturbo impulsivo o CW viene trasmesso ad alta frequenza e con un duty cycle (variabile) adatto, l'AGC si posizionerà per ricevere il falso segnale. Il radar non saprà ricavare la modulazione necessaria per tracciare nè il segnale reale, troppo debole, nè il disturbatore (track-on-jam). Nei confronti dei radar monopulse invece, bisogna ricordare che le informazioni angolari sono ottenute con un singolo impulso. Se l'AGC è disturbato, la media delle correzioni sarà corretta, ma la loro ampiezza sarà o troppo grande (ricevitore saturato) o troppo bassa (guadagno troppo basso del ricevitore).

Altre difese adottate dai radar (EPM):

Blanking : oscura parte del segnale di disturbo ricevuto, sulla base del calcolo dei tempi, della fase e frequenza del segnale o della direzione di arrivo, per ridurne l'efficacia.

Beam-to beam correlation: utilizzata su radar che impiegano fasci multipli di rilevamento sovrapposti. I segnali non correlati a quelli dei fasci adiacenti sono rifiutati automaticamente.

Pulse position memory: l'impulso radar deve essere ricevuto in due successivi periodi di ripetizione degli impulsi, nello stesso intervallo di distanze, prima di essere processato.

I radar di ultima generazione (come gli AESA) sono ancora più difficili da disturbare. Molti possiedono caratteristiche tali da renderne lo stesso rilevamento problematico (L.P.I. : a bassa probabilità di intercettazione). Di questi radar si è parlato abbondantemente altrove, così non entrerò nel dettaglio. Sintetizzando, si può dire che il radar attuale emette da ogni

elemento radiante (e possono essercene migliaia!) impulsi a bassissima potenza (pochi Watt), con agilità estrema di frequenza e fasci multipli altamente direttivi, senza praticamente lobi laterali, su bande di frequenza molto estese, con controllo variabile della potenza, con compressione degli impulsi o "pulse burst", con forme d'onda variabili in modo casuale, con ricevitori intelligenti e processori anti-disturbo sempre più sofisticati. Eppure…La nuova generazione di Jammer imbarcati sull'EF18 Growler si dice sia in grado di mettere nei guai anche questi sistemi.

Intanto, assieme ai metodi "tradizionali", si stanno studiando nuove tecnologie, ancora coperte da segreto. Accanto a modalità che prevedono il sovraccarico dei circuiti del radar nemico con emissioni concentrate di altissima potenza (ancora in fase sperimentale) , qualcosa di diverso comincia a trapelare.

Active Cancellation: nuovo metodo di inganno, concettualmente semplice. Il jammer genera un segnale uguale a quello riflesso dal velivolo, ma fuori fase di 180° (anti-phase copy), per fornire un segnale composto pari a zero, in grado di cancellare l'eco in modo totale. In teoria non richiede neppure potenze elevate, visto che la potenza dell'eco riflesso è limitata. Il problema è che l'emissione deve essere calibrata con precisione, altrimenti il segnale verrà amplificato invece che annullato. Inoltre, mentre le caratteristiche del segnale in arrivo sono determinabili, quelle del segnale riflesso richiedono la perfetta conoscenza della riflettività dell'aereo alle varie frequenze ed angoli di incidenza delle onde radar. Se è fattibile con i radar a bassa frequenza è oltremodo difficile con quelli ad altissima frequenza…E se poi i radar sono molti? La velocità di processazione diventa elevatissima. L'obbiettivo è realizzare un sistema in grado di cancellare l'eco in molte direzioni contemporaneamente, per nascondere il velivolo alle reti radar. Si sospetta possa essere operativo sui velivoli Stealth (B2, F22), che, per le caratteristiche di bassissima riflettività, sarebbero i migliori candidati per l'applicazione del sistema.

Adesso trattiamo qualcosa di diverso. Qui non si parla di "attacco elettronico" in senso stretto, perché i prossimi sistemi fanno parte del cosiddetto "mechanical jamming". Ho pensato di inserirli perchè non è possibile terminare l'argomento senza parlare del "Chaff"e degli altri metodi passivi di difesa.

Chaff, Active expendable,Corner reflector, Towed decoy, Radar decoy (RPV e Drone).

Chaff: strisce di fogli di metallo o , più spesso, fibre di vetro metallizzate tagliate alla metà della lunghezza d'onda del segnale radar da disturbare. Ogni elemento si comporta come un "dipolo". Il Chaff è stato uno dei primi sistemi antiradar, impiegato già nella seconda guerra mondiale e conosciuto allora in molti modi: window, düppel, giman-shi. Lanciato in quantità, forma una nuvola

riflettente che può schermare il velivolo o creare una falsa eco. Il problema è che la nube in questione rimane quasi immobile e si disperde dopo una quindicina di minuti.

Il chaff può essere lanciato in quantità direttamente dall'aereo, creando corridoi di decine di km, ma l'effetto non è dei migliori perché l'aereo apparirà al vertice di un segnale allungato. Diversi dispositivi, interni o in pod, sono in grado di prelevare il materiale riflettente da rocchetti contenenti migliaia di km di filo, tagliare ad alta velocità il chaff nella misura richiesta ed espellerlo nella quantità voluta. Per coprire una serie più ampia di frequenze, si possono formare nubi con chaff tagliato a differenti lunghezze (broadband chaff). Oppure si può lanciare il chaff tramite cartucce, di varie dimensioni, che in due secondi creano una traccia sullo schermo radar nemico. Le cartucce russe da 26mm, ad esempio, danno una RCS di 5 mq, quelle da 50mm, di 15-20 mq. Il chaff può essere inserito anche in razzi e proiettili. E'molto efficace contro i radar ad impulsi più vecchi, che non possono distinguerlo dal vero bersaglio. E'invece rifiutato facilmente dai radar dotati di MTI (moving target indicator) o da quelli Doppler. Molti lo ritengono, per questo motivo, superato. Invece…

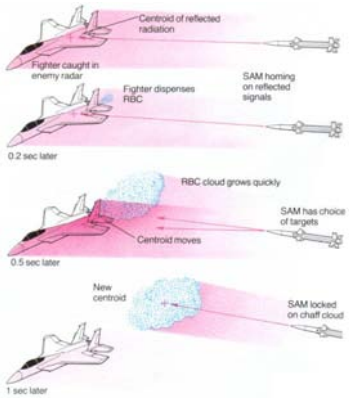
I nuovi "smart"threat-adaptive dispenser , come gli ALE 45 e 47 lanciano chaff e flare secondo schemi intelligenti in grado di affrontare minacce sofisticate.

Il chaff può essere usato per obbligare un radar ad operare in modalità Doppler, funzione che rende difficile il "Jitter"(sbalzi continui della frequenza di ripetizione degli impulsi) e favorisce l'uso di certi tipi di attacco elettronico.

Rilasciare il chaff durante l'esecuzione di una manovra in direzione del fascio radar, può provocare lo spostamento del tracking dall'aereo alla falsa eco (nei radar Pulse Doppler o MTI), a causa della lenta processazione di molti radar comparata alla manovra dell'aereo nel clutter del fascio principale.

JAFF (jamming+chaff) o ILLCH Chaff Illumination : l'aereo lancia una nuvola o un corridoio di chaff e un transponder ritrasmette il segnale radar incidente verso la nube, che funge da specchio ed allontana il missile che si dirigerà sul falso bersaglio più attraente.

Seduction chaff: tecnica utilizzata per presentare un'esca con RCS comparabile o maggiore ad un missile a guida radar che abbia già acquisito il bersaglio. Deve essere lanciato molto vicino al bersaglio da difendere, in modo che il sensore possa acquisire contemporaneamente anche la nube esca, tecnicamente ad una distanza inferiore alla "pulse width" del radar.



Distraction chaff : si generano un certo numero di nuvole chaff come falsi bersagli. Questi devono essere posizionati rispetto al bersaglio in uno schema che assicuri che il missile individui per prima cosa un falso eco credibile, prima che avvenga l'acquisizione o dopo essere stato depistato da tecniche come Angle/Range Gate Stealing. Non è necessario che la falsa traccia abbia una RCS elevata, ma deve essere lanciata ad una notevole distanza per distrarre il missile. Il sensore del missile in arrivo è prima sedotto dal disturbatore e poi forzato a inquadrare il chaff già dislocato. Il chaff può essere lanciato in sequenza, utilizzando piccoli razzi, ad una certa distanza da una nave in modo da simulare un bersaglio in movimento.

Active expendable decoy jammers (AED) : spesso assieme al chaff si lanciano anche piccoli dispositivi di disturbo (jammer) o inganno (deception repeater), dotati di paracadute ed alimentati a batteria. Utili per degradare ulteriormente le funzioni del radar o sedurre i missili ad autoguida. La loro potenza è, però, limitata. Inoltre la velocità di caduta rende possibile l'identificazione come esche. Tra questi possiamo citare il Sanders POET (Primed Oscillator Expendable Transponder) ed il GEN-X (Generic Electronic Expendable). Risultati migliori possono essere ottenuti utilizzando le esche rimorchiate (towed decoy).

Corner Reflector : sono costituiti da diedri o triedri (superfici concave a due o tre lati) in grado di riflettere interamente le onde elettromagnetiche verso la sorgente. Sono in grado di amplificare enormemente la traccia. La versione moderna è la Lente di Luneburg. I Corner reflector possono, per esempio, essere utilizzati a bordo di velivoli senza pilota e simulare così la traccia di un bombardiere. O possono essere posizionati su galleggianti ad una certa distanza da una nave e confondere così il nemico.

Towed decoy : esca rimorchiata. E' una delle migliori contromisure. Il cavo convoglia i segnali generati dall' RWR che comanda la trasmittente nell'esca, per trasmettere una copia amplificata del segnale o semplice disturbo. Nel primo caso, la falsa eco trasmessa è molto più forte di quella reale, e il missile punterà sull'esca. Nel secondo caso, il seeker non sarà in grado di rilevare la distanza, e passerà alla modalità 'home-on-jam', puntando sull'esca. L'uso di

contromisure del tipo X-EYE, X-POL e Blinking risulta ancor più efficace, perché il decoy è ad almeno 100 metri di distanza. Il decoy è piccolo e forse sfuggirà all'impatto e, anche se distrutto, l'aereo si salverà. Le esche rimorchiate limitano la manovrabilità del velivolo e l'uso del postbruciatore. Tra i più conosciuti l'ALE50 e ALE55 americani ed il sistema imbarcato sul Typhoon (DASS).

Benchè i Towed decoy siano una buona soluzione, l'esplosione di una testata massiccia potrebbe coinvolgere ancora l'aereo. L'esca perfetta è un drone che simuli in tutto l'aereo bersaglio.

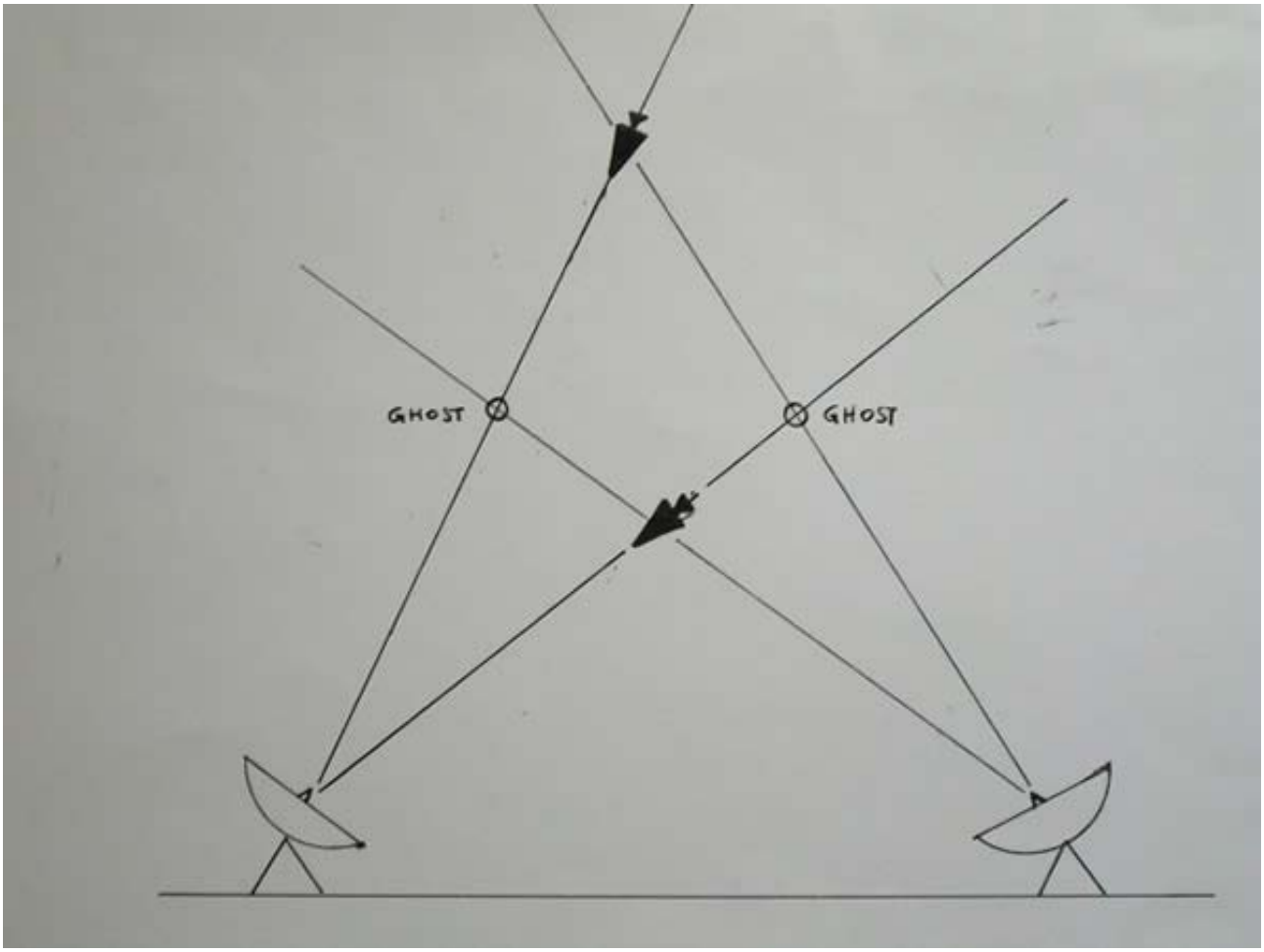
Radar decoy (drone e rpv): passivi o attivi. I passivi hanno un corner reflector o chaff dispenser. Quelli attivi hanno di solito un "repeater". Devono avere una traccia comparabile a quella del velivolo e simularne velocità ed accelerazione. L'uso di piccoli velivoli senza pilota utilizzati come esche, ha molti precedenti. Un esempio per tutti: l'ADM20 Quail. Lanciato dai B52 e dai B47, era in grado di simulare la traccia radar e termica del bombardiere e disturbare i radar nemici con l'uso di repeater e chaff. Poteva effettuare due virate programmate ed una variazione di velocità e quota. Nel 1982 gli israeliani hanno utilizzato il Samson. Il modello recente più conosciuto è l' ADM 141 TALD.

ADM-20 QUAIL DECOY (GVG / PD)

Oltre ai metodi trattati, altri problemi possono traviare la vita degli operatori radar. Uno di questi è l'Autoinganno.

Una rete radar può essere estesa, teoricamente efficace, ma non integrata in modo adeguato. I dati provenienti dai sensori radar provocano così la mancata correlazione delle coordinate. Questo porta alla sovrastima del numero dei velivoli attaccanti ed il rischio che per ogni traccia compaiano due (o più) echi con i dati rispettivi.

Ma anche una rete radar perfettamente integrata (integrated network) presenta un rischio potenziale. Se un Jammer disturba uno o più radar, gli stessi possono reagire triangolando la posizione del disturbatore. La triangolazione fornisce il principale dato mancante: la distanza. E consente l'attacco contro il bersaglio. Sfortunatamente questo sistema funziona solo contro un numero limitato di jammer (1-2). Vediamo perché, in termini semplici.



Come si può vedere la triangolazione di due jammer fornisce si la posizione, ma crea contemporaneamente due Ghost (fantasmi). E il guaio è che, all'aumentare del numero dei disturbatori, il numero dei Ghost aumenta in modo esponenziale. Così per due disturbatori appaiono 4 tracce, per tre disturbatori 9 tracce! E così via…Esistono tecniche per aggirare l'ostacolo, ma

questo dimostra ancora una volta l'estrema complessità dell'argomento "guerra elettronica".

Nel trattare l'argomento "attacco elettronico" ho avuto un occhio di riguardo per la componente "aerea", ma ovviamente le tecniche indicate trovano uso anche nel combattimento navale e terrestre. Naturalmente con potenze in gioco e dimensioni differenti. Se una nuvola di chaff di 10 metri quadri può essere sufficiente per un aereo, una unità navale è in grado di creare nuvole di 10000 metri quadri! A proposito del Chaff: la teoria dice che va tagliato alla metà della lunghezza d'onda di interesse. Così facendo, però, le laminette metalliche risulteranno efficaci anche per i multipli della lunghezza d'onda. La durata di una nuvola di chaff è variabile, a seconda della quota e delle correnti, da un minimo di 5 minuti a bassa quota fino a 30 minuti o più alle alte quote.

Una nota circa il tempo di reazione dei dispositivi di disturbo. Un buon apparato in pod sub-alare in modalità automatica è in grado di emettere un segnale di disturbo circa 1 secondo dopo la ricezione di un segnale ostile. Vi sembra un buon valore? Allora sappiate che sistemi navali come l'SLQ32 in dotazione alle unità americane sono in grado di rispondere al "primo" impulso ricevuto! Praticamente in tempo reale, prima ancora che il segnale possa essere visualizzato sui monitor dell'unità nemica.

Quanto "dura" un disturbo? Dipende dalla situazione, in genere è bene non superare i 20-30 secondi, passati i quali o il radar ha cessato di emettere o (peggio) ha cominciato a tracciarvi passivamente. Per quanto tempo è efficace una tecnica di "interruzione di traccia"come l'RGPO (Range gate pull off)? Circa 10 secondi. Passati i quali il radar riuscirà a riagganciare il bersaglio (meno se c'è un operatore abile o se il radar è molto moderno), obbligando a ripetere il disturbo. Non dovete pensare che 10 secondi siano pochi: un aereo si sarà allontanato già di parecchi km, e questi possono fare la differenza.

by Gian Vito
2009