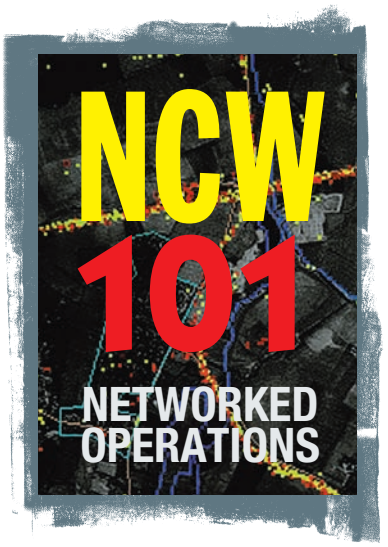


Information Warfare vs ISR Systems

NCW 101 Part 15

Dr Carlo Kopp

Intelligence, Surveillance and Reconnaissance (ISR) capabilities are the 'eyes and ears' of any Network Centric Warfare (NCW) oriented warfighting system. As such, the application of Information Warfare (IW) techniques against ISR systems can be highly profitable, if successful.

The traditional approach to discussing this problem is usually split into two separate discussions, one dealing with technical Electronic Warfare measures against sensor equipment and another dealing with deceptions aimed at operators and imagery analysts or interpreters. This way of looking at the problem is increasingly problematic, with increasing levels of automation in ISR systems, especially in terms of automated cueing operators or analysts to items of interest in the ISR picture. Where do we draw the line between 'technological' deceptions aimed at automated machinery in ISR versus the human 'wetware' of the ISR system user?

A much more general approach to this problem is to look at the deceptive measures in the framework of the four canonical strategies of IW (refer previous NCW101) and identify whether the deception is targeted at the ISR sensor/system's capability to gather raw data or its capability to interpret the raw data, accepting that the intended victim may be a piece of hardware, software and/or wetware. In effect, we look at the victim's networked system as a system, rather than its disparate parts.

ISR systems today can be broadly divided into radar based, passive (RF) radio-frequency based and electro-optical (EO) based systems, often fused with geographical or other databases intended to aid interpretation and further exploitation. A radar based system may involve the use of imaging 2D or even 3D synthetic aperture radar, inverse-synthetic aperture radar, narrowband or ultra-wideband radar, earth and foliage penetrating radar, ground, air or maritime moving target indicator radar using DPCA techniques, or pulse Doppler radar. Some of these radars produce imagery of areas or objects, and some produce coordinate, kinematic and often identification data for targets as outputs. Many modern radars can interleave these modes and fuse the outputs into a single situational picture, containing imagery output, kinematic and ident parameters for targets. This increasingly creates vulnerabilities for a sophisticated attacker to exploit.

Passive RF sensors will typically locate a threat emitter with some accuracy, and identify it with the most sophisticated systems capable of accurate geolocation and 'fingerprinting' of specific pieces of emitter equipment, based on production tolerance caused variations in signal format.

Noise jamming of radar is an active degradation attack. Depicted are Cold War era EF-111A Raven and Spoon Rest D.

EO sensors vary widely in effective range, sensitivity, resolution, and may operate in visible, near Infrared / shortwave, mid-Infrared / midwave and far infrared / longwave bands, or if a hyperspectral sensor, it may operate over dozens or even hundreds of bands. Imagers may be framing cameras, video cameras and pushbroom stripmappers or linescanners.

A sophisticated opponent may perform a multispectral attack, simultaneously targeting multiple sensor types in multiple ways, while also aiming to compromise interpretation of gathered data.

Passive Degradation Attacks

Degradation attacks are intended to bury the signal in noise, hiding it from an opponent. All forms of camouflage, be they optical or electronic, fall into this category, as does stealth technology. Such attacks primarily target the physics of the sensor to reduce the contrast of the signal against the background, although they may also target interpretation.

A good example of this strategy is an opponent who uses multispectral camouflage netting to cover deployed equipment. Such netting is opaque to radar across a wide range of radar and optical bands making the hidden target look like terrain or foliage.

The conventional approach to beating this technique is to increase spectral coverage of the ISR system to find a band where the camouflage is less than perfect, exposing the target. Hyperspectral imagers are intended to achieve precisely this effect, as it is extremely difficult to design a multispectral camouflage identical to a background across hundreds of individual narrow bands.

Other approaches to beat multispectral camouflage include Coherent Change Detection (CCD) where an ISR system images an area with the same sensor over a period of time, from the same point in space. A computer then compares consecutive images pixel-by-pixel to spot changes, which are flagged to an operator. A hillock or thicket of trees, which moves around day by day over time is evidently not going to be what it seems to be. The problem with CCD techniques are false positives, a problem observed in Iraq, where seasonal changes in the environment (windborne trash, innocuous earthworks, and dumping of garbage) were all revealed by CCD systems requiring investigation – to no effect. Data is not information and turning the raw data into information can often prove very expensive.



Visual camouflage is a passive degradation attack. It has a long and literally colourful history.

There has been a long running argument in professional circles over the merits or otherwise of sophisticated and expensive camouflage, the extreme of which are top end stealth platforms such as the B-2A costing up to 50 per cent more than non-stealthy systems. The argument is always that a sensor can be built to punch through any camouflage. The counterargument is the cost of the sensor and the processing overhead to exploit it. A massive high-power aperture radar or multistatic radar built to see a stealth aircraft at 100 miles will be manifold the cost of a conventional radar. A hyperspectral pushbroom imager will be several times the cost of a single or dual-band infrared linescanner, with commensurately more expensive post-processing of imagery output.

The argument distils down to the same argument between projectile weapon designers and armour plate or concrete bunker designers. The end result is evolutionary growth in sensors and camouflage, with resulting growth in costs to develop and deploy, and further costs in writing off uncompetitive legacy equipment and systems.

At this point in military history stealth techniques against radar have the upper hand, whereas in most instances in the optical bands the advantage goes to the sensor side of the contest.

Passive degradation will remain a key technique to deal with both for implementors of stealth and camouflage, and implementors of sensors, at least for the foreseeable future.

In general, the only reliable strategy for defeating passive degradation is to employ sensors operating in bands well outside of the useful effect of the stealth or camouflage measures, where nature permits this. The reality of optical and radio propagation physics is, however, that the atmosphere is not always cooperative – with cloud, fog and haze being opaque to light and millimetric band radar, and dense raincloud and rain often opaque to centimetric band radars. In the lower radar bands, returns from targets such as vehicles may be extremely difficult to distinguish from terrain features, as the radar wavelength increases relative to the physical size of target shape features or indeed whole targets. The 'out of band' solution to the passive degradation attack may therefore be genuinely problematic.

An interesting case study lies in the latter phases of the Battle for the Atlantic during the 1940s when the Kriegsmarine equipped U-boots were equipped with radar warning receivers. The Allies shifted their radar to a shorter wavelength, defeating this defence, but the Kriegsmarine assumed the Allies beat their countermeasure by the use of infrared sensors, and invested heavily in sophisticated infrared band camouflage for U-boot snorkels, obviously to no effect.

In the domain of passive RF sensors used to hunt for radars and radio emitters, there has been a progressive shift away from legacy narrowband RF modulations, increasingly to wideband noise-like low probability of intercept (LPI) spread spectrum and frequency hopping modulations. These appear as noise to conventional radar homing and intercept receivers, making them much harder to detect – classical degradation strategy in action. The cost has been a considerable increase in the complexity and cost of radars and communications equipment, followed in turn by increasing complexity and cost in homing and intercept receivers, as ISR users seek to defeat evolving emitter technology.

Active Degradation Attacks

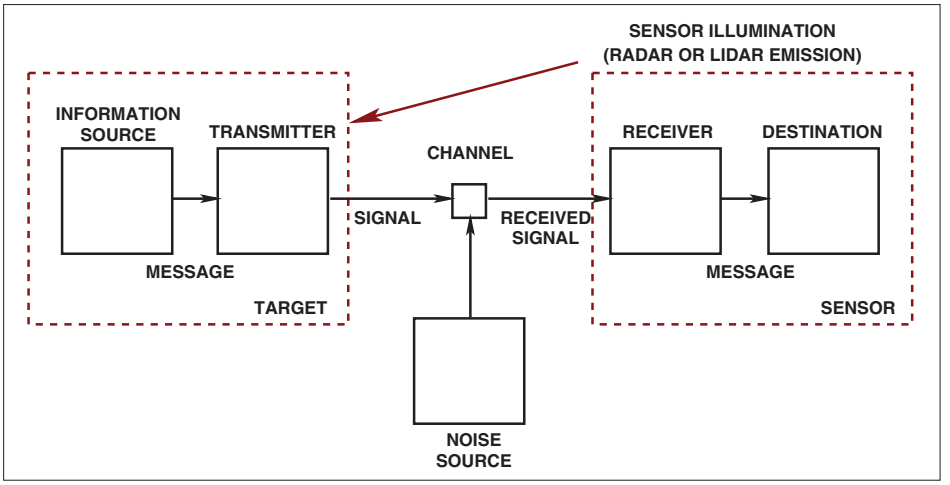
Much of traditional EW falls into the category of active degradation attacks, where noise-like signals are transmitted at a victim receiver to degrade its sensitivity or indeed wholly conceal the target from detection. Active degradation has also been used as a supporting mode of attack to increase the effect of a passive attack – the most prominent recent case study is the US Air Force's use of EF-111A Raven standoff jammer aircraft in 1991, and EA-6B Prowler aircraft in 1999 and 2003, to support attacking F-117A and more recently B-2A stealth aircraft. Stealth might work well, but it works ever better if the victim radar is drowning in manmade noise.

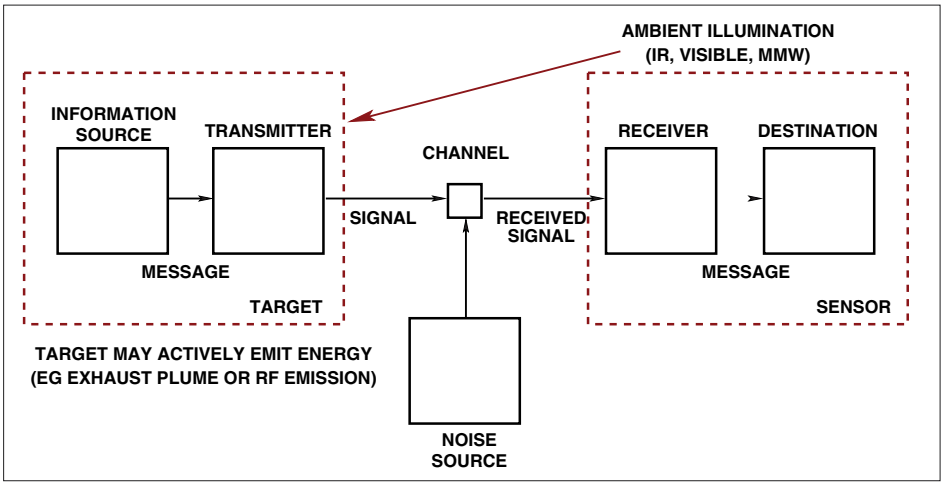
The basic drawback of active degradation is that the victim knows itself to be under attack, and thus surprise is usually lost. A good case study of this was the bombing of Baghdad in 1991, when Iraqi air defences hosed the sky blindly with barrage artillery fire, the instant an EF-111A Raven jammer lit up to support a penetrating F-117A stealth fighter. Soon thereafter the US discontinued this pre-emptive jamming support, shifting to reactive jamming only if an immediate threat to the F-117A was detected.

While active degradation is often more effective than passive degradation, the loss of surprise may render it less useful.

Corruption Attacks

Corruption attacks invariably involve some kind of deceptive or mimicking play by an attacker, intended to deceive the victim by making a target look to be something other than what it really is. If detection is inevitable, then confusing the enemy becomes a high priority.





NCW 101 NETWORKED OPERATIONS

right: Corruption attacks deceive the opponent as to the identity of a target. Decoys are an excellent example of seductive corruption attacks. Depicted inflatable decoys made by Aerostar Inc.

below: An anti-radiation missile attack is a basic example of a denial through destruction attack against a sensor, in this instance a microwave radar. (USAF)

A corruption attack is always targeted at the mechanism – be it machine or wetware – which provides for the recognition of a target or a signal.

Corruption attacks have a colourful history, from wearing an opponent's uniforms in land warfare, hoisting opponents' or neutral flags in naval warfare, flying captured aircraft in aerial warfare, broadcasting bogus radio traffic with orders or directives, and using decoys to seduce operators, sensors or weapon seekers.

The principal play is to make a threat system appear to be something non-threatening, or a non-threatening object appear to be a threat, to divert fire. This symmetry is as old as the business of warfare (and biological evolution in general).

A well orchestrated and implemented corruption attack can be difficult to detect and defeat. The best mechanism would appear to be the detection of inconsistencies or incongruities.

If a unit of friendly troops appears in a very improbably location, are they friendlies or are they hostiles equipped with friendly uniforms, equipment and IFF transponders?

Much of the evolution to increasingly complex radar and radio signal formats, IFF formats, and increasingly the use of encryption is the direct result of an ongoing effort to defeat corruption attacks.

The 911 kamikaze attacks are a good case study. Assuming the airliners were hijacked to bargain for hostages, the US was slow in responding to what was actually an attack using in effect passenger-laden oversized cruise missiles. The hijackers played on the classical hijack scenario successfully, as immediate fighter intercepts to shoot down the four aircraft were not launched.

Many corruption attacks are 'one shot plays', as once the ruse has been exposed it will no longer be successful.

An unfortunate byproduct of successful corruption attacks is the risk that friendly forces suffering identification problems, or being in the wrong place at the wrong time, will be fired upon.

The plethora of EW techniques intended to break track or lock in victim radars qualify as corruption attacks, intended to defeat the range or angle measurement of a sensor and introduce a false perception in the victim system or operator of the location of the target. False target generators are a more sophisticated jamming technique, often expensive to implement, but seen carried by support jamming aircraft and heavy bombers. The victim system or operator sees a nonexistent formation of aircraft where there should be none. This is a classical corruption attack no different from inflatable decoy trucks, tanks and SAM systems. The latter ruse is aimed at EO and imaging radar sensors.

Corruption attacks will remain a plague in the warfighting business since they are so profitable when they are successful. A terrorist who elicits a bombing raid on innocent civilians is a good example of how this play can be effective, no differently from the terrorist hiding a satchel bomb in a pram to get close to a checkpoint.

The technological defence is primarily to evolve technology that is difficult to mimic by an opponent, and wetware defence is for the human element to actively anticipate this play in combat.

Denial Through Destruction Attacks

Smashing or blinding an opponent's sensor system or device is a denial through destruction attack, the aim of which is to temporarily or permanently remove that ISR element from the battlespace.

Denial through destruction attacks have almost as colourful a history as other techniques. This attack may be used independently, or may be used to support a more complex compound deception strategy.

The independent use of denial through destruction is characteristically observed in the opening hours of an aerial bombardment campaign when the victim's radars are systematically crippled or destroyed by attack using hard kill weapons, the aim being to blind the opponent's air defence system to incoming aircraft. Other good examples are the use of lasers to temporarily or permanently blind electro-optical systems, operator eyeballs, or electro-optical ISR satellites in low orbit. If a High Power Microwave weapon is used against a sensor system, or a high power AESA used to blind a victim radar or passive surveillance system, then the denial through destruction strategy is being applied.

The use of a counter-ISR weapon such as an ASAT launched against an ISR satellite, or an 'anti-AWACS' missile launched against an airborne ISR platform are the latest incarnations of this strategy to become popular.

As with active degradation attacks, the victim knows an attack is underway and thus surprise is lost. What critically distinguishes soft kill denial through destruction attacks from active degradation attacks is that the former is aimed at the victim's receiver, but the latter is aimed at degrading the channel as a transmission environment. Although the means may be similar, the focus of the attack is different.

The hard kill form of denial through destruction attack will progressively increase in popularity because it inflicts attrition on victims' ISR systems, which are inherently expensive, often scarce in numbers, and difficult and slow to replace due to high complexity and long production times. Once the ISR system or its carrying platform are removed from the battlespace the numerical ratio of forces has been incrementally shifted in favour of the attacker.

NCW, with its high dependency on ISR systems, will compel opponents to pursue the hard kill form of the denial through destruction attack because it is so profitable in the short term tactical context, and the long term strategic context. No nation can afford to lose multiple AWACS/AEW&C platforms or ISR satellites day after day in a conflict, and no tactical engagement can be successfully pursued by ISR/NCW dependent platforms if their ISR systems are destroyed.

Denial Through Subversion

Subversion attacks, which involve implanting a self-destructive instruction into a victim system, are common in biological systems and computer networks, but much less common as a mode of attack used against sensors.

More than often this mode of attack is connected to a sensor only insofar as the sensor is the channel via which the self destructive directive is delivered to the victim system, usually employing a corruption strategy.

Arguably, jamming attacks intended to cause premature initiation of proximity fuses might be classed as a subversion attack.

Assessing the Big Picture

The reality of the information age is that information has become the new 'high ground' in modern conflicts, especially between technological opponents.

The increased diversity and complexity seen in modern sensors and ISR systems is a double edged sword. It provides more opportunities to defeat IW techniques played by an opponent, but it also creates more opportunities for a clever opponent to exploit specific weaknesses.

A future warrior will need to understand the weaknesses and strengths of his or her sensors and ISR systems, moreso than has been historically required. Simple sensors and simple deception techniques required a basic understanding to manage robustly, and increases in sensor complexity and diversity require proportionate increases in operator intelligence and understanding to survive in a more complex, faster moving and more diverse battlespace.

Smarter systems will require smarter warriors.