

blinking jamming with others decoys or aircraft to deal with HoJ missiles.

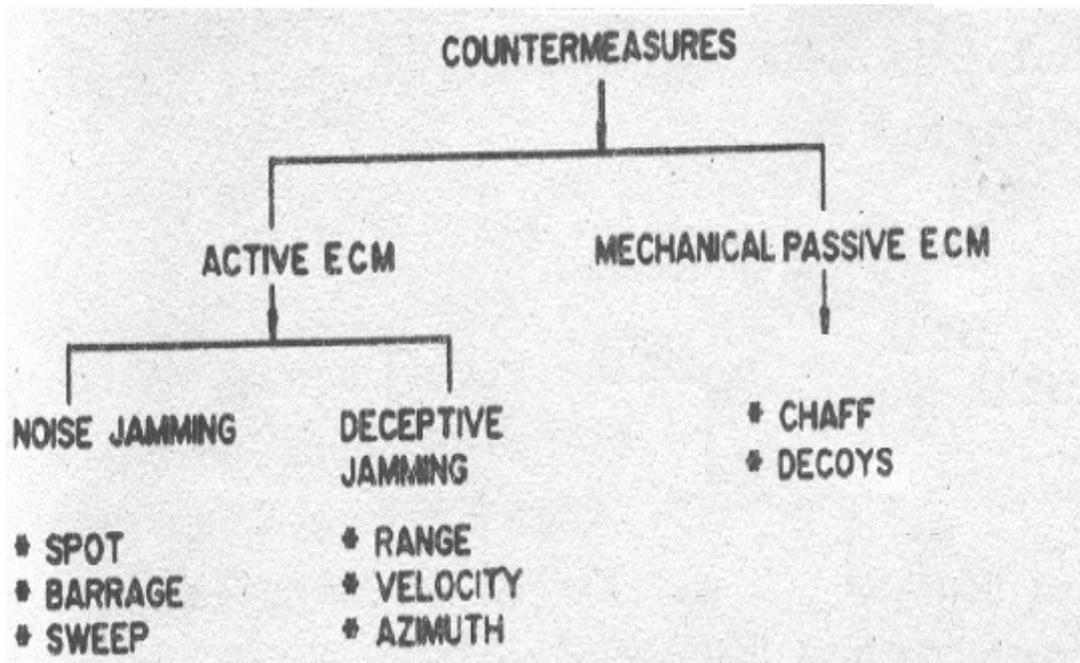
- Compatible with a wide range of platforms and weapons racks , a single fighter can carry as many as 18-20 decoys using triple and multiple ejector racks

**Disadvantages:**

- Occupied weapons station thus reduce missiles-bombs load
- Increase aircraft total drag and radar cross section when carried on pylons ( not apply to aircrafts with internal weapons bays )
- Non-Cooperative Target Recognition (NCTR ) techniques such as jet-engine modulation used by modern radar (most radars after 1980s) can distinguish decoys from real aircrafts.
- Reduce platforms agility when carried in large number

# Electronics Countermeasure Techniques

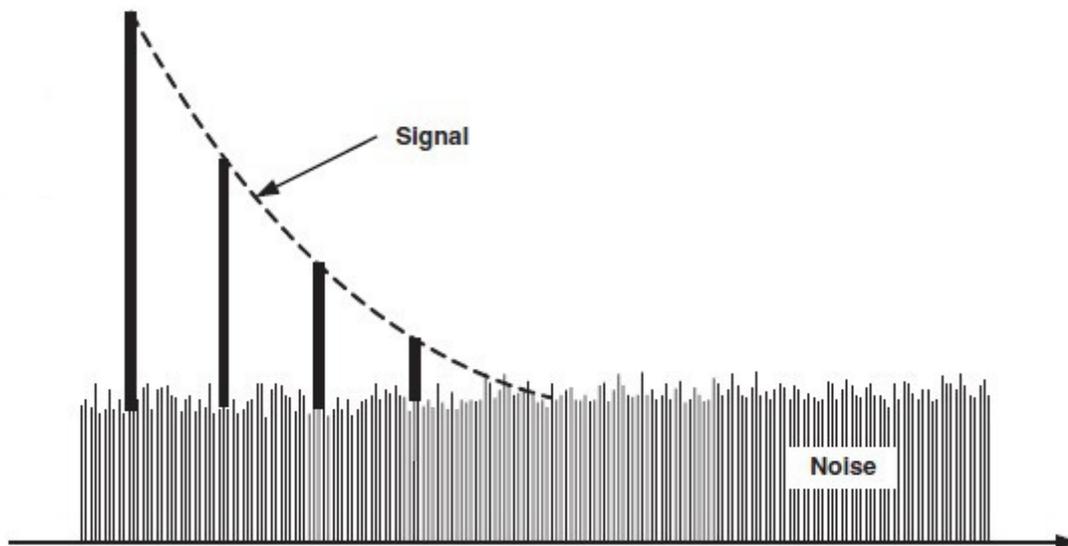
Radar countermeasures are often divided to electronic (active) and mechanical (passive) types. Mechanical countermeasure systems reflect radar waves passively no transmitting antenna or receiver required , some example of passive countermeasure are chaff, air launched decoys. By contrast, active electronic countermeasure (jamming) involves systems that transmitting radio waves to reduce the effectiveness of enemy radar ,an example of active electronic countermeasure system are ECM pod , FOTD .



Some common jamming techniques will be explained below. To begin with , jamming can be categorized

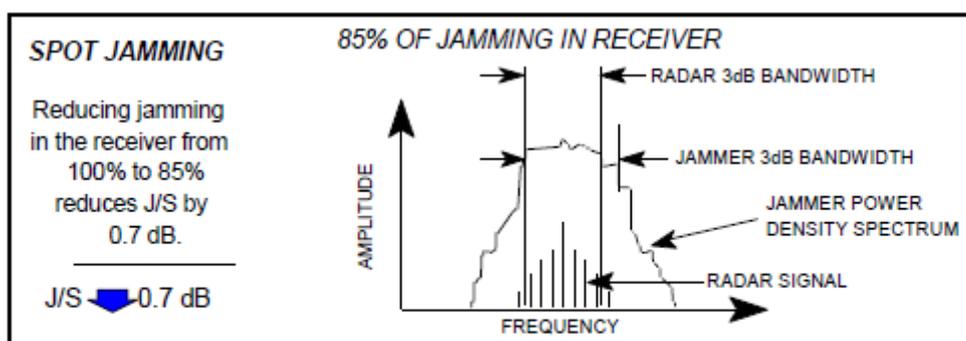
into two general types: (1) noise jamming and (2) deceptive jamming.

## Noise Jamming



Noise jamming is the form of electronic countermeasure where jammer transmit an interference signal (white noise) in enemy's radar direction so that the aircraft reflection is completely submerged by interference. This type of jamming is also called 'denial jamming' or 'obscuration jamming'. The primary advantage of noise jamming is that only minimal details about the enemy equipment need be known. Within the general class of noise jamming, there are three different techniques for generating noise-like signal.

### Spot Jamming:



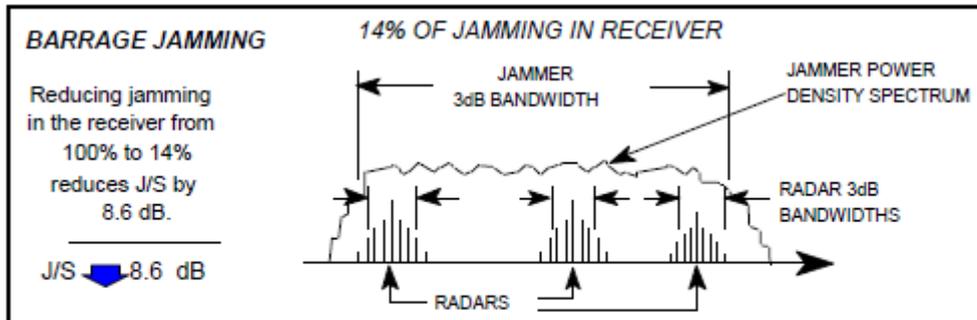
Spot Jamming.

In this type of jamming, also called "point jamming" or "narrow-band jamming", all the power output of the jammer is concentrated in a very narrow bandwidth, ideally identical to that of the radar. Spot jamming is usually directed against a specific radar and requires a panoramic receiver to match the jamming signal to the radar signal.

### ***Counter-countermeasures:***

- Because the jammer can only jam one frequency, a frequency agile radar would hardly be affected. Hence, frequency hopping (radar change operating frequency randomly) is the usual method to deal with spot jamming
- HoJ missiles

### **Barrage Jamming:**



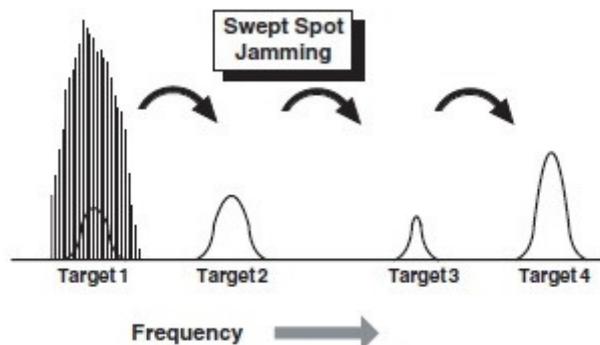
**Barrage Jamming.**

In this type of jamming, all the power output of the jammer is spread over a bandwidth much wider than that of the radar signal. In other words, it involves the massive and simultaneous jamming of the whole of the frequency band.

### ***Counter-countermeasures:***

- Barrage jammers have to spread energy over a wide frequency spectrum, so it is less effective against high power radar.
- Increase radar duty cycles (duty cycle is the time transmitter runs for one out of 100 microseconds, higher duty cycles increase range), higher duty cycles reduce jammer effectiveness
- High gain radar (gain describes how well the antenna converts input power into radio waves headed in a specified direction, higher gain means radar beam is narrower and it converts more percentages of its energy in specific direction)
- HoJ missiles

### **Sweep Jamming:**



This is also similar to barrage jamming. In this case, the power output of the jammer (jammer frequency) is swept back and forth over a very wide bandwidth, sometimes as much as an octave (a 2:1 band). It is generally true that the bandwidth of sweep jamming is wider than that of the barrage jamming, but the relative bandwidth is often determined by the hardware used. The actual difference between barrage

and sweep jamming lies in the modulation techniques and size of the frequency band covered. Barrage jamming often uses an amplitude-modulated signal covering a 10 percent frequency band (i.e., bandwidth equal to 10 percent of the central frequency). Sweep jamming often uses a frequency modulated signal and the frequency is swept back and forth over a wide frequency bandwidth. Both barrage and sweep jamming are used when the exact frequency of the enemy system is not known.

***Counter-countermeasures:***

- Frequency hopping
- High gain , high power radars
- Increase duty cycles
- HoJ missiles

## **Deception Jamming**

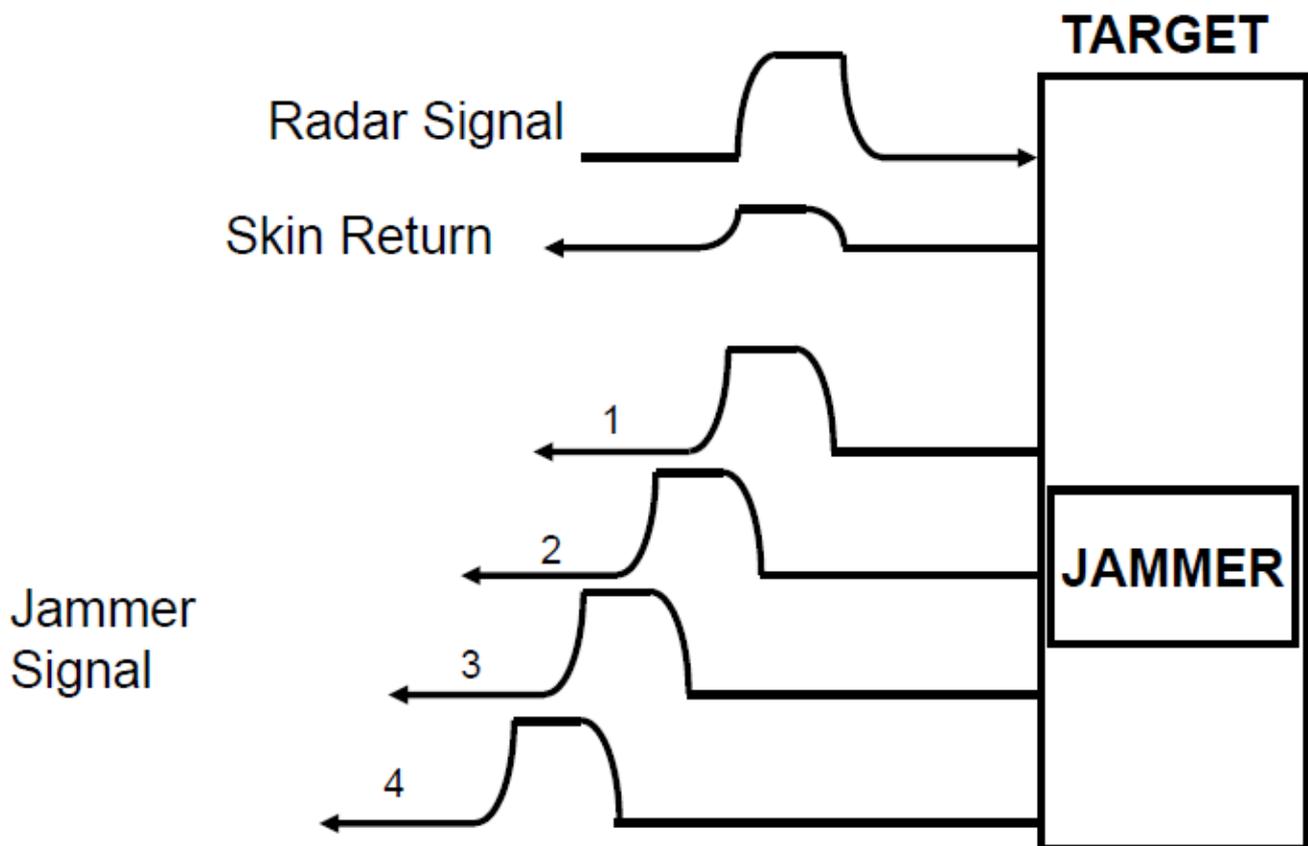
Deception jammers carry receiving devices on board in order to analyze the radar transmission, and then send back false target-like signals in order to confuse the radar..This is in contrast to noise type of jamming,whose objective is to obscure the real signal by injecting a suitable level of noise-like interference into the victim system.Techniques like “noise jamming” are useful for taking a radar installation out of commission, but more sophisticated deception jamming can make the enemy think their radar is still working when it is actually reporting incorrect target range and velocity information With deception jamming, an exact knowledge of not only the enemy radar’s frequency, but all other transmission parameters is required. Deceptive jamming, in a way , is spot or point jamming of a more intelligent nature, HoJ mode of missiles are often less effective again deception jamming because missiles often do not know they are being jammed ( It important to note that , if jamming is detected then HoJ can still be used ).

In recent years capability of radar deceptive jamming has been enhanced significantly with the development of Digital Radio Frequency Memory (DRFM) techniques .Jammers with DRFM technology are widely reported in literature , for example ALQ-187(v)2 , ALQ-131 EA PUP , Falcon edge , ALQ-211(V)9 , ALQ-214(V)3 , Spectra , ASQ-239.DRFM is a technology in which a high-speed sampling digital memory is used for storage and recreation of radio frequency signals.The most significant aspect of DRFM is that as a digital “duplicate” of the received signal, it is coherent with the source of the received signal. As opposed to analog ‘memory loops’, there is no signal degradation caused by continuously cycling the energy through a front-end amplifier which allows for greater range errors for reactive jamming and allows for predictive jamming.

Within the general class of deceptive jamming, there are also a few different techniques:

### **Range Deception**

# RANGE GATE PULL-OFF



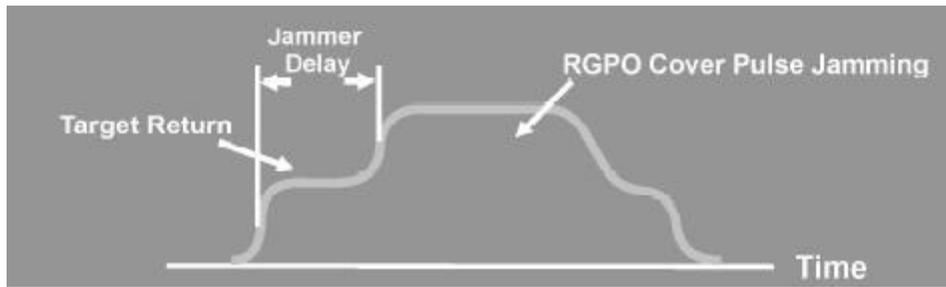
The most common type of deception jammer is the range deception (range-gate stealer), whose function is to pull the radar tracking gate from the target position through the introduction of a false target into the radar's range-tracking circuits. At start, the jammer sends back an amplified version of the signal received from the radar. The deception jammer signal, being stronger than the radar's return signal, captures the range-tracking circuits. The deception signal is then progressively delayed in the jammer by using an RF memory, thereby "walking" the range gate off the actual target (range-gate pull-off or RGPO). When the range gate is sufficiently removed from the actual target, the deception jammer is turned off, forcing the tracking radar into a target reacquisition mode.

p/s: jammer can sometimes perform Range gate pull in , which is the similar technique as Range gate pull off , the main different is the target will appear to get closer to radar instead of getting further away

## Counter-countermeasures:

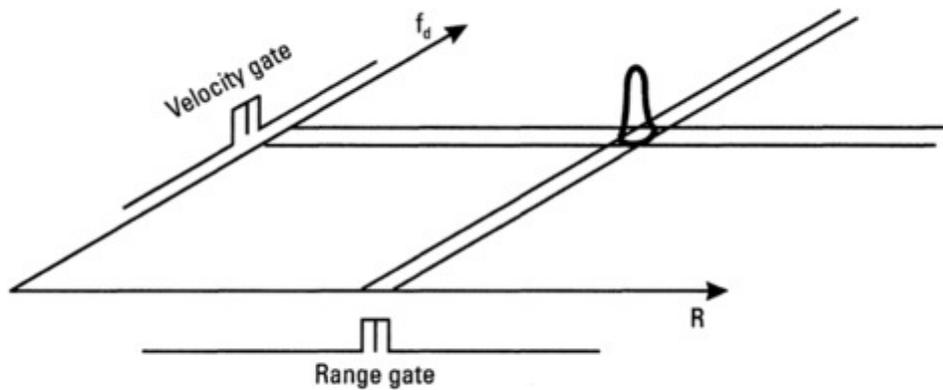
- PRF jitters : a radar calculate range to a target by measuring the elapsed time between pulse transmittal and target return reception. Thus, the maximum required range of the radar determines the maximum pulse repetition frequency of the radar .In Jitter mode, the time between successive pulses is allowed to vary in a totally random manner over a series of set intervals as long as the maximum range condition is met. In theory, an infinite number of PRI patterns can be generated by combining stagger and jitter. Varying pulses render the jammer incapable of anticipating when the next illuminating pulse is due to arrive.
- Frequency-hopping : as the jammer need time to analyze signals and turn into it.
- Leading-edge tracking : taking measurements not according to where the center of the return signal is but rather at the leading edge. All RGPO/RGPI cover pulse jamming tends to lag the target's

returns by some increment of time



○ Monitoring signal strength.

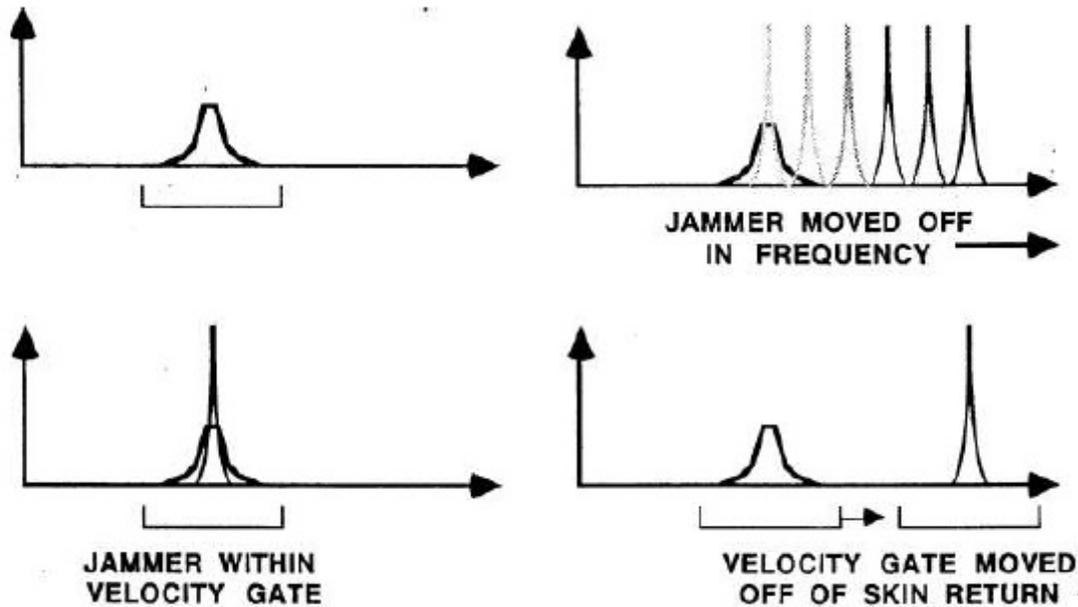
○ D  
on both the range and velocity axes. In this way the target produces an echo that, being characterized in both range and velocity (Doppler) allows double tracking. If the jammer attempts to open a one gate not coherent with the other, it is ignored



Sophisticated radars can exploit double tracking in range and velocity.

### Velocity Deception

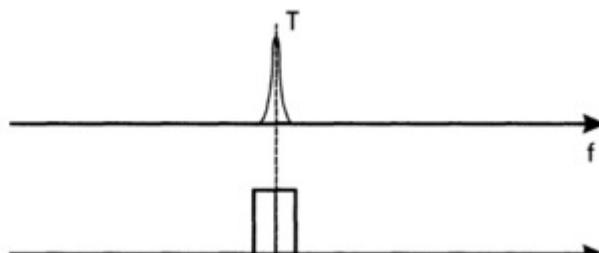
# Velocity Gate Pull-off

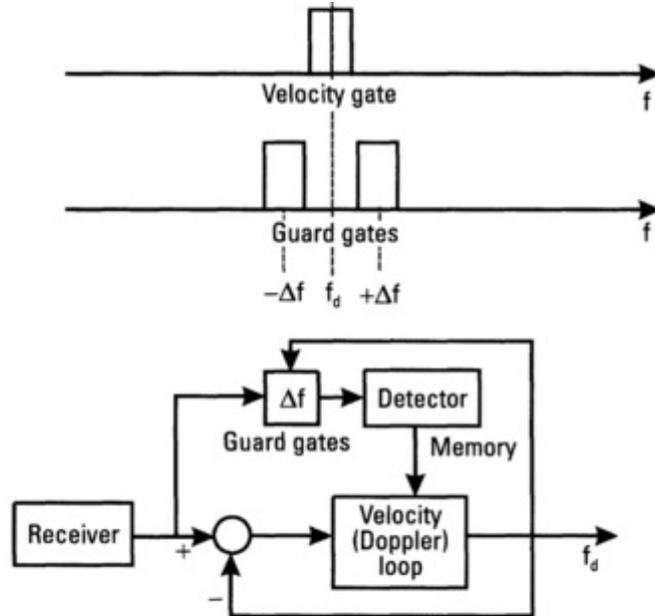


In velocity deception jamming, the Doppler shift is interfered with. At the start of jammer operation, the illuminator signal is detected by the jammer and an exact false, strong Doppler-shifted signal is sent back to the radar. The radar locks on to the incorrect Doppler signal and the jammer slowly sweeps the false signal's frequency more away from the actual Doppler frequency of the target. When the radar has been led far enough away in frequency, the jammer is turned off and the radar is once more left without a target. The basic principal of velocity deception is similar to range deception, thus it is sometimes called Velocity Gate Pull-Off ( VGPO )

## Counter-countermeasures:

- PRF jitters
- Frequency hopping
- Leading-edge tracking
- Double tracking
- Guard gate: a counter techniques that entail presenting sensors around the gate in which tracking is performed so that as soon as the presence of additional echo is detected ,the tracking system switches to memory for a short time and then reacquires the old target .Accordingly , when a deception jammer tries to lure the tracking gate to a false target , as soon as the true echo and the deceptive echo separate , the true echo will enter the guard gate, thus blocking the tracking gate. When the sensors indicate that the deceptive echo has gone, the gates will again position themselves correctly .

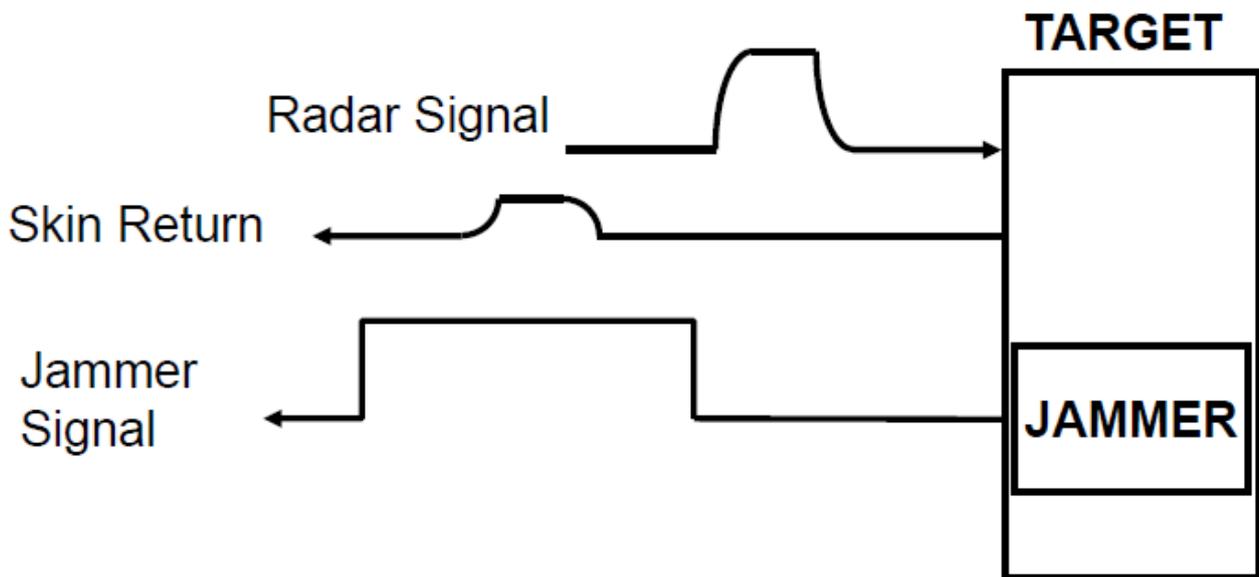




Guard-gates ECCM.

Cover Pulses

# COVER PULSES



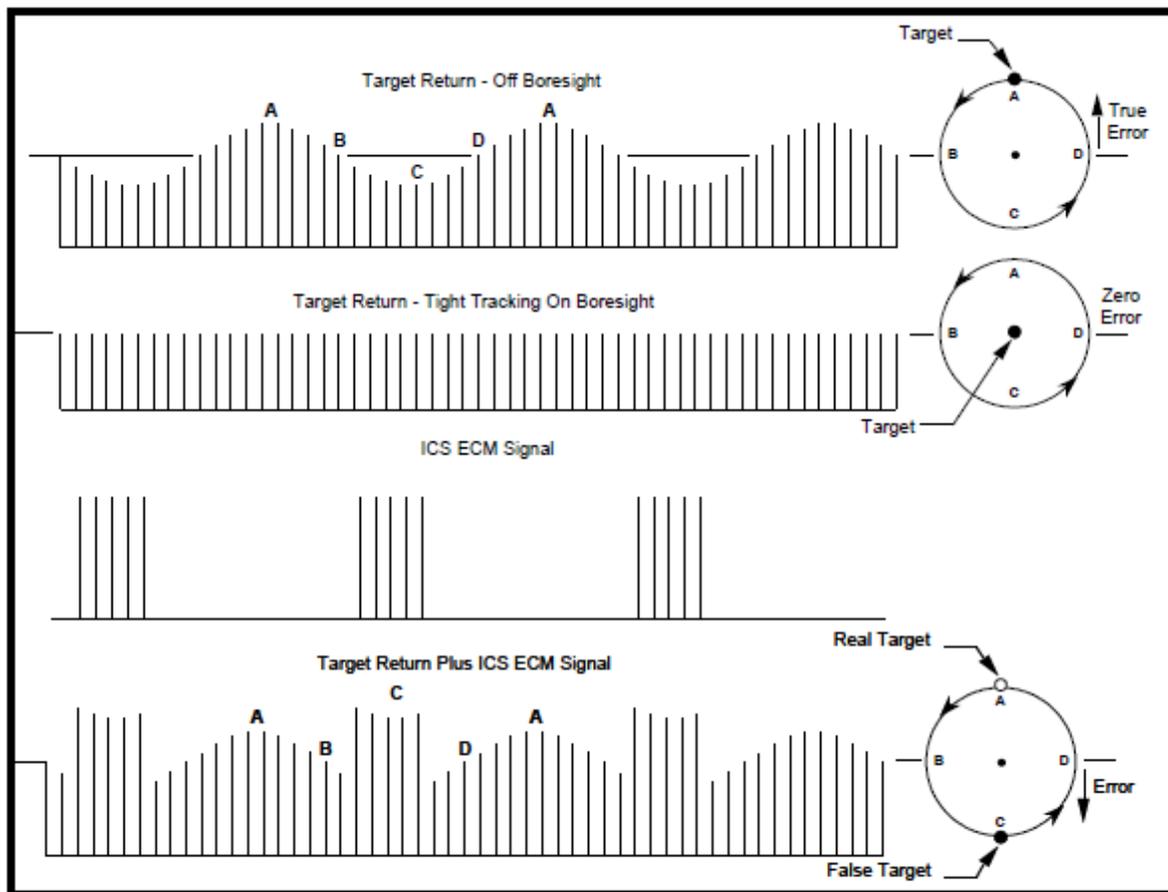
## Denies Radar Range Information

This is a hybrid type of jamming which incorporates some of the features of both spot or barrage noise and deception jammers. . This type of jammer generates a noise burst which is 'on' before and after the actual target return thereby covering the true return. This type of jammer allows a low powered repeater to respond to a number of threat radars by time sharing.

*Counter-countermeasures:*

- High gain , high power radar to burn through jamming signal
- HoJ missiles

## Inverse Gain (Inverse Con-scan ) Jamming



### Inverse Con Scan

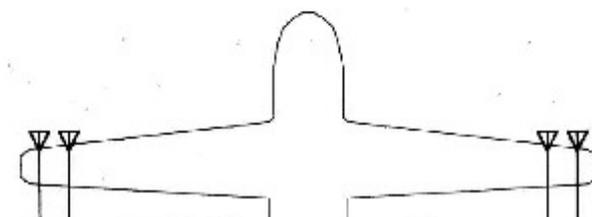
Inverse gain jamming is used to capture the angle-tracking circuits of a conical scan tracking radar. This technique repeats a replica of the received signal with an induced amplitude modulation which is the inverse of the victim radar's combined transmitting and receiving antenna scan patterns. Against a conically scanning tracking radar, an inverse gain repeater jammer has the effect of causing positive feedback, which pushes the tracking radar antenna away from the target rather than toward the target. Inverse-gain jamming and RGPO are combined in many cases to counter conical scan tracking radars.

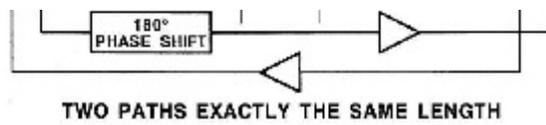
#### *Counter-countermeasures:*

- Monopulse radar
- Random conical scan frequency : changing the scanning speed in a pseudorandom way within a given domain
- Lobe on receive only (LORO )
- Conical Scan on Receive Only ( COSRO)
- Frequency hopping
- PRF jitters

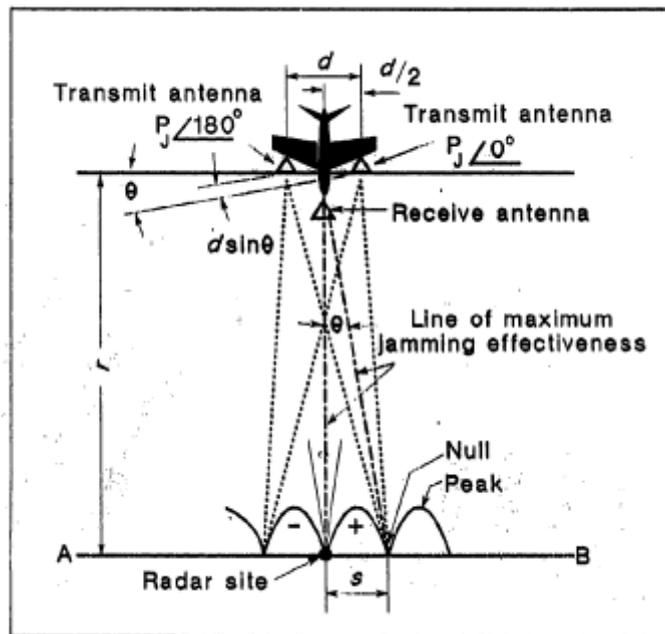
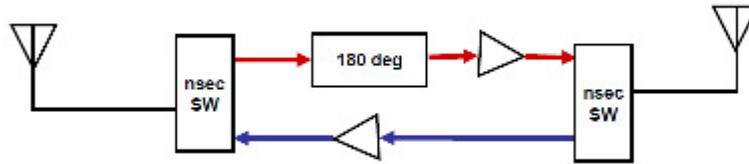
## Cross Eye Jamming

### Cross Eye Jamming





## Cross Eye Implementation



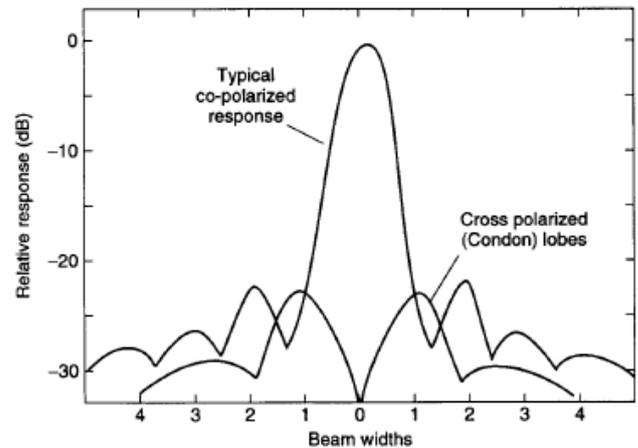
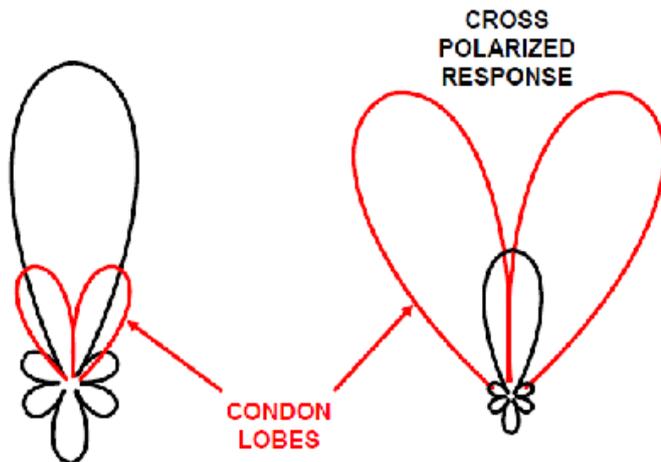
▪ Cross-eye concept applied to a radar.

Cross-eye jamming is an angle deception ECM technique that employs two spatially separated jamming sources. Each source acts as a repeater-type jammer transmitting the same signal at the same time, and if the two signals arrive at the missile monopulse antenna approximately  $180^\circ$  out of phase, wavefront distortion occurs. The missile seeker, presuming that the signal source lies along the normal to the wavefront, tries to re-aligns its antenna at right angles to the distorted wavefront. This antenna re-alignment results in incorrect missile tracking which in turn results in incorrect steering information being passed to the missile autopilot. This may potentially result in a substantial missile miss distance. In a cross-eye jamming system, a  $180^\circ$  phase relationship between the two jamming sources may be maintained by setting up a retro-reflective transmission system. In this type of system, each of the jamming antennas is acting as the signal source for a repeater-type jammer. However, the signal received by one antenna is transmitted by the other, and vice versa. In this way, the total propagation delay from seeker to receive antenna to transmit antenna and back to seeker is identical for both signal paths and, everything else being equal, the phase of the two signals arriving at the seeker will be identical. A  $180^\circ$  phase shifter is then added to one of the paths to create the wavefront distortion effect. Successful operation of cross-eye jamming creates an interferometric null between the jamming signals in the direction of the victims radar. The jamming signal must compete with the real target return to capture the radar angle tracker. To achieve that the angle noise caused by the real radar target must perturb the radar's antenna off the jamming signal null by an amount sufficient for a positive jamming to signal ratio to be generated. As a result, the jamming to signal requirement of at least 20dBsm is required for successful cross-eye jamming operation.

### ***Counter-countermeasures:***

- PRF jitters
- Frequency hopping
- High gain , high power radar to burn through jamming signal
- Increase radar duty cycles

### **Cross-Polarized Jamming**



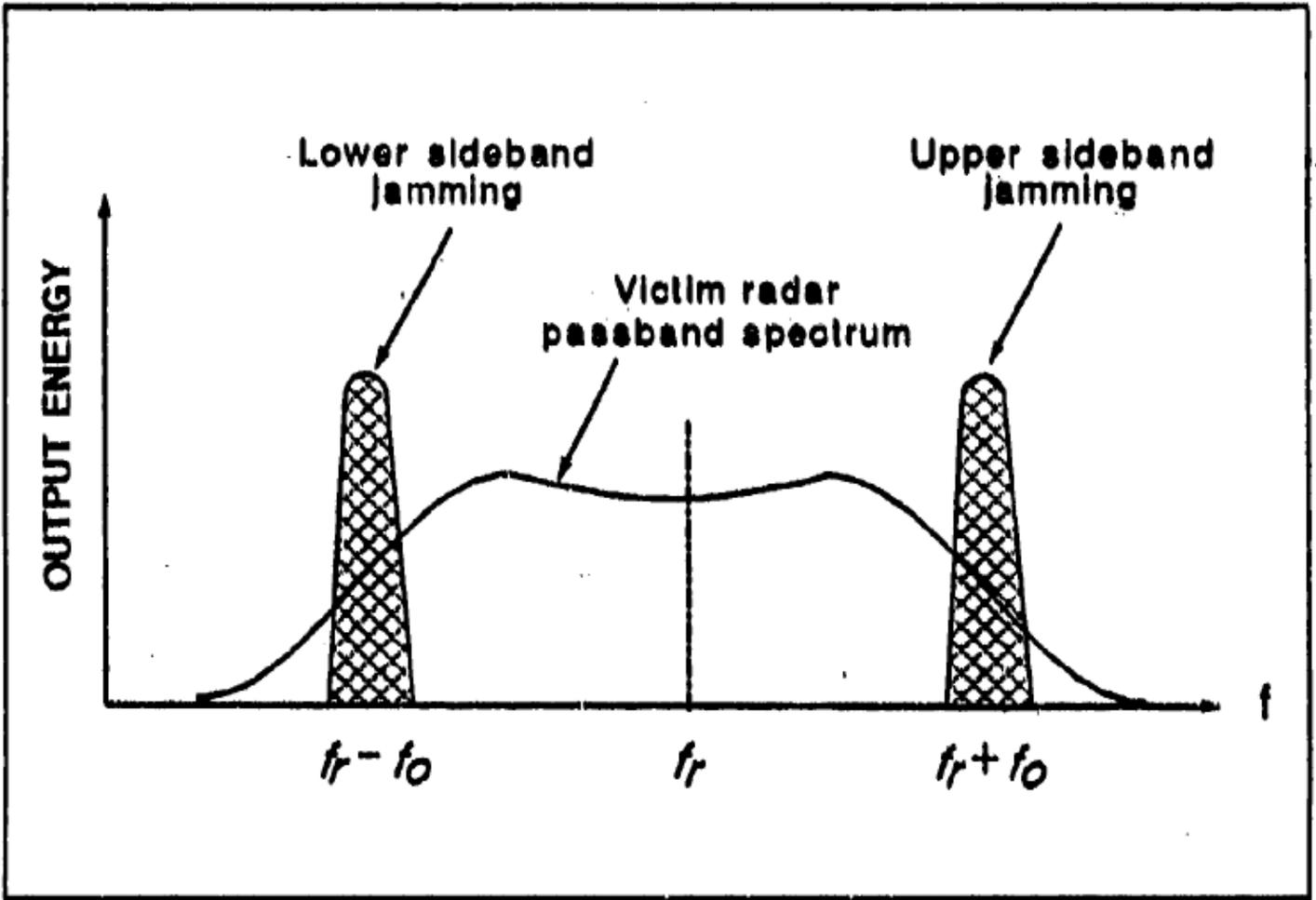
Cross-polarization response of a parabolic antenna.

The polarization of an electromagnetic wave is defined as the orientation of the electric field vector. As we know electric field vector is perpendicular to both the direction of travel and the magnetic field vector. The polarization is described by the geometric figure traced by the electric field vector upon a stationary plane perpendicular to the direction of propagation, as the wave travels through that plane. Reflectors type antenna response to cross-polarized signals very different from normal polarization signals , and cross-polarized jamming exploited that fact. The jammer use 2 transmitting antennas which are 90 degrees out of polarization ( for example : one can be vertical and the others horizontal ) , this cause the victims radar to react erroneously with very significant tracking error.

### ***Counter-countermeasures:***

- Polarization filter
- Cross-Polarized jamming cannot affect flat plate antenna (such as AESA , PESA radars) since there is no forward geometry
- Cross-Polarized jamming requires very large J/S to overcome weakness of condon lobes ,thus, high gain , high power radars are possible counter to this kind of jammer.

### **Skirt Jamming**



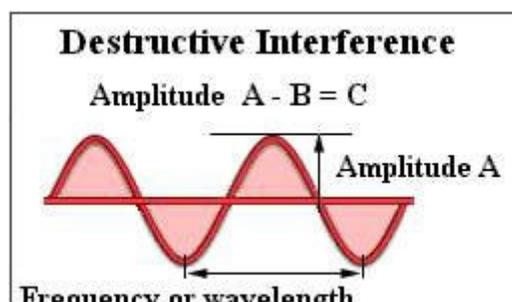
**Waveform of skirt frequency jamming.**

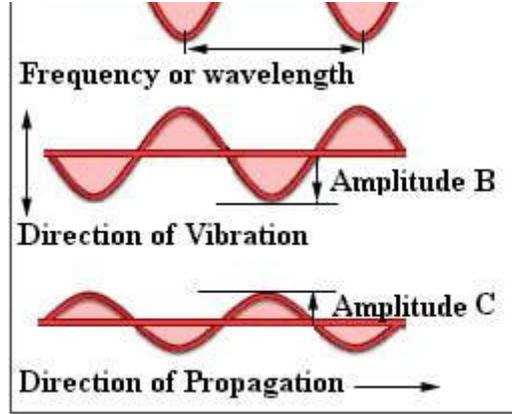
In skirt jamming, the jammer exploits the phase response of filters in the radar receiver by injecting a strong jamming signal into a region just above or below the filter frequency. This can cause non-linearity in the phase response across the wanted band, which can affect the radar's tracking circuitry.

**Counter-countermeasures:**

- Skirt frequency jamming effectiveness, depends on the unbalance between the sum and difference channels, at these frequencies where rapid phase shifts are present in each channel. Thus, it can be counter by careful design and construction of radar.

**Active Cancellation**





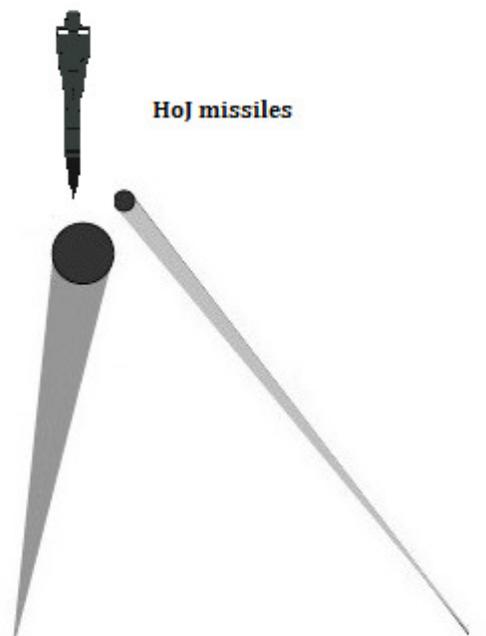
Active cancellation is a theoretical military jamming technique that involves the sampling of an incoming radar signal, analyzing it, then returning the signal slightly out of phase, thus “cancelling” it out due to destructive interference. While there are no official information about jamming systems using this technique in service, it is rumored to be in use on Rafale with SPECTRA suite.

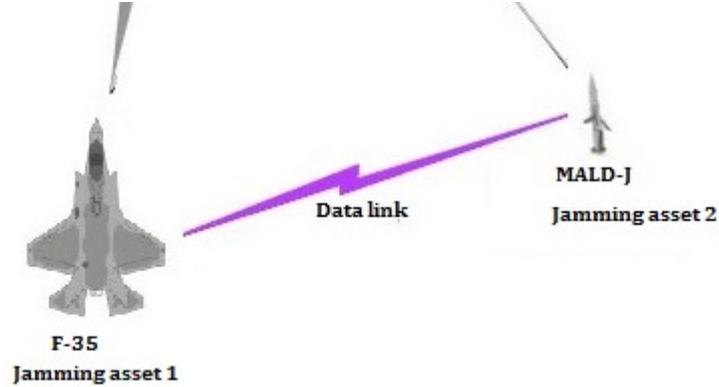
**Counter-countermeasures:**

- Frequency hoping ( active cancellation require exact information about pulses to produce cancellation pulses , thus frequency agile radar are likely unaffected )
- PRF jitters ( cancellation pulses need to be transmitted at exact moment to produce desirable interference effect , random PRF render the jammer unable to predict when the next pulse coming )
- Multiple radars

# Jamming Tactics:

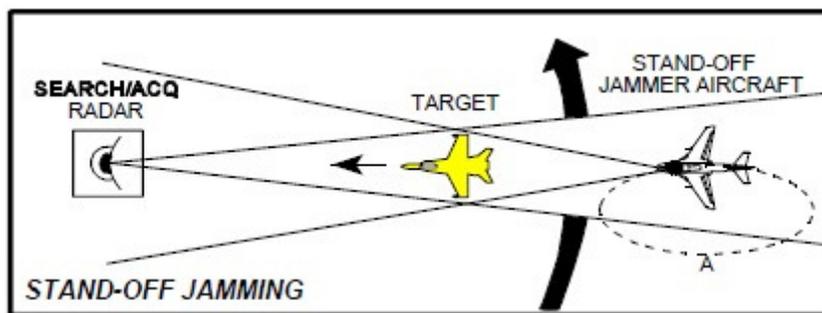
**Blinking Jamming**





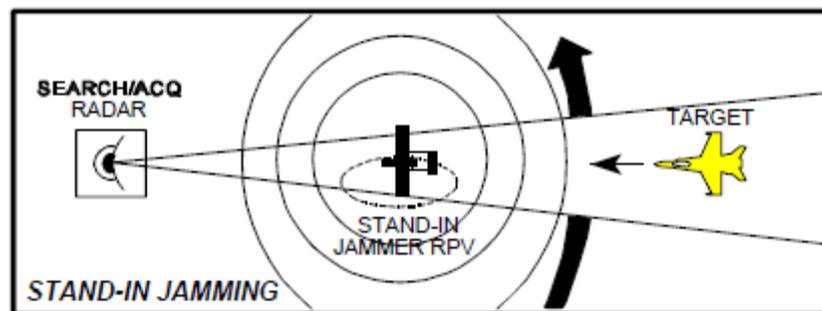
Blinking jamming is an effective jamming tactics against monopulse radar seeker and home on jam missiles. It causes line-of-sight angle to step continuously between the two angular positions through 2 jamming assets emitting by turns. The 2 assets can send returns to hostile radar at the rate close to servo bandwidth( typically a few Hz), this can cause resonate at radar target and result in large overshoot, if apply again HoJ missiles , it would cause missiles to yaw wildly and miss both targets.

**Stand-off Jamming**



Support jamming signal is radiated from one platform and is used to protect other platforms, for stand-off jamming (SOJ) the support jamming platform is maintaining an orbit at a long range from the radar – usually beyond weapons range. The advantage of this method is that jamming platform can be safe from HoJ missiles, the disadvantages is that it much harder to maintain sufficient J/S ratio.

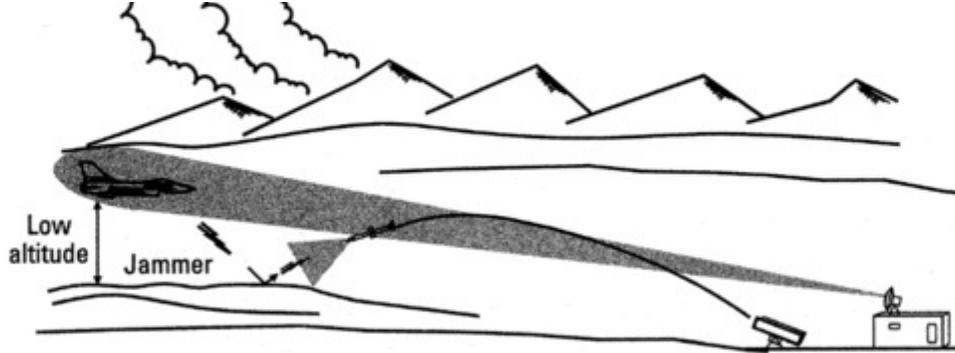
**Stand in Jamming**



Support jamming signal is radiated from one platform and is used to protect other platforms. For stand in jamming (SIJ) a remotely piloted vehicle is orbiting very close to the victim radar while transmitting jamming signal. Since the jammer is closer to hostile radar , the power required to screen the same target of SIJ is much lower compared to SOJ.

**Terrain Bounce Jamming:**



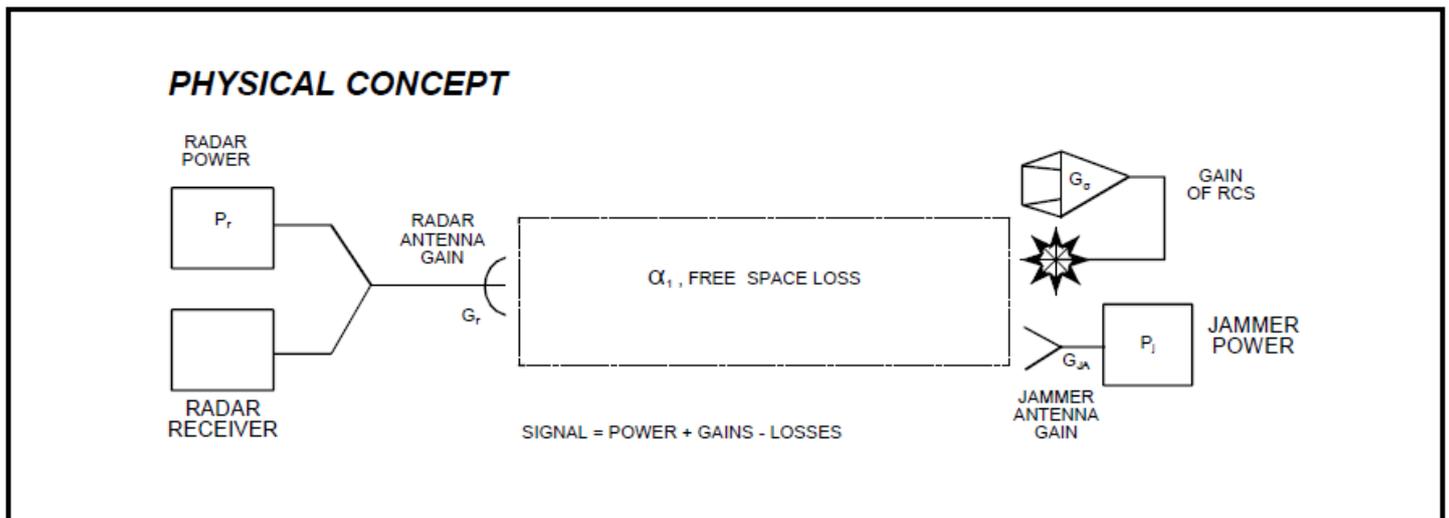


**Terrain-bounce jamming** exploits ground reflectivity to deceive the tracking radar or the seeker of a missile. It can be used in low-altitude flight.

Terrain bounce jamming is a unique jamming tactic created to deal with HoJ missiles. Normally the electromagnetic beam from jammer is transmitted toward the victim radar in a direct path thus, home-on-jam missiles will be able to track the angle (direction) of the jammer signal and fly at that direction. Terrain bounce tactic exploits the fact that ground/sea surface can reflect radio waves. Jammer operator will direct jamming beam toward these surface instead of directly at the hostile radar so the jamming beam will come from a different direction from the actual jammer. As a result, this tactic can be used to trick HoJ into believing that the jammer is located somewhere on the ground. Terrain bounce tactics work best when aircraft fly at low altitude, near flat surface such as the sea. Main disadvantage of this tactic is that the effective radiated power of the jammer is reduced.

## Jamming-to-Signal Ratio:

When jamming is factored into the radar equation, the quantities of greatest interest are the Jamming to signal ratio (J/S) and Burn-Through Range. "J-to-S" is the ratio of the signal strength of the jamming signal (J) to the signal strength of the target return signal (S). It is expressed as "J/S" and is often measured in dB.



Radar Jamming Visualized

Apart from their unique requirements of each specific jamming technique, for jamming to be effective  $J$  must exceed  $S$  by some amount, therefore, the desired result of a  $J/S$  calculation in dB is a positive number. It is a common misconception that  $J/S$  ratio required to jam any radar is a fixed value. In reality, however, the required  $J/S$  varied significantly depending on jamming techniques and radar type.

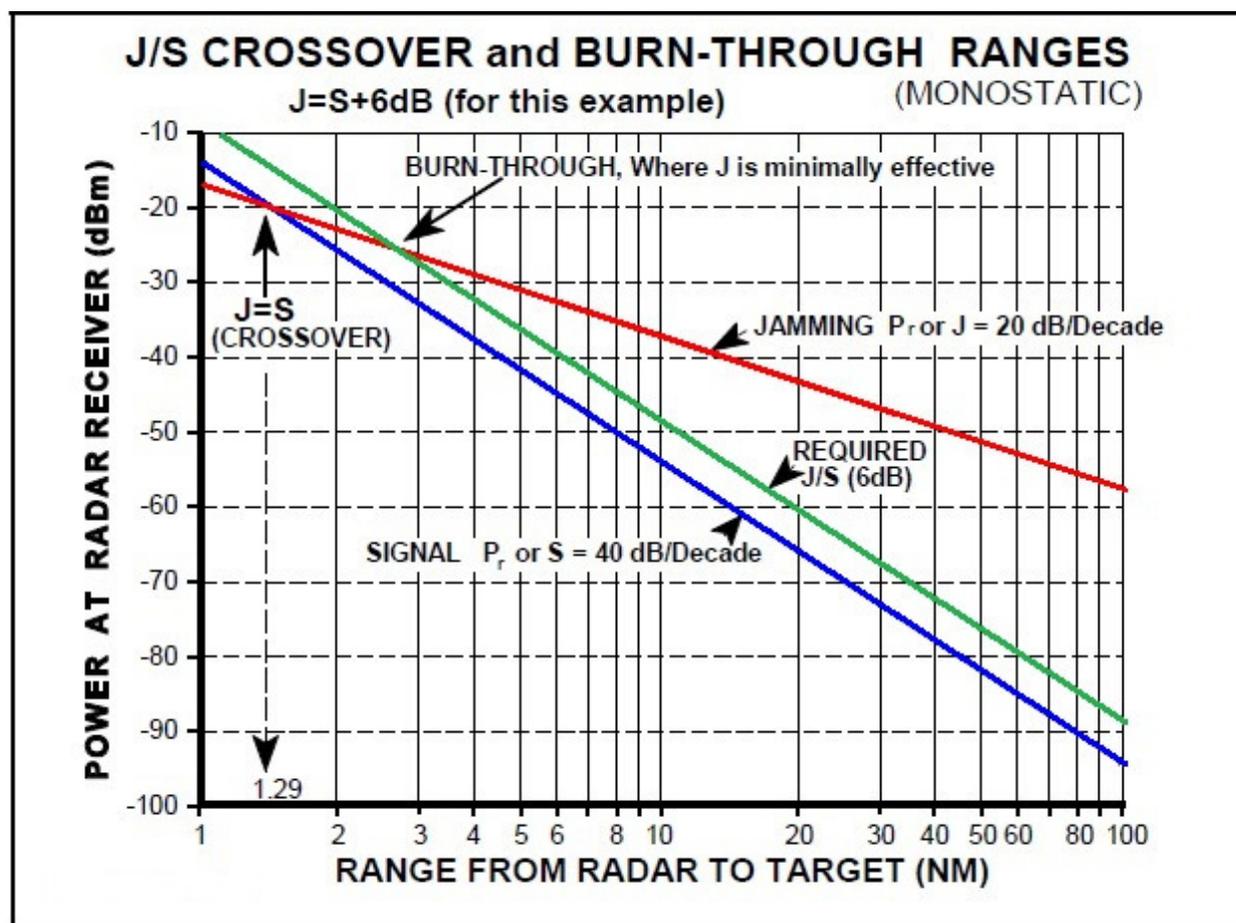
Type of Radar

Type of Jamming

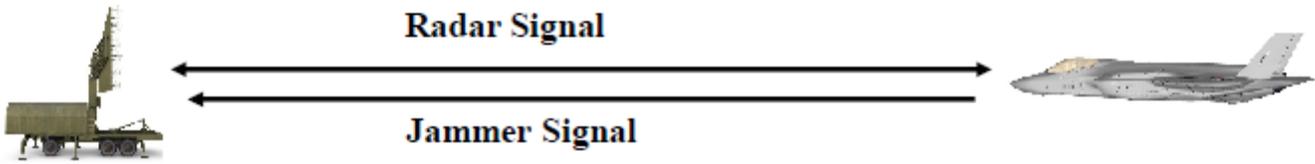
J/S required

Type of Radar	Type of Jamming	J/S required
Pulsed	Noise	0-6 dB
	RGPO	0-6 dB
	RGPI	0 dB
	Cover Pulses	0 dB
Continuous-wave( CW )	VGPO	0-6 dB
CONSCAN or Lobe Switching	Inverse Gain	10-25 dB
Track-while-Scan	Main lobe blanking	10-15 dB
	Inverse Gain	20 dB
COSRO	Sweep-Audio	10-25 dB
Monopulse	Cross-Polarization	20-40 dB
	Cross eye	20 dB
	Blinking	0-3 dB

Burn-through range is the radar to target distance where the target return signal can first be detected through the ECM and is usually slightly farther than crossover range where  $J=S$ . It is usually the range where the  $J/S$  just equals the minimum  $J/S$  requirement.



## SELF PROTECTION JAMMING



Jammer located on target  
Has advantage of Radar Antenna  
Can use either Cover or Deceptive Jamming

$$S = ERP_s + G - 103 - 20 \text{ Log } F - 40 \text{ Log } R + 10 \text{ Log } RCS$$

$$J = ERP_j + G - 32 - 20 \text{ Log } F - 20 \text{ Log } R$$

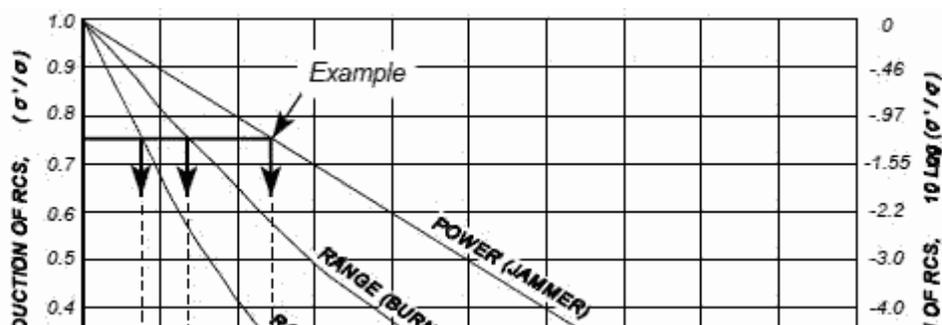
Note that distances are the same and both jammer & radar return are received with antenna gain  $G$

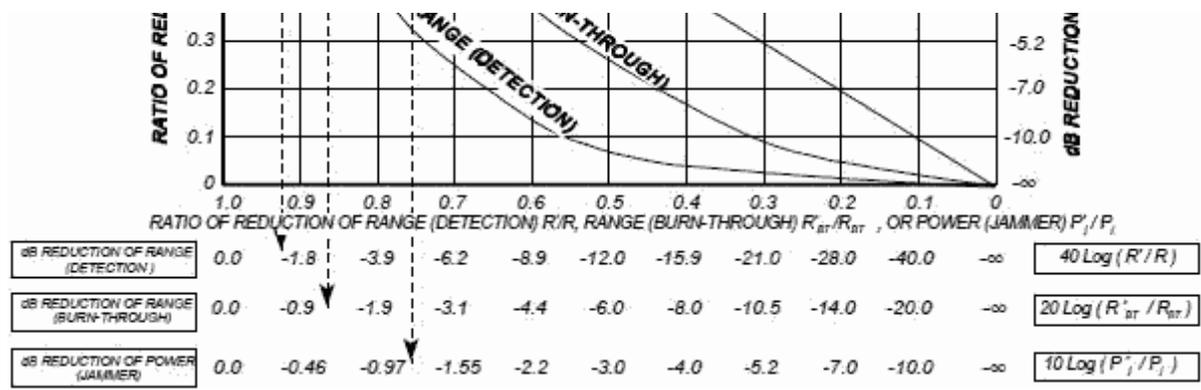
$$J/S = ERP_j - ERP_s + 71 + 20 \text{ Log } R - 10 \text{ Log } RCS$$

As shown in  $J/S$  equation above, factors affecting burn-through range are :

- $ERP_s$  = Effective radiated power of radar
- $ERP_j$  = Effective radiated power of jammer
- $G$  = Antenna gain (<https://basicsaboutaerodynamicsandavionics.wordpress.com/2016/02/24/radar-electronic-countermeasure/>)
- $RCS$  (<https://basicsaboutaerodynamicsandavionics.wordpress.com/2016/03/04/stealth-techniques-and-benefits/>) = Target radar cross section
- $R$  = distance to radar

The relation between radar , jammer power and jamming effectiveness is well known and easily to understand for most enthusiasts. However, one factor that often be overlooked when talking about jamming is radar cross section ( RCS ) of target.

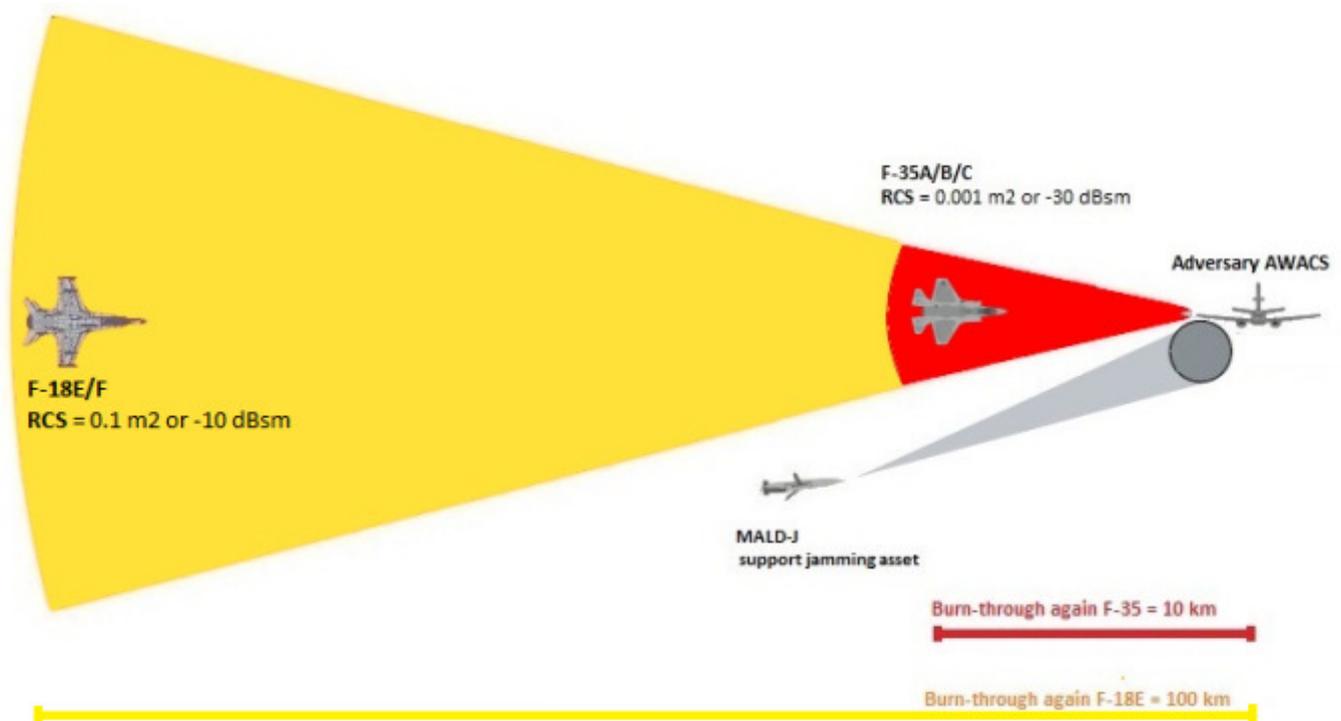




From radar equation, we can see that the power requirement for jamming will decrease directly proportional to RCS reduction, if the RCS of an aircraft is reduced to 0.1 (or 1%) of its original value, then consequently the jammer power required to achieve the same effectiveness would be 0.1 (or 1%) of the original value.

For example, a clean Rafale has radar cross section around 0.1 m<sup>2</sup> (-10 dBsm), an F-35 has radar cross section around 0.001 m<sup>2</sup> (-30 dBsm), so the RCS value is decreased by 99%. Thus, if Rafale needs a 100 kW jammer to deceive or overwhelm adversary radar, then a F-35 in the same situation, wanting to do the same thing will need a jammer with transmitting power of merely 1 kW.

Alternatively, if jamming power is kept constant and RCS changed then from the radar equation, we can see that the burn through distance will be reduced dramatically.



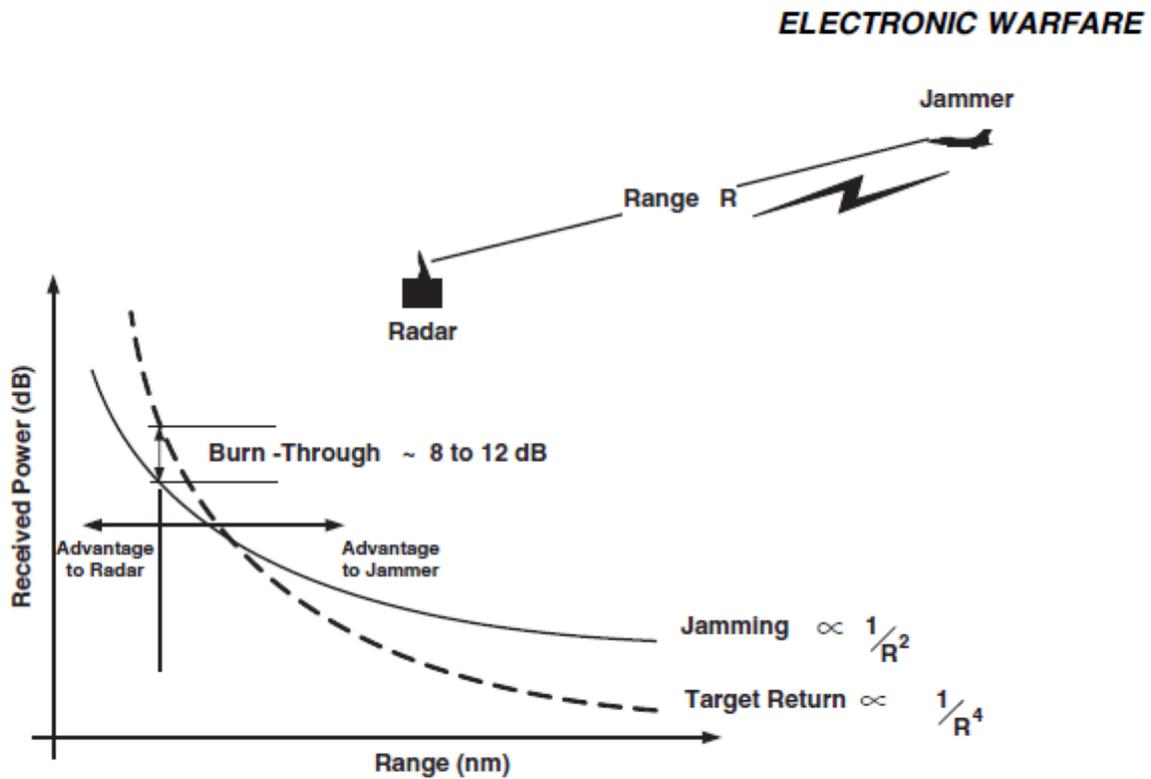
Range (radar burn-through): The crossover equation has:

$$R_{BT}^2 = \frac{P_t G_t \sigma}{P_j G_j A \pi} \quad \text{Therefore, } R_{BT}^2 \text{ is proportional to RCS } (\sigma) \text{ or } \sigma^{1/2} \text{ is proportional to } R_{BT}$$

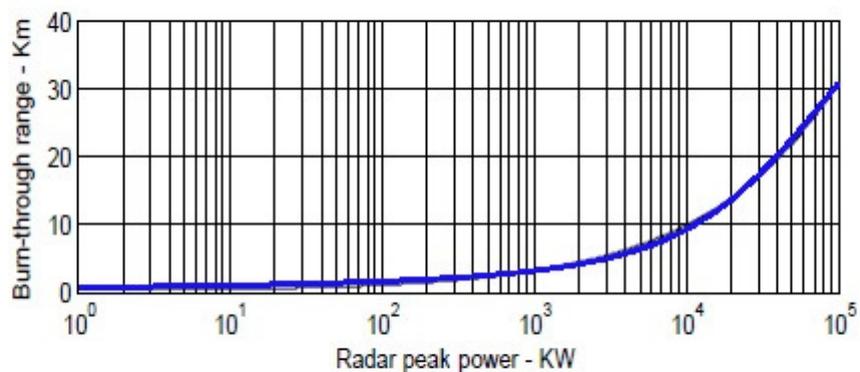
From radar equation, it is easy to see the exponential relationship between RCS ( $\sigma$ ) and radar burn-through range. For example: If RCS of aircraft is reduced by 99% and jamming power is held the same then radar burn-through range will be reduced by 90%.

Another factor that is often ignored when discussing jamming effectiveness is distance. Since jamming signal only has to travel one way, as the distance gets bigger, the jammer has more advantage than the

radar because jamming signal decrease at slower rate than aircraft reflection. In the other words : for self-protection jamming the further the jammer is from the threat radar, the easier it would be for that jammer to jam the threat radar .



Effect of burnthrough.



Jammer Peak Power and Radar Peak Power to Cross Over Range

By contrast ,for support jamming the closer the jammer to threat radar , the easier it would be for the jammer to cover others assets because in this case aircraft reflection is not depend on the distance between the jammer and the threat radar so getting the jammer closer to the radar is better.

## References:

- Kwon,Ki Hoon(September 1989)*OPTIMIZING ECM TECHNIQUES AGAINST MONOPULSE ACQUISITION AND TRACKING RADARS*
- Avionics Department (October 2013 )*Electronic Warfare and Radar Systems Engineering Handbook*
- Filippo Neri and EW-101 *Introduction to Electronic Defense Systems*
- Van Nostrand Reinhold (1987) *Principles of Modern Radar*
- Adrian Graham (2011) *Communications, Radar and Electronic Warfare*
- James N. Constant (1981) *Fundamentals of Strategic Weapons: Offense and Defense Systems*
- Warren du Plessis (26 August 2009)*Practical Cross-Eye Jamming*
- Zhang Yan ,ZHAI Zhen-gang ,LI Ping (2009) *The Analysis on Angle Noise Produced by Blinking Jamming*
- Dr. T.W. Tucker ,Bill Vidger (2009) *Cross-Eye Jamming Effectiveness*
- Dave Adamy (2012) *Overview of Modern Radar Electronic Protection*
- James D. Townsend, Michael A. Saville, Seng M. Hongy, Richard K. Martin (2008) *Simulator for Velocity Gate Pull-Off Electronic Countermeasure Techniques*
- C. Schleher, *Electronic Warfare in the Information Age*. 685 CantonStreet, Norwood, MA 02062: Artech House, 1999
- National Air Intelligence Center, ( Beijing, China, 1995) *Design of Phase Quantization Digital Radio Frequency Memories*
- Watson, Charles,( M.S. thesis, Naval Postgraduate School, Monterey, CA, 1996.)*A Comparison of DDS and DRFM Techniques in the Generation of "Smart Noise" Jamming Waveforms"*
- J. Ward, ( MIT Lincoln Laboratory, Lexington, MA, Tech. Rep. 1015, December 1994)*Space-Time Adaptive Processing for Airborne Radar*
- Sun Guoying; Li Yunjie; Gao Meiguo, (2009); *An Improved DRFM System Based on Digital Channelized Receiver, Image and Signal Processing*,. CISP '09. 2nd International Congress on , vol., no., pp.1-5, 17-19 Oct. 2009
- J. Townsend, ( March 2008.) *Improvement of ECM Techniques Through Implementation of a Genetic Algorithm* MS Thesis, AFIT/GE/ENG/08-34. School of Electrical and Computer Engineering, Air Force Institute of Technology (AU), Wright-Patterson AFB OH
- Herley, 6-18 GHz DRFM Subsystem Specification Sheet. Nov. 1999. [Online]. Available: <http://www.herley.com/pdfs/drfm.pdf> (<http://www.herley.com/pdfs/drfm.pdf>). [Accessed: Jan. 25, 2016].
- Kor Electronics, Wideband Digital RF Memory. Jan. 2012. [Online]. Available:<http://www.rhombustechologies.com.au/10bit%20Insert%20FINAL.pdf> (<http://www.rhombustechologies.com.au/10bit%20Insert%20FINAL.pdf>). [Accessed: Jan. 22, 2016].
- Mohinder Singh (1988) *Electronic Warfare*.

- Gian Luca Onnis ,Have you ever seen a picture of a fighter plane towing a radar decoy? Here it is [Online] .Available: <http://theaviationist.com/2012/04/16/towed-decoy/> [Accessed: March. 22, 2016].
- Budget Line Item Justification: PB 2017 Air Force
- J. Michael Madewell *Electronic Countermeasures*
- Carey, D., and Evans, W.,(May 1987) *The Patriot Radar in Tactical Air Defense*, Microwave Journal, Vol. 31, pp. 325–332.
- Wiley, R., *ELINT: The Interception of Radar Signals*, Norwood, MA: Artech House, 1985.
- Macfadzean ( 1992) *Surface-Based Air Defense System Analysis*, Norwood, MA: Artech House
- Xiao Tian (2012) *Radar Deceptive Jamming Detection Based on Goodness-of-fit Testing*

About these ads  
(<https://en.support.wordpress.com/about-these-ads/>)

## 2 thoughts on “Electronic Countermeasure (ECM)”

Pingback: [Radar Fundamentals \(Part I\) – Aircraft 101](#)

Pingback: [Radar Fundamentals \(Part II \) – Aircraft 101](#)

[Blog at WordPress.com.](#)