# ROYAL SCHOOL OF ARTILLERY

*BASIC SCIENCE & TECHNOLOGY SECTION*

## Principles of Electronic Counter Measures and Electronic Protection Measures in Radar Systems

### INTRODUCTION

At the end of 1940, the Germans were using radar, at a frequency of around 36 MHz, to detect and direct attacks on British shipping in the Straits of Dover. The British could detect their transmissions using a simple receiver. By mid-February of 1941, British scientists had designed and built a radar jammer and used it, successfully, against the German radar. Since then, the battle between radar designers and jammers has continued unabated.

The aim of the jammer is to produce Electronic Counter Measures (ECM) that degrade the performance of a radar. Meanwhile, the radar designer includes anti-jamming features, called Electronic Protection Measures (EPM), in the radar system with the intention of combating the enemy's use of ECM. ECM can also be called 'Electronic Attack' (EA).

This handout aims to describe the various techniques used for ECM and EPM in the context of Air Defence Radars, such as Rapier.

### RULE ONE OF JAMMING

The most basic concept of jamming is that you jam the *receiver* - not the transmitter. To be effective, the jammer must get his signal into the victim's radar receiver – through the antenna, input filters and processing system.

A radar transmitter might operate with power levels of thousands of Watts and illuminate a large volume within a radius of tens of km around the radar. Its associated receiver might operate with echoes much less than one millionth of a Watt (μW) and is at one single location in space. A jammer, operating at a sensible range of at least a few km from the radar, has only one practicable solution – to jam the receiver.

### TYPES OF COUNTER MEASURE

There area a number of different types of signal that can be used to jam a radar receiver or to mask a target. The general categories are:

- **Noise Jamming**: tries to make the radar receive a (random) signal that is much greater than the echo so that the echo signal cannot be identified.
- **Deception Jamming**: tries to make the radar receive a false signal (or signals) that causes the radar to indicate an incorrect range or angle to the target. Might also cause the radar to indicate multiple false targets.
- **Decoys**: tries to make the radar receive a strong signal that resembles the type of target for which it is searching. The decoy tries to look and behave more like a target than the real thing. Chaff is the traditional decoy but UAVs are more effective (and more expensive).
- **Stealth**: not a form of jamming, but a counter measure. A stealthy target is designed to produce the minimum echo signal at the radar receiver, beneath the detection level of the receiver at 'normal' detection ranges.

### JAMMING LOCATION

The jamming signal will normally be carried by an aeroplane that can manœuvrre to the best position for jamming. The three locations for the jamming equipment are:

- **Stand-Off Jamming**: a lot of power and weight is needed for effective jamming so a large aeroplane, positioned out of range of the air defence system, can be used to generate the jamming signal.
- **Self-Screening Jamming**: the attacking aeroplane carries its own jamming equipment. This ensures that the jamming is in the right place but it reduces the effective payload of the aeroplane.
- **Escort Jamming**: the jammer accompanies the aeroplanes that it is trying to hide from the radar. Sometimes called 'Stand-In' jamming.

### PROTECTION MEASURES

All protection measures involve making the radar system, especially the receiver, much more complicated and expensive than it needs to be for 'ordinary' use. Luckily, some of the commonly applied protection measures have the advantage of increasing the performance of the radar system when jamming is not present. Thus, a radar system with comprehensive EPM will usually perform better than an 'ordinary' radar under all circumstances.

The simple types of EPM that could be used by a radar system include:

- **Frequency Agility**: the radar switches to a new frequency (e.g. from 3.05 GHz to 3.07 GHz) in an unpredictable way so that the jammer cannot keep up.
- **PRF Agility**: the radar switches between a number of different pulse-repetition frequencies (e.g. from 10 kHz to 12 kHz) in an unpredictable way.
- **Signal Coding**: the transmitted pulse carries a digital code that is difficult for the jammer to identify and, therefore, to match. A 'chirped' pulse also carries a type of coding.
- **Target Behaviour**: chaff is relatively easy to identify because, although ejected from a fast moving aero-

plane, it quickly slows down and drifts with the wind. Doppler processing can easily distinguish between slow-moving chaff and a fast-moving fighter aeroplane.

## NOISE JAMMING

This type of jamming may also be called 'Cover Jamming' and it aims to conceal the echo by placing another signal into the receiver. By adding a random element (noise) to the jamming signal and by gradually increasing the power, the radar receiver might not even recognise the signal as jamming.

Radar echoes are generally weak – often similar in strength to the natural atmospheric and receiver noise. This natural noise varies from hour to hour and many radar receivers monitor the noise, automatically raising the level at which they recognise a target when the noise increases and reducing it when the noise decreases. If the 'noise' increases gradually, because it is jamming and not really noise, then such receivers will steadily raise their target-detection thresholds until no targets are recognised. A clever radar will monitor the noise levels at each azimuth and be able to recognise when this type of jamming is present.

**Main-Lobe Jamming**: the jammer is capable of receiving the outgoing pulse from the radar. When the jammer receives a high-intensity signal then the radar antenna must be pointing directly at him. Any jamming signal that he transmits will be detected by the radar as having come from the correct azimuth. This is the easiest opportunity to jam as the antenna receives best from this direction. The jamming will span more that one beamwidth (e.g. 2°) of the radar's coverage. This is because the beam does not have a sharp edge and, although it fades away beyond 2°, a strong jamming signal can affect the radar beyond the edge of the nominal beam width.

**Burn-Through**: the equations governing the strength of a signal at any distance are different for jammer and radar because the radar signal covers the distance twice (out and back) whereas the jammer's signal only goes one way. The variation of the signals with range is such that the radar signal is an inverse 'fourth-power' law whereas the jammer's signal is an inverse 'square' law. If we plot a graph showing the strength of the radar echo from any range and a graph showing the strength of the jamming signal from any range than it turns out that the radar echo increases faster than the jamming signal. This means that, for any practical jamming scenario, there is always some range where the echo is visible above the jamming. This range is called the 'Burn-Through' range. A typical graph is shown in Figure One, where the burn-through range is about 3.9 km.

The effect of jamming is to delay the detection of the target, rather than to block it completely. However, if a fast-moving fighter aeroplane were detected at a range of only 3.9 km from an air defence system then there would probably not be sufficient time for it to be engaged.

**Three-Dimensional Radar**: these radars can discriminate between targets at different angles of elevation. Effectively, the radar has multiple receivers – one for each elevation range. A jammer can have only one elevation and, consequently, can jam only one elevation beam, through its main-lobe, at a time.

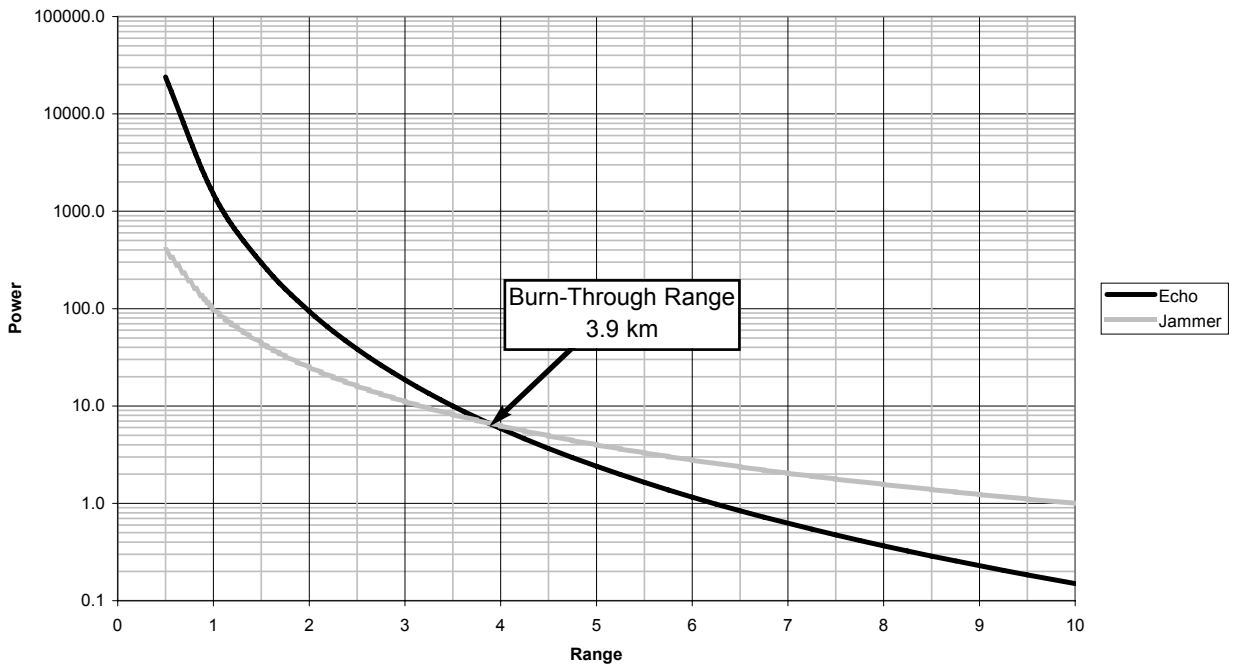



***Figure 1: Variation in the Power at a Radar Receiver with Range to Target and Jammer***

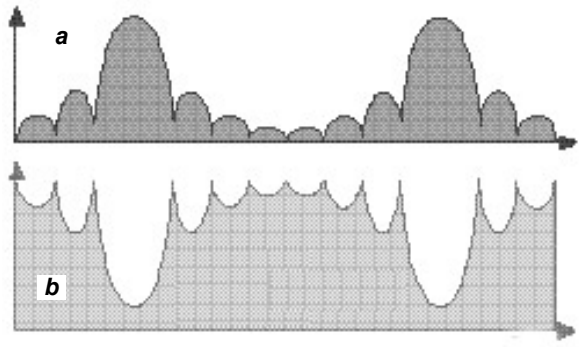



***Figure 2:***
***a: Variation in Signal Strength with Azimuth***
***b: Inverse Gain Characteristic for Jamming***

## SIDE-LOBE JAMMING

A conventional dish antenna might have side-lobes that are only 20 dB down on the main beam, and many other smaller lobes too. A jammer could observe the variation in signal strength from the radar as the antenna rotates – he would observe, over two antenna rotations, variations simular to those of Figure Two, (a), where the large peak is the main-lobe. If he adjusts the strength of his jamming signal in the opposite manner, as indicated in Figure Two, (b), then the receiver noise would be raised equally, at all azimuths, and the radar would be jammed at all azimuths.

Any jamming signals, including deception jamming, that enter the antenna via a side-lobe will appear to the radar as if they had originated in the direction of the main-lobe. Thus, side-lobes allow a jammer to inject signals at false azimuths and to deceive the system. One way of countering this is to design a radar antenna that has very low side-lobes – but this requires precision manufacturing and a phased-array antenna that will be very expensive (e.g. Rapier FSC) and must rotate to scan. Steerable phased-arrays (e.g. Cobra), that do not rotate, but are steered by varying the phase at each element, have inferior side-lobe performance as their individual elements cannot be kept precisely in step – even very small errors in the phasing will produce significant sidelobes.

**Side-lobe Blanking**: if a radar can distinguish between a signal that it receives through a side-lobe and a signal that it receives through the main beam then the jammer will be thwarted. Side-lobe blanking achieves this with the use of a secondary, omni-directional antenna, as follows:

- Since omni-directional antennae have fairly low gains then this antenna will always receive a fairly small signal, say -15 dB below the main beam.
- When any signal enters the radar receiver via the main beam then, because the main-beam has high gain, its signal strength will be much greater than that from the omni-directional antenna. (E.g. Main beam gives 0 dB, omni-directional gives –15 dB.)
- When a jamming signal, directed at a side-lobe enters the receiver then, because side-lobes have a gain around 20 dB less than the main beam, its signal strength will be reduced by 20 dB - and now, the omni-directional antenna will be receiving the stronger signal. (E.g. side-lobe gives –20 dB, omni-directional gives –15 dB.)
- Whenever the signal from the omni-directional antenna is bigger than that from the radar antenna then the receiver is blanked, to eliminate the false targets.
- Any real targets in the main beam will nearly always give a strong signal and will be detected.

Figure Three shows the antennae of the Surveillance Radar of Rapier FSB2 with the Omni-Directional Antenna mounted on the top.

**Coherent Side-Lobe Suppression**: any signal can be eliminated by mixing it with an identical signal that is in anti-phase. An omni-directional antenna can receive a jamming signal and this can be processed to be in anti-phase with the part of the jamming signal that enters via the side-lobe. Mixing the two leaves just the target signal, which is unaffected by the process because it does not enter via the side-lobe. This works because the jammer is on a different azimuth from the target, the difference being equal to the angular difference between the main beam and the side-lobe.

## DECEPTION JAMMING

The purpose of deception jamming is to inject false signals into the radar receiver so that these signals are interpreted as ‘real’ targets. By giving these targets ideal properties, the signal processing circuits in the radar are deceived into treating them as high-priority targets and the perpetrator is ignored by the radar. Examples of the sorts of trickery that a deception jammer might employ are:

- **Repeater Jamming**: the jammer receives the outgoing signal from the radar and, after a short delay, then re-transmits it back to the radar, perhaps at fairly high power to make it seem like an important tar-

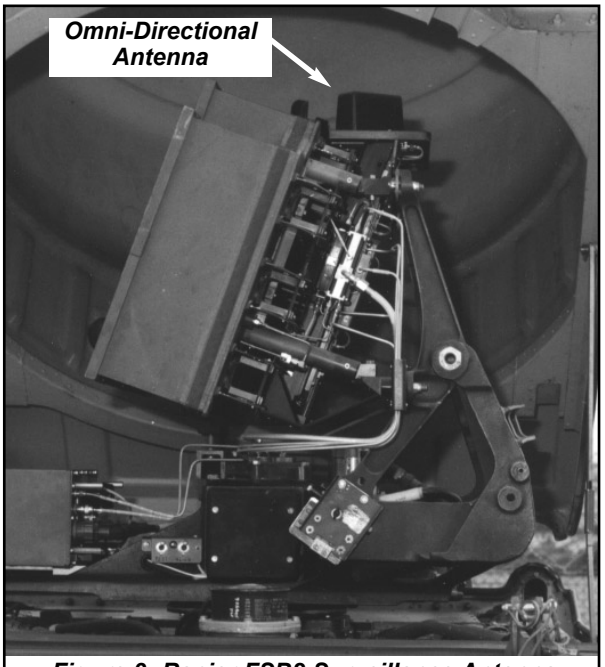



***Figure 3: Rapier FSB2 Surveillance Antenna***

get. This produces false targets with a range greater than the jammer. (E.g. a 10 μs delay in re-transmission would produce a false target 1.5 km beyond the jammer.)
- **Anticipatory Jamming**: the jammer repeats the signal after a much longer delay so that it appears to be an echo from the next radar pulse (a second-trace echo). This causes false targets at ranges less than that of the jammer.

Using the above techniques, either in the main lobe or in a side-lobe, the jammer can place a wide variety of patterns of confusion on the victim's radar.

**Look-Through**: if the jammer needs to monitor the radar's transmissions so that he can re-transmit them for deception then he must normally switch off his jamming at frequent intervals otherwise his outgoing jamming will drown-out the signal from the radar. This is a tricky problem to solve as the radar might be able to operate normally whilst the jamming is momentarily interrupted.

## EPM AGAINST DECEPTION JAMMING

Control of side-lobes allows jamming only in the main beam – so the true azimuth of the jammer can be discovered. The radar can vary its PRF and carrier frequency and this allows it to identify, and reject, second-trace echoes. This removes false targets whose ranges are less than that of the jammer (anticipatory jamming). Then, having eliminated false targets closer than the jammer, the other false targets (repeater jamming) will be at a greater range than the jammer. Therefore, the closest target is real.

## DECOYS

The oldest radar decoy is chaff (called 'window' in WW2). This consists of thousands of small strips of conducting material that are ejected en-masse by the target or nearby aeroplane. Chaff works best when its length is about one-half of the wavelength that the radar is using (e.g. chaff of length 5 cm for a radar of wavelength 10 cm, frequency 3 GHz). Drawbacks of using chaff are that its length must be about right, it moves at the velocity of the wind (not a fighter aeroplane), it falls quickly to Earth and it tends to align vertically as it falls which makes it less effective against horizontally-polarised radars. Chaff is not very expensive, and it continues to be used. It can be quite effective for ships as the chaff drifts in the wind at a similar speed to that of a ship.

**UAV Decoys**: designed to attract the attentions of air defence systems, these small air vehicles carry corner reflectors that give a very strong return and are easy to mistake for much larger aeroplanes. By engaging the decoy, the air defence battery reveals its position and might expend its ready-to-use missiles by the time the real threat arrives.

**Seduction Decoys**: once the radar has detected and, perhaps, locked on to a real target then the target could release a seduction decoy. This decoy is designed to be more like a target than the real thing and the radar locks onto it, instead. Although the radar a would detect that the signal strength had increased when the decoy is deployed, this might not be recognised as being caused by a decoy. Variations in signal strength are common in radar systems, especially for a manœuvring target which presents different aspects (reflecting surfaces, corners, etc.) as it manœuvres.

## DECOY PROTECTION MEASURES

Chaff is relatively easy to distinguish from a fighter aeroplane if the radar is using Doppler Processing. Predictive tracking by the radar can be used to estimate where the target should be on the next radar scan as the known capability of an aeroplane to manœuvrre limits the possibilities. An aeroplane that released chaff as a decoy would be providing the radar with a target that suddenly went from 300 $ms^{-1}$ to 20 $ms^{-1}$ in an impossibly short time. (Chaff tends to slow down and drift in the wind very rapidly because it has low mass and relatively high air resistance.)

UAV and seduction decoys are much more difficult to identify as they are designed to return a signal as strong, if not stronger, than the real thing. They might also be capable of manœuvring in a similar way to the real thing. A decoy could be identified by:

- **engine modulation**: a jet engine has rotating turbine blades and these can produce a characteristic echo (perhaps, with Doppler). A decoy would be unlikely to have the same engine as the real thing.
- **range profiling**: a decoy is usually very small and returns a relatively simple echo. A real target has variations in cross-section along its length so that, for example, an advanced radar could distinguish a sequence of echoes firstly from the nose of the aeroplane, then the engines & wings and, finally, the tail. For an aeroplane of length 30 m this would take 0.2 μs to occur and requires very good range resolution from the radar. It would be very difficult for a decoy of shorter length to duplicate this effect.

## ARM DECOY

When an AD radar detects an incoming Anti-Radiation missile (ARM) then it can stop radiating - but the missile might already have detected the radar and memorised its (approximate) location. The ARM will probably continue in the general direction of the radar and might explode quite close.

It is possible to erect a number of decoy antennae, located several hundred metres from the radar and to ectivate these antennae at the same time as the real radar shuts down. The decoys could be:

- **Active Radiators**: contain a transmitter that matches the real radar. More expensive than passive decoys.
- **Passive Reflectors**: the output of the real radar transmitter could be directed towards the decoy which would reflect the signal. The ARM would then go for the decoy. The reflector could be spring-loaded and return to its operating position for re-use (unless the ARM scores a direct hit).

## LOW PROBABILITY OF INTERCEPT RADARS

To jam the radar, the jammer must know that that the radar is operational and its location. A conventional radar is quite easy to detect from a distance much greater than its own maximum range. A low probability of intercept (LPI) radar transmits signals that are very difficult to detect and, therefore, difficult to jam.

All electrical signals must compete with naturally occurring 'noise'. One of the main features of noise is that its power depends directly on the bandwidth. If the bandwidth is doubled then so is the noise power. For a conventional radar, the bandwidth of the transmitted signal is equal to $^1/_\tau$, where '$\tau$' is the duration of the pulse.

For example, a conventional radar pulse of duration 10 μs has a bandwidth of 100 kHz. Because the receiver bandwidth is narrow then the noise is kept low and the signal is detectable. If an enemy tried to listen for such a pulse using a receiver with a bandwidth of 1 MHz then his receiver would have ten times as much noise yet the signal would not have increased at all.

LPI radars use very wide bandwidths in their transmitted pulses to force the enemy to widen the bandwidth of his receiver as he attempts to detect the radar's signals. Eventually, the noise power in the wide-band receiver exceeds the signal power and reception fails.

The obvious problem is that if the enemy cannot detect our radar signals then how can we detect them? There are two, different solutions to this problem and both require detailed knowledge of the nature of the transmitted signal. The enemy cannot gain this knowledge until he detects the signal and – catch 22 – he cannot detect the signal unless he knows its nature. The radar system, of course, has the key to the signal. It is the same as (in some systems it is the reverse of) the key that was used to encode it before transmission.

**Chirped Transmissions**: during the outgoing pulse, say 10 μs, the carrier frequency of the radar is steadily increased over a range of, say, 10 MHz. This has the effect of widening the bandwidth of the pulse from 100 kHz to 10 MHz (equals the frequency shift during the chirp). The carrier frequency might shift from, say 3.000 GHz to 3.010 GHz, during the 10 μs pulse. If an enemy were listening on a frequency of, say 3.005 GHz with a bandwidth of 100 kHz then he would detect nothing because the signal passes so rapidly through his bandwidth (in 1% of the pulse duration) that it is drowned by the noise which, of course, is present for 100% of the time. Since he does not know when, or indeed if, the pulse is going to arrive then he cannot switch off his receiver at other times.

**Direct-Sequence Spread-Spectrum Transmission**: here, the phase of the carrier signal is reversed at a high rate (the 'chip' rate) according to a pseudo-random binary code. This has the effect of spreading the signal over a bandwidth equal to the chip rate, say 10 MHz, and it can only be recovered by applying the same code in the receiver. In effect, the signal is encrypted and can only be de-crypted using the same key. The enemy interceptor now has a very difficult task of detecting a signal that covers a very wide bandwidth and, without the correct code, is masked by the noise. In fact, the random nature of the key used to encode the signal makes it resemble noise.

## JAMMING AN LPI RADAR

Very difficult and it requires lots of power! This is because the jammer does not know, at any instant, the precise frequency that the radar is using. Therefore, he must spread his jamming power over all possible frequencies. If, for example, by frequency hopping or chirping, the radar uses only 10% of the bandwidth at any one time then the jammer would have to both widen his bandwidth and increase his power by ten times to achieve the same amount of jamming as with a conventional radar.

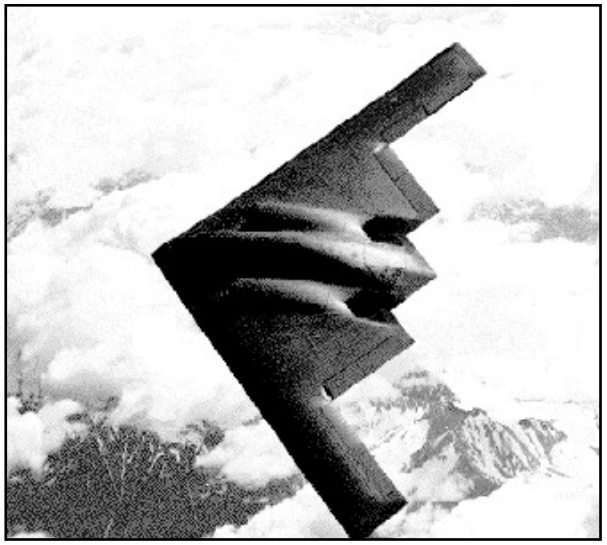
## ADDITIONAL BENEFIT OF LPI RADAR

The range resolution of a radar depends on the inverse of the bandwidth of the transmission. LPI radars deliberately widen their bandwidths to make ti difficult for the enemy to detect them. This gives an additional benefit that the range resolution is increased by the same factor that increases the bandwidth. A conventional radar pulse of duration 10 μs cannot resolve two targets on the same azimuth when they are closer together than 1.5 km. When a chirp is used to widen the bandwidth of the pulse to 10 MHz then the radar could now distinguish between targets 15 m apart. (In practice, the improvement would be less because the decoding of the chirped pulse is imperfect.)

## JAMMING A TRACKING RADAR

When attempting to acquire a target, a tracking radar will, typically, sweep its beam across a region of space seeking the strongest return. If a jammer can detect this then he could use repeater jamming to send back false echoes. These echoes would have to increase in power as the tracking radar scans away from the target and decrease in power as the radar scans towards the target. This could fool the tracking circuits into angular mis-alignment. This technique does not work with mono-pulse radars as, during mono-pulse tracking, the radar does not scan.

To deceive a tracking radar in range then it would be necessary to repeat a very strong signal with increasing delay. This would attract the tracking mechanism using a process called 'range-gate stealing'. Once the radar tracks away from the real target then the jamming is switched off leaving the radar tracking an empty bit of space. It must then try to scan to re-acquire the target, which, presumably, has moved rapidly away in the meantime.



## STEALTHY TARGETS

Radar reflections that are in the direction of the radar allow the target to be detected. This provides two opportunities to reduce radar detection:

- cause the reflections to go in another direction – not back to the radar.
- treat the surface of the aeroplane to reduce the amount of energy that is reflected.

Additional techniques might be applied to reduce visible, thermal, aural and electromagnetic detection, but these have little effect on radar.

A target that uses any of the above techniques could be describes as a stealthy target. The surface of such an aeroplane is carefully shaped so that radar reflections occur at glancing angles. Wherever possible, the surface is made using a non-metallic material, such as carbon fibre. Carbon fibre composites (like fibre-glass, but using carbon fibres instead of glass fibres) can be quite effective at absorbing radar waves. Any remaining metallic surfaces can be coated with a material that absorbs, rather than reflects, the radar energy.

## RADAR ABSORBENT MATERIALS (RAM)

This sounds easy - just apply a special coating and the aeroplane will become invisible to radar. Unfortunately, the thickness of the RAM needs to be up to half the wavelength of the radar waves in use if absorption is to be significant. At 10 GHz, the required thickness would be around 1 cm; at 3 GHz, it would need to be 4 – 5 cm thick; at 1 GHz it would scarcely be practical. Some operational radars, from the 'Soviet' Era, continue to use the lower frequencies, around 1 GHz.

One common type of RAM is a sort of paint with small iron spheres embedded in it – the coating is heavy. This means that only those parts of the aeroplane that cannot be shaped to reduce reflections will actually be coated with RAM, otherwise the payload of the aeroplane will be significantly reduced by the weight of RAM.

## DETECTING STEALTHY TARGETS

Since these targets are designed not to reflect much energy back to an ordinary radar (called mono-static - because it occupies just one location) then we need a different sort of radar to detect them.

**Bi-Static Radar**: A bi-static radar uses a transmitter at one location and a receiver at another – there can also be several receivers. The echoes from the stealthy aeroplane could be received by some of the remote receivers and its position discovered. However, this requires quite a bit of technology to implement and good communications links between the various sites.

**Non-co-operative Radar**: commercial television transmitters broadcast on frequencies around 1 GHz or less (in UK, it's around 600 MHz) at very high powers. Since these frequencies correspond to long wavelengths then RAM is not very effective. Whenever any aeroplane flies in a region where there are TV signals then it will cause changes in those signals (e.g. Doppler Shift) that can be picked up over a number of sites and analysed by a computer to determine the track of the aeroplane. As above, this requires a good deal of technology and communications.

**Data Fusion**: this is a technique in which data from several sources are combined or overlaid to produce a composite picture. A stealthy target might give a poor return on several types of sensor but, when correlated between a number of different types of sensor (e.g. radar, thermal, audio, TV) then a target could be detected at a greater range when using any single sensor. As above, this requires expensive technology and communications.

## NOT ALL NOISE IS JAMMING

The wartime radar systems on the East coast of England were used to detect the approach of German bombers. The antennae were huge masts, hundreds of feet tall. On occasions, the noise level in the receivers became quite high and significantly reduce the detection range of the system. Fearing that the Germans were jamming their radar, the British investigated further.

It was found that the 'jamming' began and ended at around the same times each day - just after dawn and then a few hours later. Eventually, it was realised that the 'enemy jamming' was, in fact, radio interference from the Sun. This was not really acted upon until shortly after the war when radio telescopes, such as that at Joderell Bank, were used to perform scientific research on the sun's radio signals and those from distant stars.

## SELF-TEST QUESTIONS

1. When an attempt is made to jam a radar system then the jamming is always directed at the:

a. Target.
b. Radar transmitter.
c. Radar receiver.
d. side-lobes.

2. When a radar receiver detects an increasing amount of noise in its signal then it:

a. lowers the level at which is recognises a target.
b. increases the level at which it recognises a target.
c. uses Doppler processing to remove it.
d. widens its bandwidth.

3. When an aeroplane that is equipped with a self-screening, noise-jamming device flies towards a radar that is trying to detect it then the radar :

a. can detect it beyond the burn-through point.
b. indicates several false targets at a greater range than the aeroplane.
c. can detect it when it is close than the burn-through point.
d. indicates several false targets at a closer range than the aeroplane.

4. An aeroplane, flying within range of a radar system, is equipped with a repeater jamming device which records then re-transmits the radar's signal, with a short delay. The radar system:

a. cannot detect any targets on that azimuth.
b. sees two targets: the aeroplane and a false target at a greater range.
c. cannot detect any targets at that elevation.
d. sees two targets: the aeroplane and a false target at a closer range.

5. For a jammer to cause a radar to detect false targets on several different azimuths, the jamming signal must enter the radar via:

a. both main beam and side-lobes.
b. the main beam only.
c. a single side-lobe.
d. the omni-directional antenna.

6. When an omni-directional antenna is used for side-lobe blanking then the jamming signal is identified as such when the signal in the:

a. omni-directional antenna is stronger than the signal in the main beam.
b. main antenna is stronger than the signal in the omni-directional beam.
c. omni-directional antenna is in anti-phase to that in the main beam.
d. main beam is in anti-phase to that in the omni-directional antenna.

7. A UAV decoy could be differentiated from the main target because the decoy causes the radar to receive:

a. a stronger echo signal than the real target.
b. a weaker echo signal than the real target.
c. a signal with a different engine modulation.
d. a signal from a different range.

8. One important difference between a LIP (Low Probability of Intercept) radar and a conventional radar is that the LPI radar has:

a. a higher output power than a conventional radar.
b. a narrower bandwidth than a conventional radar.
c. a wider bandwidth than a conventional radar.
d. a pulse that contains one single frequency.

9. The front of a stealthy aeroplane has a flat plate, inclined at 45° to the airframe. The main effect of this plate on the radar signal is to:

a. absorb radar energy and reduce any reflections.
b. send reflected energy back to the radar to confuse the receiver.
c. send reflected energy away from the radar.
d. reflect delayed signals to deceive the radar.

10. A stealthy aeroplane has surfaces made from carbon-fibre composite. The effect to this on a radar signal is to:

a. absorb radar energy and reduce any reflections.
b. send reflected energy back to the radar to confuse the receiver.
c. send reflected energy away from the radar.
d. reflect delayed signals to deceive the radar.

***Answers***

| 1. c | 2. b | 3. c | 4. b | 5. a | 6. a | 7. c | 8. c | 9. c | 10. a |
|---|---|---|---|---|---|---|---|---|---|

| Teaching Objectives | | Comments |
|---|---|---|
| **H.02.01 Describe the purpose of ECM and EPM in radar systems** | | |
| H.02.01.01 | State that ECM aims to degrade the performance of a radar. | |
| H.02.01.02 | List the types of ECM. | Noise, Deception, Decoys & Chaff, Stealth |
| H.02.01.03 | State that the more complex the radar the more difficult it will be to jam effectively. | |
| H.02.01.04 | Describe common strategies adopted by jammers. | Stand-off, Self-Screening, Escort. |
| H.02.01.05 | State that EPM are taken by the 'victim' radar to deny the use of enemy ECM. | |
| **H.02.02 Describe the properties of noise jamming ECM and EPM** | | |
| H.02.02.01 | Describe the purpose of noise jamming. | |
| H.02.02.02 | Describe the features of main-lobe jamming | Limited to around one beam-width. |
| H.02.02.03 | Describe the concept of 'Burn-through Range' | Quote illustrative figures for a basic radar. |
| H.02.02.04 | Describe the features of frequency agility as an EPM. | |
| H.02.02.05 | Describe the use of coded pulses as an EPM. | |
| H.02.02.06 | Describe the use of 3-D radar as an EPM. | Multiple elevation beams – only one can be jammed by each jammer. |
| **H.02.03 Describe the properties of side-lobe jamming ECM and EPM** | | |
| H.02.03.01 | Describe the concept of inverse-gain jamming. | Could jam on any azimuth. |
| H.02.03.02 | Describe the techniques used to control side-lobes and their effects on noise jamming. | Includes use of ultra-low side-lobe antennae. |
| H.02.03.03 | Describe the techniques of side-lobe blanking and coherent side-lobe cancellation. | |
| **H.02.04 Describe the properties of deception jamming ECM and EPM** | | |
| H.02.04.01 | Describe the purpose of deception jamming. | |
| H.02.04.02 | Describe the techniques of repeater and anticipatory jamming. | |
| H.02.04.03 | Describe the features of jamming using chaff. | |
| H.02.04.04 | Describe the features of deception using decoys. | |
| H.02.04.05 | Describe EPM methods to counter deception jamming. | Side-lobe control, variable PRF & Carrier, Leading-edge detection, Range profiling, Doppler. |
| **H.02.05 Describe the properties of LPI Radar Signals** | | |
| H.02.05.01 | State that the transmitted pulse is encoded and that its bandwidth increases. | Chirp and Pseudo-random binary phase. |
| H.02.05.02 | Describe the effect of a wide bandwidth on receiver noise when the coding of the pulse is unknown. | |
| H.02.05.03 | State that the radar can de-code its own pulse because it has the code. | |
| **H.02.06 Describe the properties of Stealthy Targets** | | |
| H.02.06.01 | Describe the features of a stealthy target. | Surface shaping, constructed of composites, RAM coatings. |
| H.02.06.02 | Describe how non-co-operative radar and data-fusion techniques can detect stealthy targets. | |

**FURTHER READING**

For those who wish to research the subject further, the Internet Site of the 'Journal of Electronic Defence' at **http://www.jedonline.com** is an excellent source of news and background information. Their section entitled 'EW101' covers a very wide range of EW concepts with contributions from experts in the subject. Some of the information in this handout was obtained from the above Internet Site.