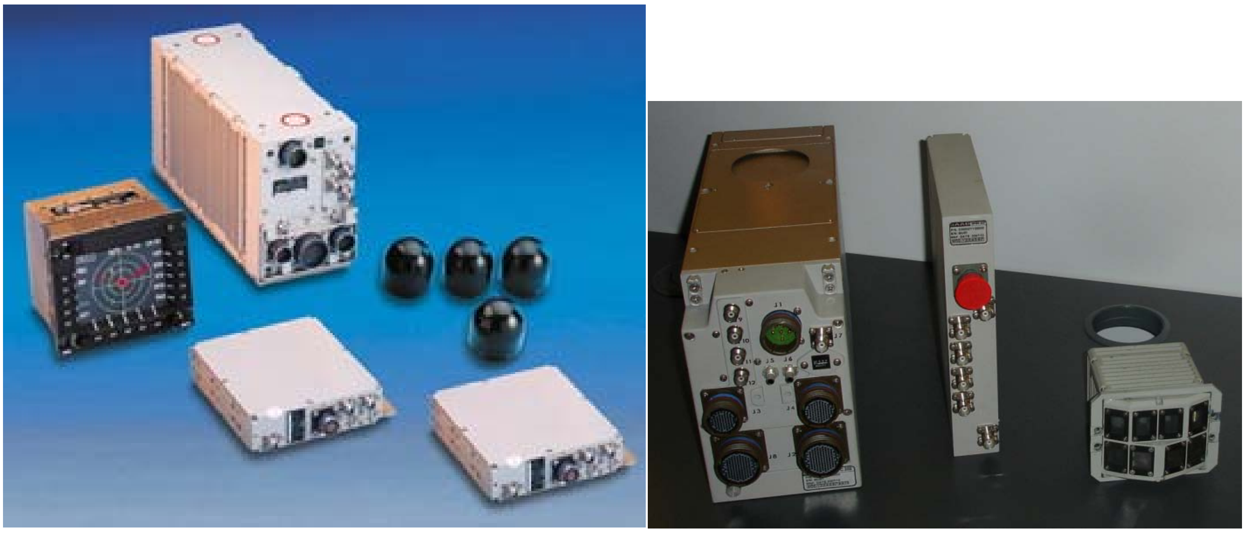


Figure 36: A typical RWR (left) and LWR (right) ESM system.

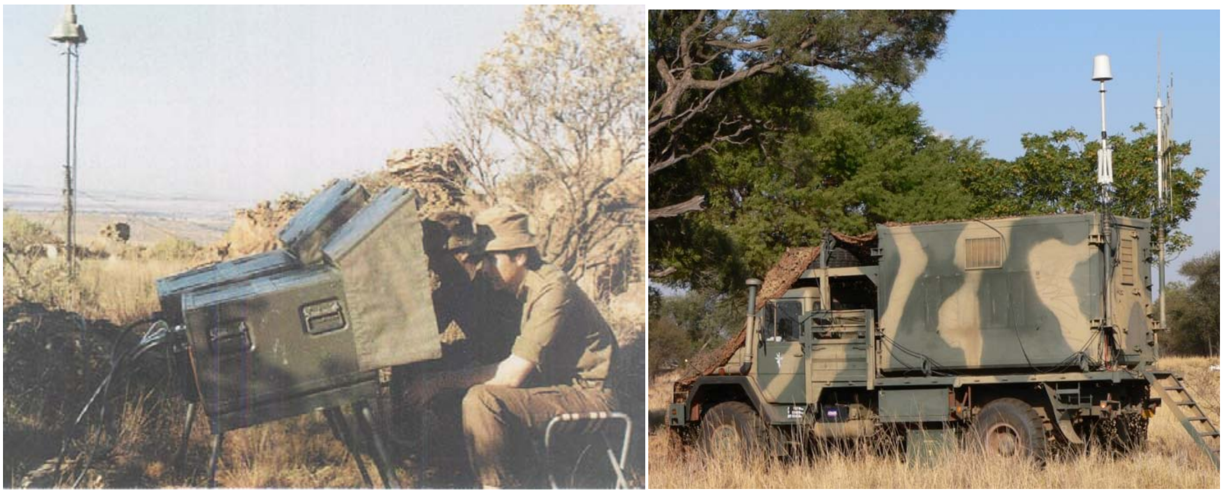


Figure 37: Examples of a tactical ELINT (left) and COMINT (right) system.

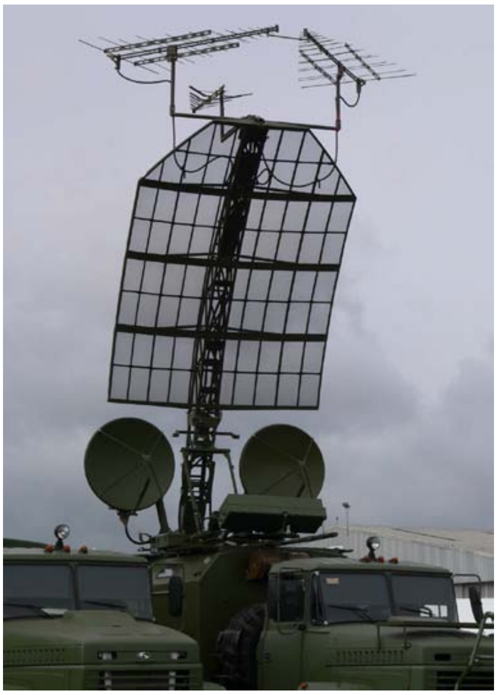


Figure 38: The Russian Kolchuga ELINT system. Four of these systems can be networked together to enable geo-location.

Figure 39: US Army Guardrail (left) and General Atomics Aeronautical Systems Sky Warrior SIGINT System (right).

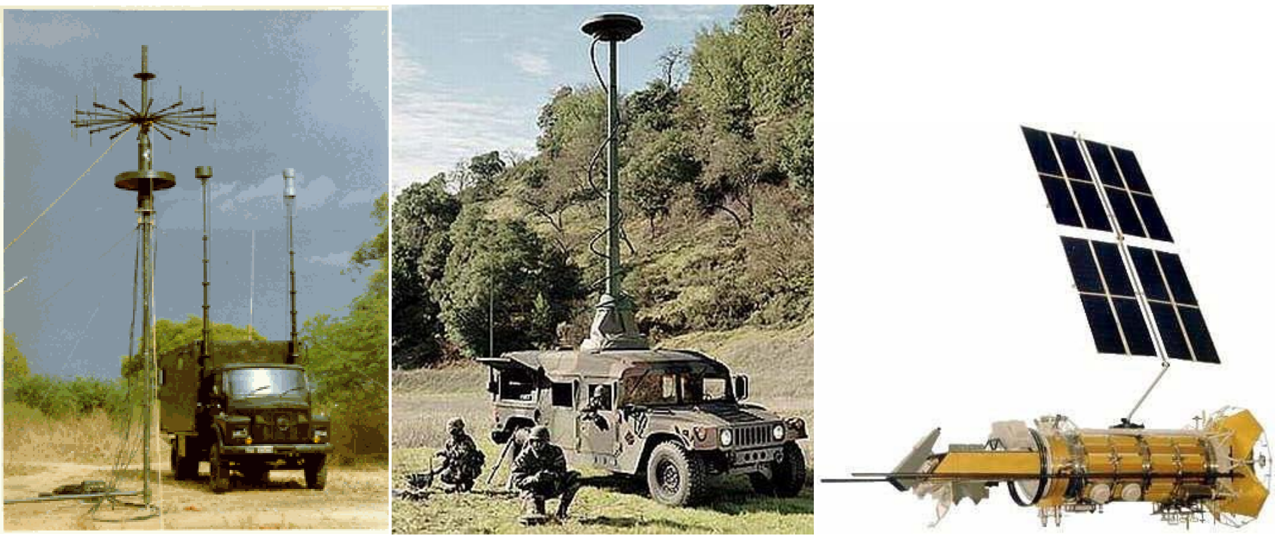


Figure 40: Typicalt tactical ground-based SIGINT systems and the Tselina 3 SIGINT satellite (right).

The most important SIGINT countermeasures are:

- Reduce the peak power that gets transmitted towards the EW receiver. This entails not only the transmitted power, but that of the antenna influences as well – transmit only in the desired direction.
- Emission Control. Transmit only when and what is necessary.
- Use waveforms that is inherently more difficult to exploit by the SIGINT receiver.

2.11 Passive Coherent Location

Passive Coherent Location (PCL) systems (also referred to as passive radar and passive covert radar) encompasses a class of radar system that detects and track objects/targets by processing reflections from non-cooperative sources of illumination in the environment, such as commercial broadcast and communication signals. PCL make use of ES receivers to perform this surveillance.

Conventional radar systems comprise a collocated transmitter and receiver, which usually share a common antenna to transmit and receive. A pulsed signal is transmitted and the time taken for the pulse to travel to the object and back allows the range of the object to be determined.

In a passive radar system, there is no dedicated transmitter. Instead, the receiver uses third-party transmitters in the environment, and measures the time difference of arrival between the signal arriving directly from the transmitter and the signal arriving via reflection from the object. This allows the bistatic range of the object to be determined. In addition to bistatic range, a passive radar will typically also measure the bistatic Doppler shift of the echo and also its direction of arrival. These allow the location, heading and speed of the object to be calculated. In some cases, multiple transmitters and/or receivers can be employed to make several independent measurements of bistatic range, Doppler and bearing and hence significantly improve the final track accuracy.

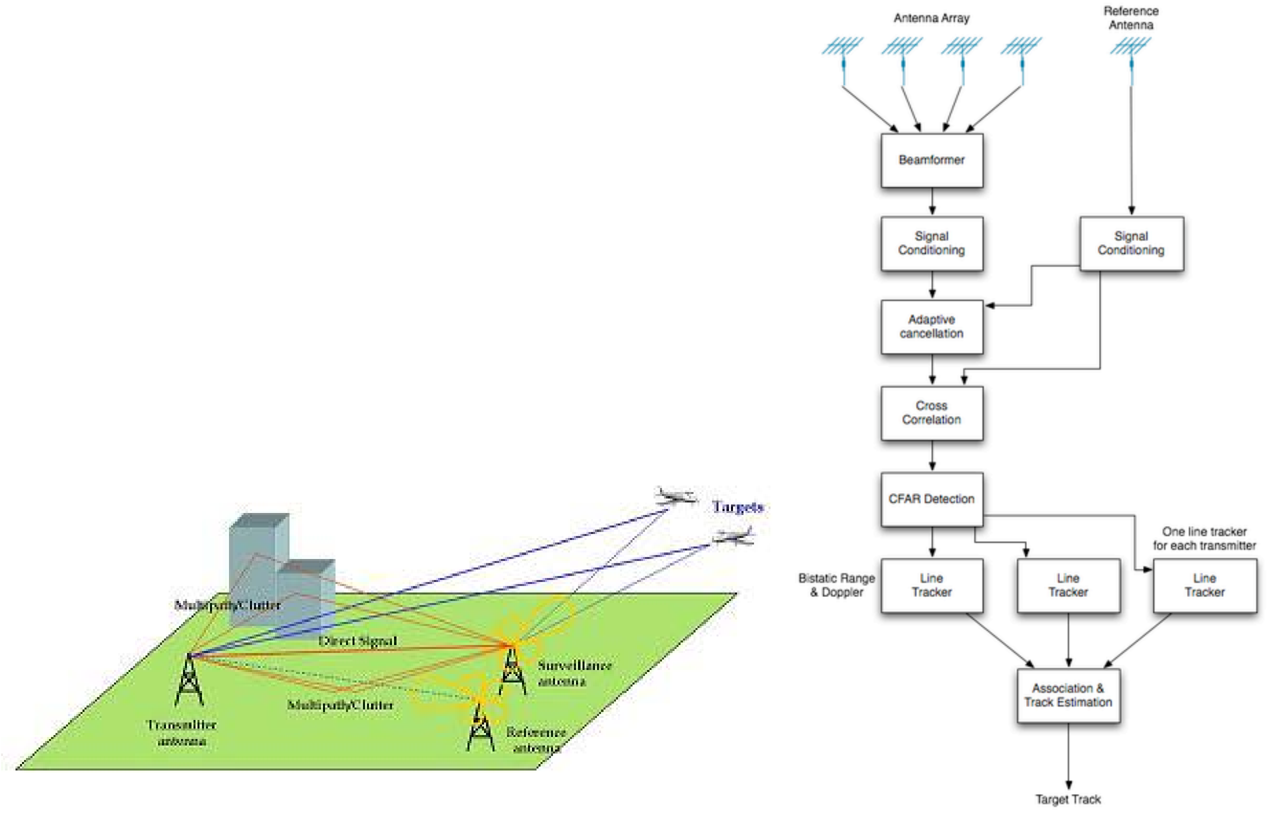


Figure 41: Generic passive radar signal processing scheme.

In order to detect and track targets, a PCL radar typically employs the following processing steps:

- Reception of the direct signal from the transmitter(s) and from the surveillance region on dedicated low-noise, linear, digital receivers.
- Digital beamforming to determine the direction of arrival of signals and spatial rejection of strong in-band interference.
- Adaptive filtering to cancel any unwanted direct signal returns in the surveillance channels.
- Cross-correlation of the reference channel with the surveillance channels to determine the object's bi-static range and Doppler.
- Detection using a Constant False Alarm Rate (CFAR) scheme.
- Association and tracking of object returns in range/Doppler space, known as line tracking.
- Association and fusion of line tracks form each transmitter to form the final estimate of an object's location, heading and speed.

PCL systems offers several advantages over current radar systems, in which the most important ones are that of cost, is undetectable to radar warning receivers due to its passive nature and allow detection of stealth platforms. Operational system examples are Silent Sentry and CELLDAR, where the emitters of opportunity are respectively commercial Frequency Modulation (FM) and High Definition Television (HDTV)-broadcasting stations as well as cell phone emissions. PCL systems were developed to act as a gap-filler radar for air surveillance to detects and tracks low-flying aircraft over terrain with poor traditional radar coverage.

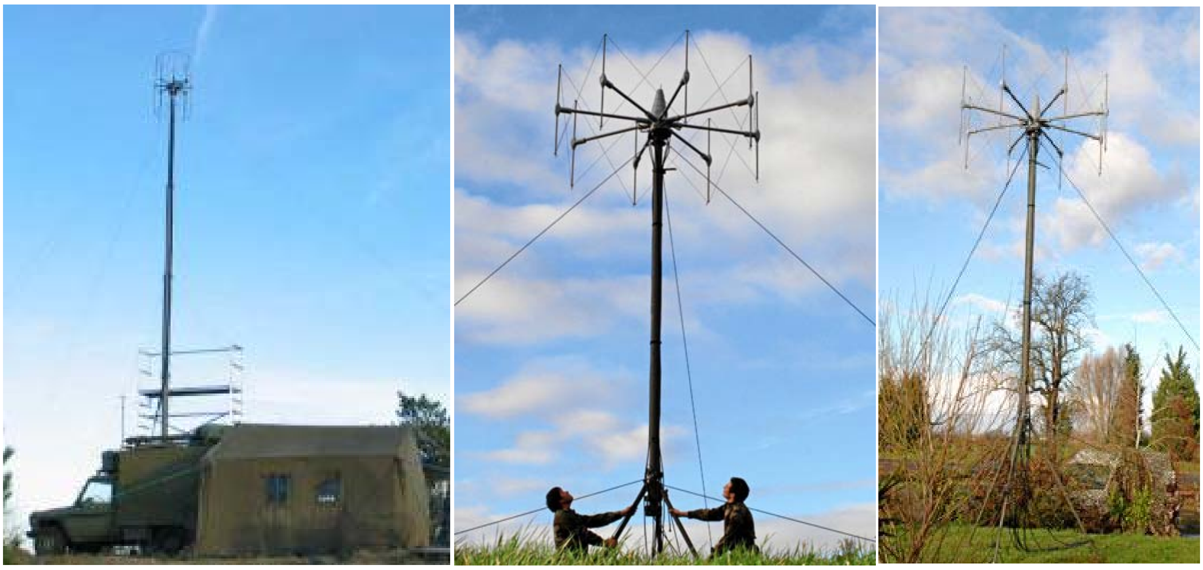


Figure 42: The USA Silent Sentry (2 x left) the Thales Homeland Alerter PCL system (right).

There is no known countermeasures against PCL based systems.

2.12 Stealth

If you cannot be seen/detected, you cannot be attacked, and that enhances mission success and survivability – and this is what stealth brings to the table. In most instances it is not a case of total invisibility, on non-detectability, but rather a case of delayed detection. This compresses the defender’s reaction timeline to the extent that he cannot timeously react, or optimally engage the target. On the other hand, if you are the defender, it requires enhanced system performance and optimized doctrine to ensure own survivability.

Although what will be discussed here is broader than the classical EW, but in many cases the same principals hold – the smaller the signature, the more stealthy the platform.

System Observables:

This is what sensors can detect.

- **Acoustic:**
  - Engine/exhaust sounds.
  - Airframe/Hull/Tire noise.
  - Propellers/blades sound.
- **Magnetic/electromagnetic:**
  - Surface ships & submarines possess enormous magnetic fields (ferrous metal) & power-generating machinery.
- .**Wake effects:**
  - Ships and aircraft generate turbulence that can be detected, often for hours after they have passed by.
- **Visual:**
  - Aircraft’s Contrails.
  - Engine Smoke.
  - Camouflage paints/patterns.
- **Thermal:**
  - Engine exhausts.
  - Air and road friction heating.
  - Absorption of solar radiation.
  - Electronic equipment.
- **Electromagnetic Emissions:**

  - Radar.
  - Communication.
  - Active EA.
  - Navigation systems (e.g. radio altimeter).
  - Secondary radar (IFF).
- **Radar:**
  - Skin return – Radar Cross Section (RCS) - including individual scatterers in the high resolution radar case.
  - Jet engine, propeller, or vibration modulation.
  - Flashes (blade and antenna).

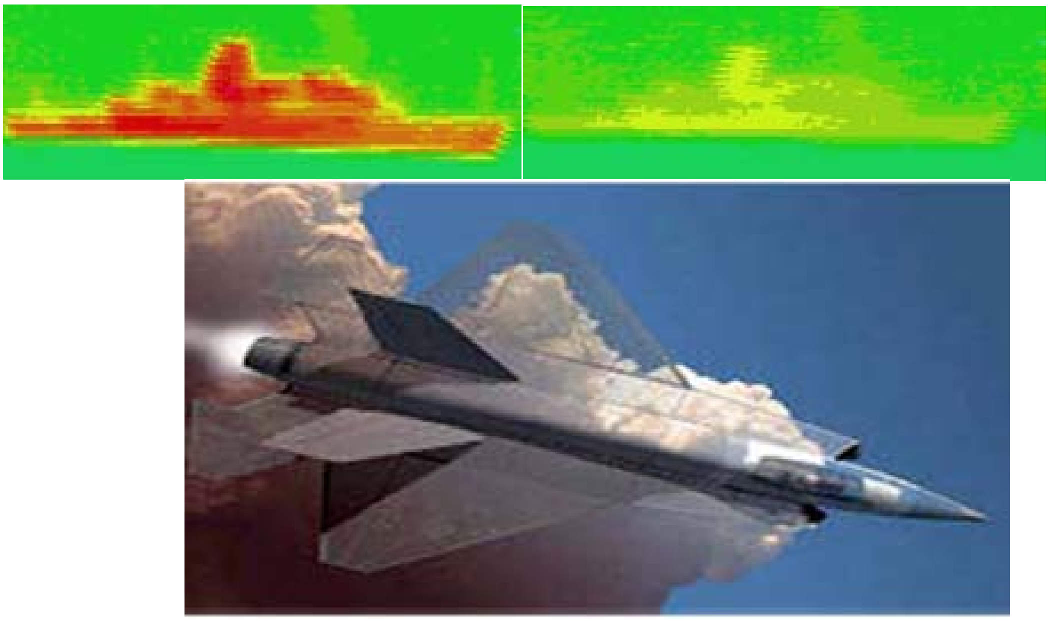


Figure 43: Effect of Solar Reflective Paints (top) and Adaptive Camouflage (bottom).

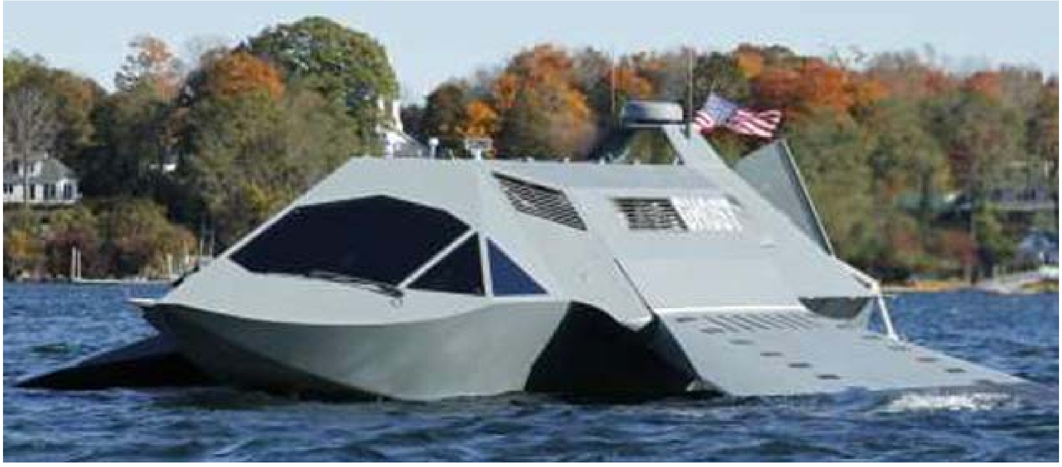


Figure 44: Hull design to reduce both the RCS as well as the wake signature.

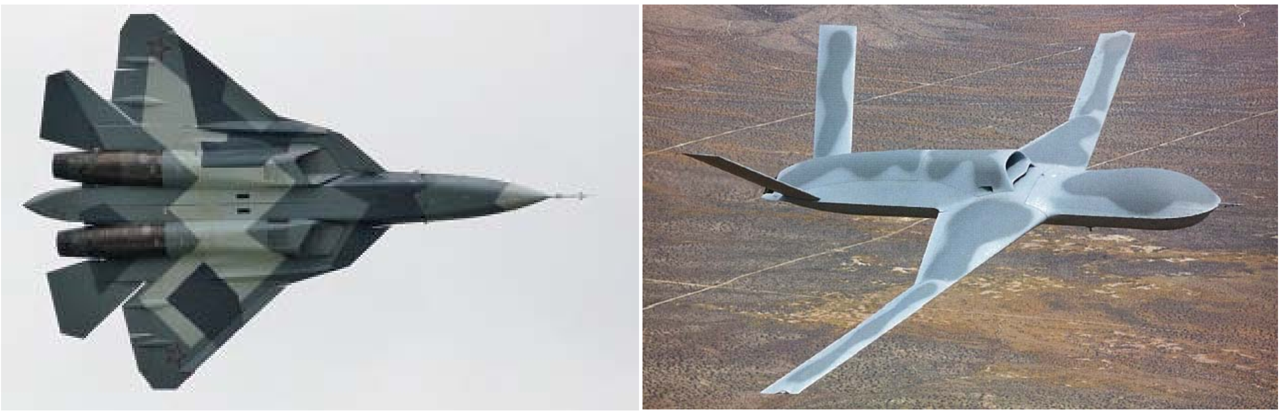


Figure 45: Russian SU-T 50 (left) and the new Predator UAV (right) – examples of low Radar Cross Section aircraft.

There are various ways to counter stealth, depending what aspect of stealth you want to exploit, but the most general countermeasure is that of networked multi-spectral sensors. Platforms cannot be stealthy from all aspects angles, and definitely not at all frequencies. For example, Radar Absorbing Material (RAM) effectiveness as a function of frequency depends on its thickness. It is therefore not practical to protect an aircraft with RAM against a low frequency threat – hence the PCL advantage.

2.13 Hostile Fire Detection

Helicopters, ground vehicles and soldiers have always been targets for enemy ground forces equipped with sniper rifles, automatic weapons and rocket-propelled grenades. As they are ballistic threats, however, they were always considered to be outside the purview of EW self-protection concepts. Armour and manoeuvre were the typically the only answers to these threats. Years of fighting in Iraq and Afghanistan, however, have changed these perceptions, especially among US and European forces and today, many new Hostile Fire Indicators (HFI) systems have been developed.

From a functional perspective, an HFI system must first detect and declare enemy small arms fire or an RPG, then it must precisely locate the source of that fire. Ideally, it will also identify or at least classify the type of weapon being fired. This is not a simple job. Helicopters, for instance, need an HFI system that can operate in the presence of noise (including outgoing gunfire) and vibration generated by the host aircraft. The noise level in a helicopter is so high that helicopter crews often do not know they are under fire until they are hit. Ground vehicles present a slightly different set of environmental challenges (dust and dirt, for instance), and they may also need an HFI capability that can accurately cue an active protection system. For soldiers, the issue is not so much noise and vibration as the size and sensitivity of the HFI. Soldiers can usually hear and locate nearby gunfire, but detecting and locating snipers at long distances is a challenge. As with any military electronics system, the goal is to have an HFI capability that is affordable, effective against a range of ballistic threats and has a minimal size, weight and power footprint on the host platform. The problem today is that no one technology is perfectly suited to perform robust HFI on all platforms.

HFI systems that use acoustic sensors to detect and locate the sound of gunfire were among the first operationally deployed capabilities in the 1990s. The technology has evolved to the point where acoustic sensors can be hosted on most ground vehicles and helicopters, but sensitivity is an issue. Another HFI solution is to use IR/ UV sensors. With more and more IR/UV-based missile warning systems being installed on helicopters and other platforms, they are excellent candidates for hosting the HFI function. The challenge is to open up the aperture, so to speak, and enable missile warners to detect the smaller IR/UV signatures of small arms without introducing false alarms in the missile warning function.

Currently the focus is on countermeasures to defeat small arms. One solution is to use Directable Infrared Countermeasures (DIRCM) systems as eye-safe visual dazzlers or disruptors against the shooters.

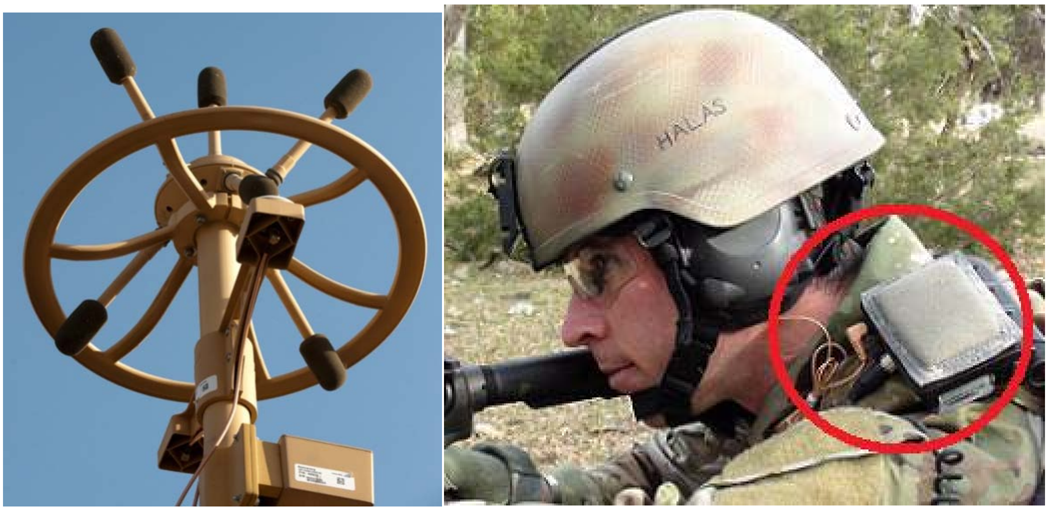


Figure 46: Boomerang acoustic (left), Soldier-Wearable Acoustic Targeting System (SWATS) (right).

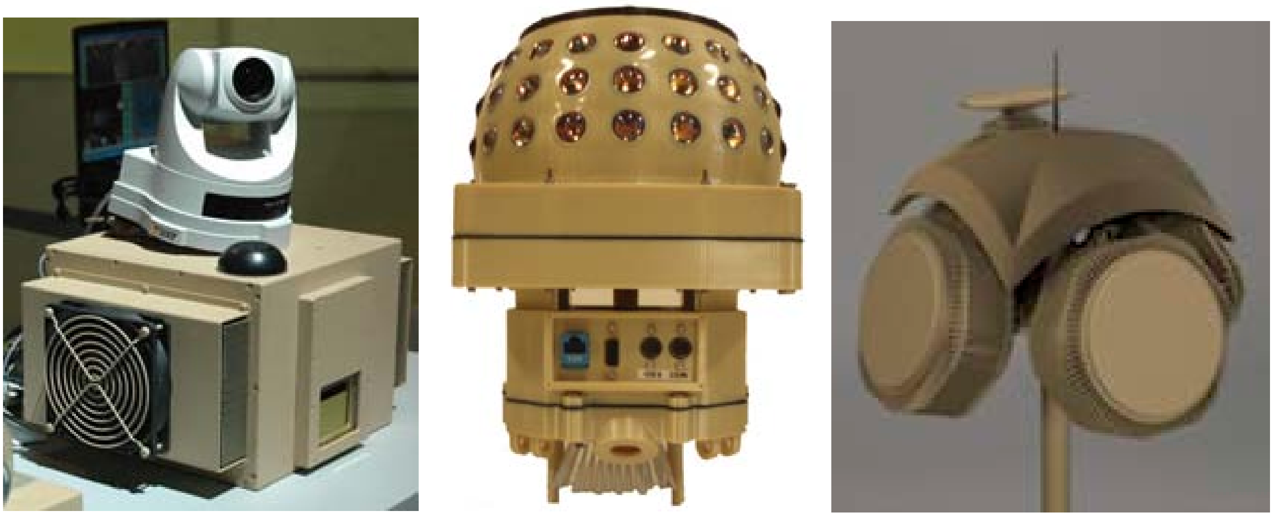


Figure 47: Apache helicopter’s WeaponWatch sector (left), ShotSense3D Shortwave Infrared 360 deg (middle), Rada pulse Doppler radar HFI system (right)

2.14 Improvised Explosive Devises

Over the past eight years, military services have fielded tens of thousands of electronic jammers of different types in Iraq and Afghanistan to protect US and Coalition forces against Remote-Controlled Improvised Explosive Devices (RCIEDs), the deadly roadside bombs used by insurgents to attack convoys and foot patrols. Called Counter RCIED Electronic Warfare (CREW) systems, the predominantly vehicle-mounted jammers automatically detect and block radio-frequency signals emitted by triggering devices, such as cellphones or garage door openers that are used to remotely detonate the bombs.

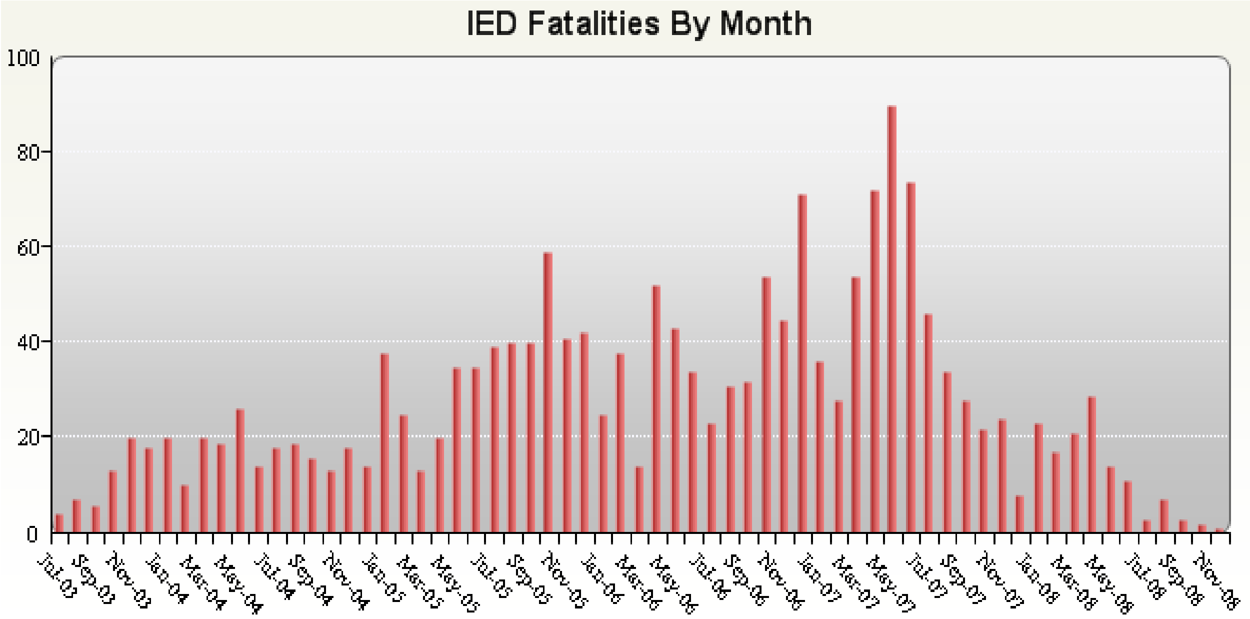


Figure 48: Operation Enduring Freedom IED Fatalities. [iCasualties.org]

The success of the RF IED jamming program is very clearly illustrated by the drop in fatalities shown in Figure 48.

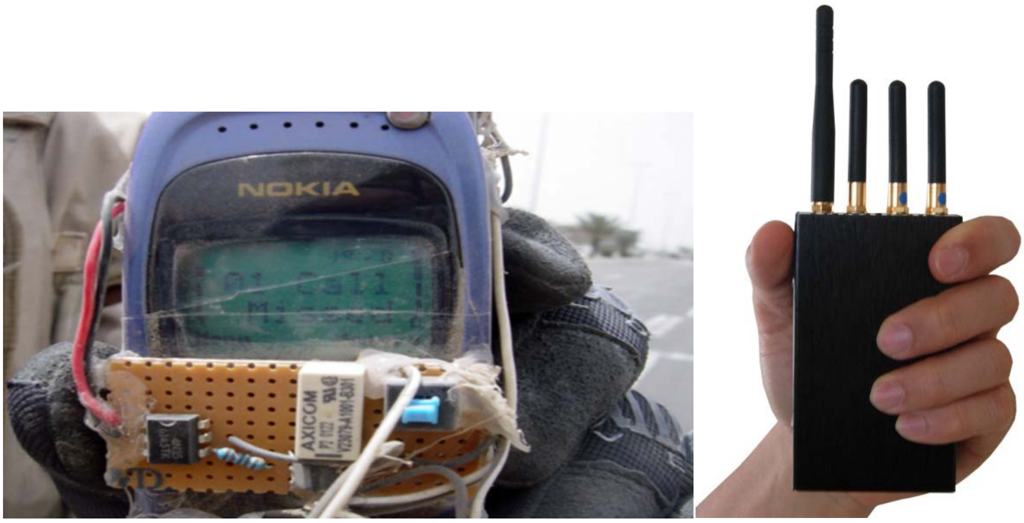


Figure 49: Cell phone IED triggering device (left) and a commercial GSM and Wi-Fi Jammer (right).

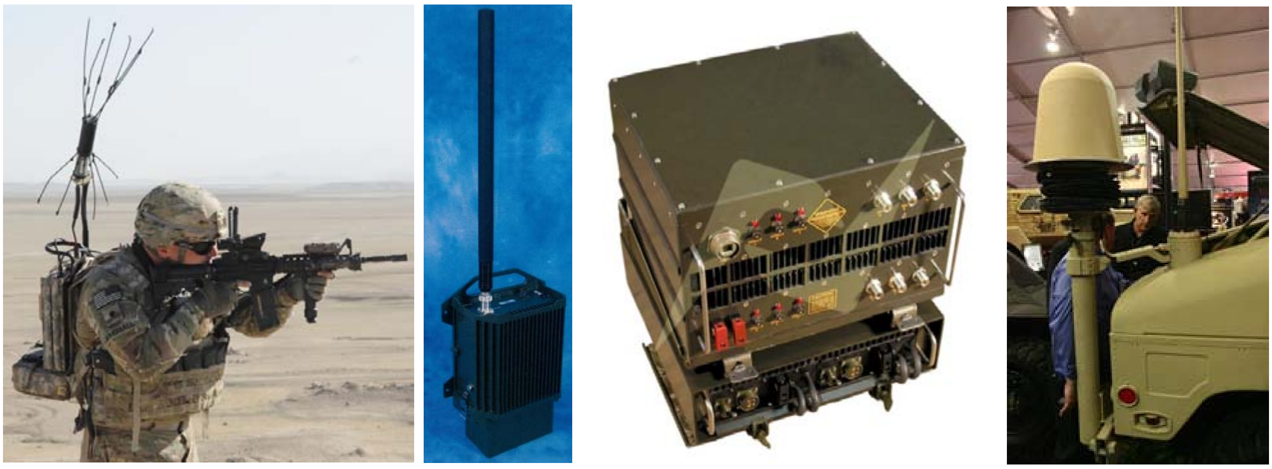


Figure 50: Man portable and vehicle mountable RF IED Jammer [SNC].

The US Army's current inventory of vehicle-mounted CREW systems consists of about 32 000 Duke V2 CREW 2.0 jammers, which the service acquired beginning in late 2005, and about 13 000 CREW 2.1 Counter Vehicle Receiver Jammer CVRJ systems and 1 300 Mobile Multi-Band Jammers (MMBJ). More than 20 000 CREW systems have been fielded since 2008, including in excess of 16 000 CVRJ, CREW 2.1 and the less numerous MMBJ used by Special Operations Forces. More than 1500 Symphony CREW systems (the only one approved for Foreign Military Sales) have been delivered.

The US is developing a next-generation JCREW 3.3 family of mounted, dismounted and fixed-site jammers intended to replace existing CREW systems in 2012. Their intention is to move beyond single-mission (force protection) CREW to ground-based EW systems with broader capabilities - called the Integrated EW System (IEWS). Key features of JCREW 3.3 are its open-architecture interface standards, which will facilitate the incorporation of advanced software applications from different vendors over time, and an emphasis on incremental software rather than hardware upgrades to keep pace with changes in the threat – i.e. pace the evolving threat.

JCREW 3.3 is required to cover a much broader frequency spectrum than the previous generation – which imposes more requirements on the RF spectrum management processes and capabilities to allow more efficient use of the spectrum. The 3.3 system has to interact not only with other jamming systems but with communications systems that might be collocated. It is not just about how to jam the device, but also how to collect information about it, how to process the information to raise the situational awareness, and how to collect relevant data and send it back for post-mission analysis.

Compatibility between IED jammers and communications systems allowing simultaneous operation remains a significant technical challenge. Software-defined radio solutions that integrate the generation of EW waveforms and communications waveforms, combined with a secure wireless link (network) to share the pertinent information are currently the only feasible solution.

In some cases, it might be advantageous not to jam a threat emitter - such as a command-and-control node, but to keep monitoring its signals and let it stay on the air. The new generation systems are expected to offer threat direction-finding and geo-location capabilities. These will allow the jammers to more effectively focus their jamming energy, thereby increasing protection range.

When NATO began its 2009 surge in Afghanistan, the threat from IEDs was picking up. There were more Taliban IED attacks and more NATO casualties than in the previous year. This was not unexpected by NATO forces, but it was obviously not welcome either. Just as they were in Iraq, IEDs have become the Taliban's weapon of choice in Afghanistan. However, the IED threat in Afghanistan is far more diverse than it was in Iraq which makes finding them a much more difficult job.

NATO's wide deployment of IED jammers has driven many bomb makers away from wireless remote controlled devices. Instead, they often build simpler IEDs that are triggered by the pressure of a vehicle's weight. In this way, they can be tailored to work against certain targets (heavy military vehicles, for example) and avoid others (lighter civilian cars and pick-up trucks). Pressure activation is a fairly indiscriminate means of detonating the bomb, and many civilians are killed by them every month.

The combat engineers in Afghanistan who perform route clearance missions have to deal with a challenging set of IED characteristics – there is a variety of IED types that are often not susceptible to IED jammers, that feature low metal content and that can be tailored so that only specific types of targets will trigger them. This makes the route clearance mission an extremely tricky and dangerous job.

Airborne surveillance, such as UAVs equipped with EO/IR sensors are effective at spotting IED teams burying their devices on roads at night. High-resolution Synthetic Aperture Radar (SAR) and EO airborne sensors may detect recently disturbed soil or subtle changes in a certain location, suggesting the presence of an IED.

When it comes to specifically locating buried IEDs, however, the job requires sensors that can operate on the ground and closer to the threat. Because of the variety of IEDs in Afghanistan, the essential need is for a sensor that provides a picture of what is in the ground, detects any kind of objects (metallic or non-metallic), and then provides, in real-time, a three-dimensional image of their shape and size on a readable display.

One of the newest counter-IED systems is the Mine Resistant Ambush Protected (MRAP) vehicle-mounted VISOR 2500 Ground Penetrating Radar (GPR). The system comprises a four-panel sensor array mounted on a sliding frame atop the forward wheel module. The array is about the width of the largest MRAPs NATO uses. IED identification also requires a skilled and experienced operator. Searching for and neutralizing IEDs takes time, and given the current threat, each target needs to be checked out before the convoy can proceed. NATO forces in Afghanistan operate more than 200 systems, and the Canadian Forces have bought an additional 21.

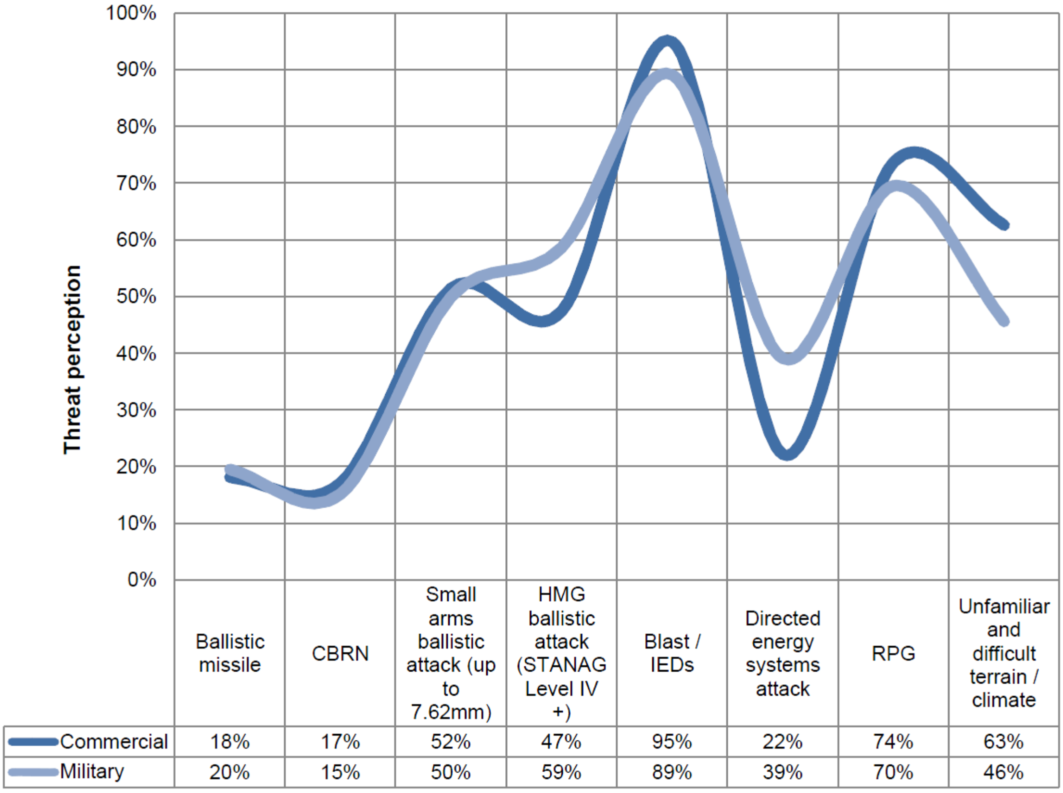
One idea the US Army is investigating is to mount GPRs on various robots, including large unmanned or optionally manned MRAP vehicles, to perform the GPR mission. Dismounted troops would have a GPR mounted on an unmanned ground vehicle or carry a hand-held GPR to sweep the ground in front of them.

Another area of interest is IED neutralization. Waiting to dig up a buried object is time consuming. The US Army is investigating new IED neutralization concepts, such as using guided munitions or high-power, long-pulse burst drilling lasers that can quickly detonate or disable IEDs at stand-off ranges up to 100 metres.

The IED threat is significant and pervading – armed forces cannot escape it in the current conflicts, nor in the next. The cost differential between the insurgents making IEDs and coalition forces developing technologies to defeat them is astounding and it is not sustainable.

2.15 Armoured Vehicles Threats

Based on the continued and persistent IED threat, armoured vehicle design requirements and the lessons learned from Iraq and Afghanistan, the future of the global armoured vehicle market, and how it is likely to evolve over the next decade in the context of the IED threat is shown in Figure 51.



	Ballistic missile	CBRN	Small arms ballistic attack (up to 7.62mm)	HMG ballistic attack (STANAG Level IV +)	Blast / IEDs	Directed energy systems attack	RPG	Unfamiliar and difficult terrain / climate
▬ Commercial	18%	17%	52%	47%	95%	22%	74%	63%
▬ Military	20%	15%	50%	59%	89%	39%	70%	46%

Figure 51: Analysis of key threats to protect against in the future. [DefenceiQ]

This shows that DEW is becoming a more important threat. Also, the role that HFI systems can play is becoming more evident due to the perceived vulnerabilities to the small arms, heavy machine gun (HMG) and Rocket Propelled Grenade (RPG) threat – which appear to be of critical importance.

While one can up-armour vehicles to protect against roadside bombs, they can only realistically be protected to certain levels. Typically vehicles are protected against STANAG Level 2 or 3 level blasts, which is the equivalent of a 6kg or 8kg explosive charge respectively. When IEDs are made with larger charges than this, the armoured vehicle becomes vulnerable to penetration - it doesn't take much time, intelligence or money to make a slightly larger IED.

The bottom line - One cannot armour oneself out of this threat. We have to be smarter, think of other approaches and technologies to protect soldiers in transit and in battle. Armour is a vital component and cannot be replaced or undervalued, but more protection is not the answer here. Detection is.

One can take care of an IED once you have found it. Protecting against the blast becomes a secondary consideration if one can significantly improve the detection of IEDs in the first instance. In addition to detection there is avoidance. IEDs are typically placed along known routes – going off-road at every opportunity could be an effective tactic to "defeat" the IED threat because, quite simply, the enemy cannot lay them everywhere.