2.3 Navigation Systems

Referred to here are the ground based Radio Frequency (RF) navigation beacons (for example, DECCA, LORAN and OMEGA) operating in the Low Frequency (LF) region and the various Global Navigation Satellite Systems (GNSS) like GPS (USA), GLONASS (Russia), Galileo (European Union), Compass (China), not to mention the various regional satellite based navigation systems operating in the Ultra High Frequency (UHF) region.

GNSS based navigation is playing an increasingly important role in the military and commercial market, not only for position information, used for navigation and precision weapons guidance, but also for time information to synchronise communication systems (for example frequency and time-hopping radios).

Due to the very low RF power received by GNSS receivers, it is extremely easy to do a denial of service attack. Spoofing is more difficult, not due to the power, but rather due to the deceiving signal integrity required. Two levels of protection are available, the first being jamming detection. If the user knows that his GNSS system has been compromised, he can fall back on other means (normally less precise) to fulfil his PNT requirements, for example Inertial Navigation Systems (INS). Accurate timing, however, is more difficult to ensure, and typically requires that each device must be fitted with expensive (cost and SWaP) timing hardware.

The second level of protection is to fit the GNSS receivers with Active Electronically Steered Antennas (AESA) to enable beam steering (in the direction of the space vehicles) and null-steering (in the direction of the “interferes”). This solution has quite a cost and SWaP implication, especially if it has to be implemented on a moving platform.

The placement (and type of antenna/antenna pattern) of GNSS antennas on platforms plays an important role to ensure good operation of the system within a hostile EM environment.

Navigation Warfare (NavWar): Deliberate defensive and offensive action to assure and prevent Positioning, Navigation and Timing (PNT) information through coordinated employment of space, cyberspace, & EW operations.

- Desired PNT Effects:
  - Assure Blue access to high-integrity PNT.
  - Perform counter-PNT (deceive, deny, disrupt, degrade & destroy Red PNT).
  - Identify, characterize or geolocate sources of Red interference with Blue PNT information ("PNT Exploit").
  - Resolve interruptions to PNT information, including unintentional Blue-on-Blue interference.

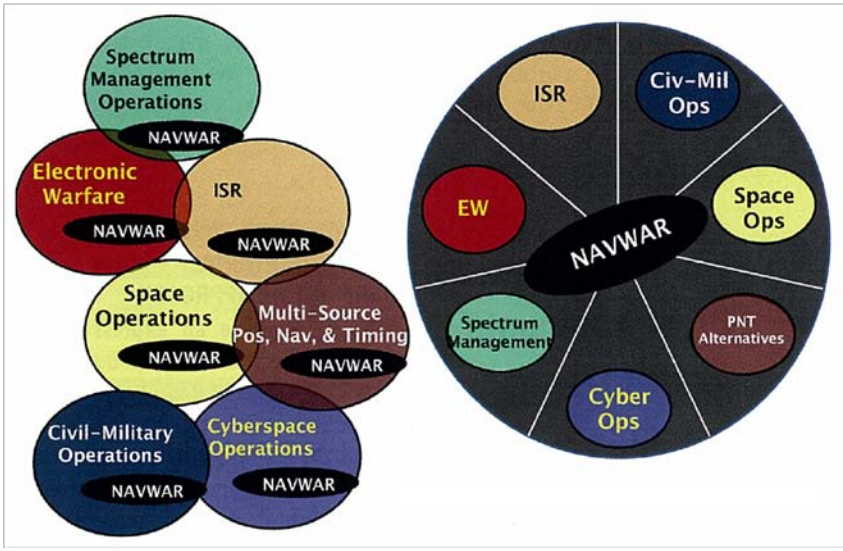

Figure 18: NavWar and its components.

2.4 Radar

Radars can determine the distance, location, and velocity of ships, aircraft, ground vehicles, missiles, munitions and people. Radar signals can be continuous or pulsed. Radar signals vary from High Frequency (HF) for Over-The-Horizon (OTH) radars to Extremely High Frequency (ELF) for proximity fuse and “look through wall” applications.

Modern radar design is primarily aimed at providing more functions and better performance and adapting better to non-stationary targets and the environment. Similar to the communication environment, many of the features listed here, although not intended as Electronic Protection measures, makes life for EW systems very difficult in terms of detection and jamming. Some of these features are:

- Active Electronically Scanned Arrays (AESA): Multi-function – surveillance – Synthetic Aperture Radar (SAR), weather, search, track, weapons guidance, communication data-links and Electronic Attack (jamming), all in one system. The AESA architecture is inherently that of a Low Probability of Intercept (LPI) nature due to the pseudo random scan and dwell antenna pattern. This requires the EW receiver to be sensitive enough to detect the radar through its antenna sidelobes. Furthermore, the multiple functions requires multiple waveforms to be transmitted, and depending on the environment and mission, will be pseudo-randomly interleaved – a very difficult identification problem for the EW receiver due to the severe EW database implications. Multiple Input Multiple Output (MIMO) radars take this approach to the next level, because they can do beamforming on transmit and/or receive: if it is done on receive, the EW receiver has no way of distinguishing the mode of the radar.
- The radar is an active device – it transmits a signal, and based on the return, will adapt its waveform to optimize detection and minimize interference and clutter. The trend is away from fixed waveforms and modes to modeless, optimally interleaving the various waveforms and functions (scheduling) – all software defined, which makes identification from an EW receiver point of view extremely difficult (how to structure and populate an EW database?).
- Wider Operating Frequency bands and overlap with "communication" frequencies. Current generation ESM and ELINT receivers are not capable of handling the huge data-rates that the communication link "interferes" introduce. The only current solution is to use channelized digital receivers in conjunction with the more established receiver architectures.
- Low Probability of Detect (LPD) waveforms. Some radars use very low peak power CW waveforms, or even Noise waveforms. Because the radar knows what it transmits and when, it can make use of processing gain to detect its targets at suitable ranges, but because the EW receiver does not have this a-priori knowledge, it has to use sophisticated digital techniques to detect these signals (in the ambient noise) and classify them. This can only be done with a digital receiver.
- Bi-static & Networked. An EW system can only detect the transmitter and jam the receiver. If these two are not co-located, as is the case for bi-static or multi-static radars, the EW efficiency suffers. Simurily, because the radars are interconnected, both (or all) will have to be jammed simultaneously to be effective – this places additional requirements on the EA systems in terms of number/coverage and/or power. On the other hand, networked sensors also have an inherent vulnerability – if false information is fed into one, the information might influence the fused information of the bigger system, which increases the effect.
- Higher resolution, both in range and Doppler nullifies some of the passive airborne countermeasure techniques such as chaff, because the chaff only blooms (has a large enough Radar Cross Section (RCS) outside the radar's range resolution cell, and hence cannot sufficiently screen the target. The effect on active jammers is that they will be required to pre-empt the incoming signal (through the use of Pulse Repetition Interval (PRI) and scan predictors) because the RF signal delay through the jammer will otherwise be too long to allow enough jamming energy into the radar resolution cell. With some of the modern radar waveforms, this is not easily accomplished.
- Multi target track. This makes it much more difficult to deceive a radar with false targets, because the radar track the false targets and the real target simultaneously, and can use additional logic to feed the decision-making processes (for example the TEWA). Therefore, the previous "break-lock" jamming techniques have become less applicable.

Figure 19: Selex Galileo's Vixen 1000E (for the Gripen NG) – left and the SAAB Erieye AEW&C AESA radar (right).

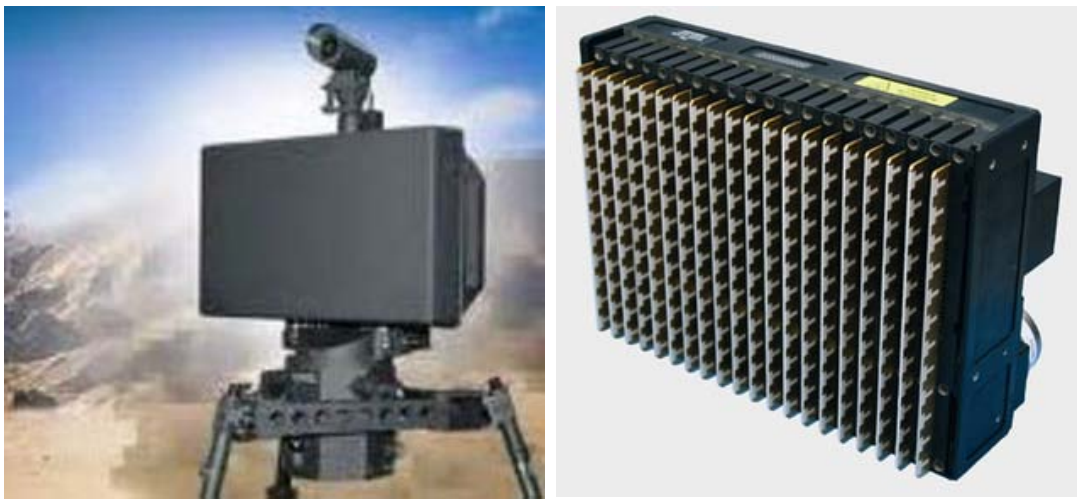

Figure 20: Cassidian's border control (left) and Selex's PicoSAR (for UAVs) AESA radar (right).

2.5 Electro-Optical Systems

Electro-Optical (EO) systems generally deal with the electromagnetic generation, control, propagation and detection of signals in the infrared (IR), visible and ultraviolet (UV) spectrums. Some of the systems operating within this range include:

- Laser communications and range finders.
- IR and Imagery guided missiles.
- Laser guided bombs and beam-riding missiles.
- Low-light and daylight systems.

IR missiles detect heat or IR signatures from a target. Generally the greater the difference between the target's heat signature and the ambient conditions, the greater the resolution and ease of targeting.

EO systems have a much better resolution than RF sensors, but suffer more from atmospheric effects such as attenuation and scintillation, and therefore normally have shorter detection ranges. The main trends in EO systems are:

- Increase in spectral bandwidth – hyperspectral. The EW implication is that soft-kill mechanisms (decoys and jamming) must operate over wider spectral bandwidths and be better spectrally matched to the platform being protected to be successful.
- Increase in special resolution (more pixels). This makes it more difficult to deceive EO devices, since they can more easily distinguish between real and false targets.

Obscurants (e.g. smoke) are the main countermeasures against EO sensors and decoys (e.g. spectrally matched flares) and Directable IR Countermeasures (DIRCM) against IR guided missiles

Figure 21: ATN PS15-4 Night Vision Goggles (left), SA-18 IR SAM (right).

Figure 22Luckyo 2.5 GBs laser communications link (left) and IRIS-T imagining IR missile (right).

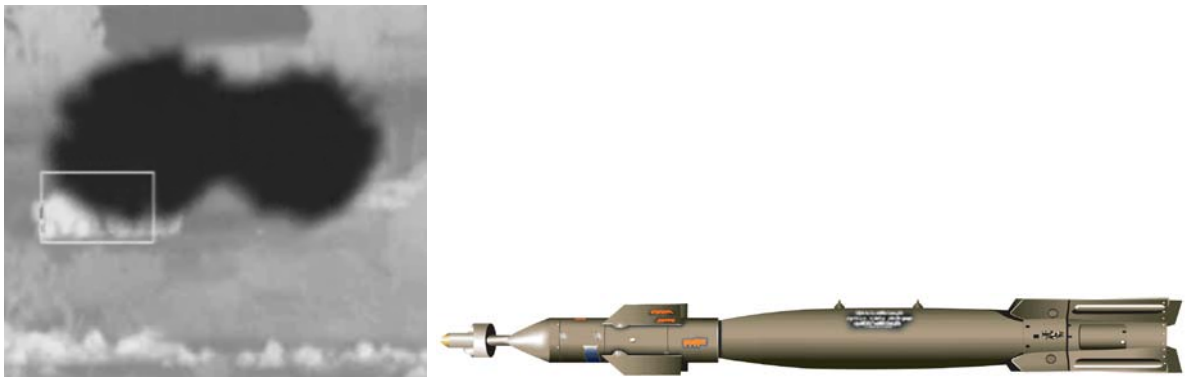

Figure 23: An Infrared image of smoke in the process of obscuring an armoured vehicle (left) against a Paveway II Laser Guided Bomb attack (right).

Figure 24: Saab's RBS 70NG man-portable laser guided air defence system.

The Electro-Optical equivalent SIGINT systems are devices like Visual (day and night), Infrared (near, middle and far) and Ultra Violet(UV) imaging systems and Infrared Search and Track (IRST) systems.

Figure 25: Examples of an IRST system on a fighter aircraft (left) and of the Thales Gatekeeper surveillance system (right).

2.6 RF Jammers

Jammers refer to both denial (e.g. noise) as well as deception (e.g. spoofing) of:

- Communication (voice and data-links).
- Radar (Synthetic Aperture Radar, Early Warning, Weapons allocation, Tracking, personnel, etc).
- Missile guidance links.
- RF Navigation Systems (GPS GLONASS, Galileo etc.).

These jammers can be man-portable, on-board or off-board weapons platforms (aircraft, ships, land vehicles, UAVs, etc.), active and be can be used in the roles of:

- **Stand-Off Jamming (SOJ)**. The platform performing this technique is outside the Air Defence (AD) system's sensor detection and effector range. This normally translates to long distances that the electromagnetic (EM) energy has to travel, which implies long propagation time delays and high-sensitivity receivers. Due to this, only denial techniques are effective.
- **Escort Jamming.** The platform performing this technique is outside the effectors' range, but potentially within the sensor's detection range. The EA platform normally has the same kinematic performance as the attack platforms, and accompanies the attacking platform throughout the mission, except for the final attack stage.
- **Self-Protection, Self Screening or Stand-In Jamming.** The platform performing these techniques is protecting itself throughout its application envelope, which will normally take it inside the sensor's detection range and associated weapon system's effector range.

An example of a Gripen aircraft with its self-protection EW suite is shown in Figure 26, whilst Figure 28 shows a stand-off communication and radar jammer with and Figure 29 a tactical communications EA system.

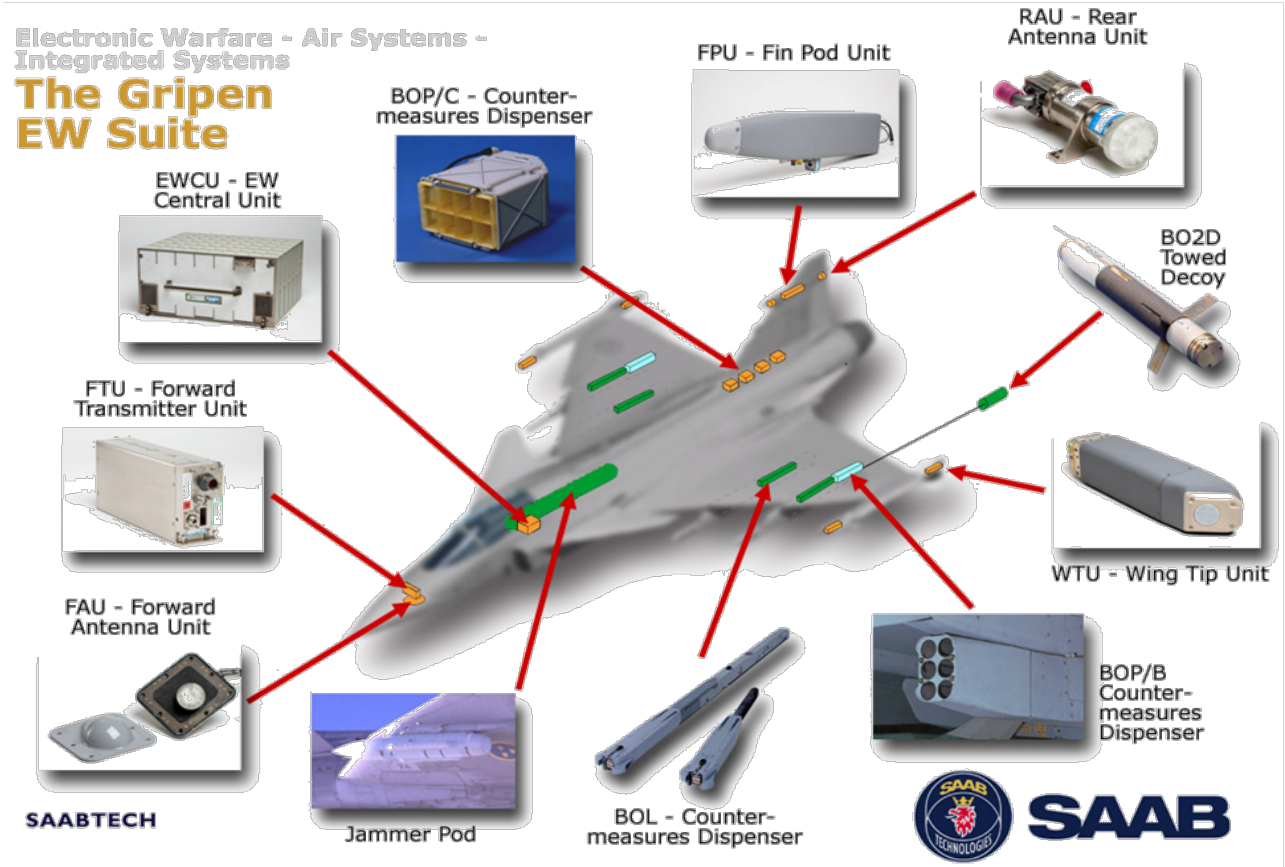

Figure 26: The complete Gripen EW suite, showing the ESM system, the decoy and dispensers as well as the built-in and pod mounted jammer – for self protection and escort jamming purposes.

Figure 27: The Next Generation Jammer is scheduled to replace the legacy ALQ-99 jamming pod (shown here on an f-18 Growler).

Figure 28: The Oryx shown in a stand-off communications and radar jamming configurations.

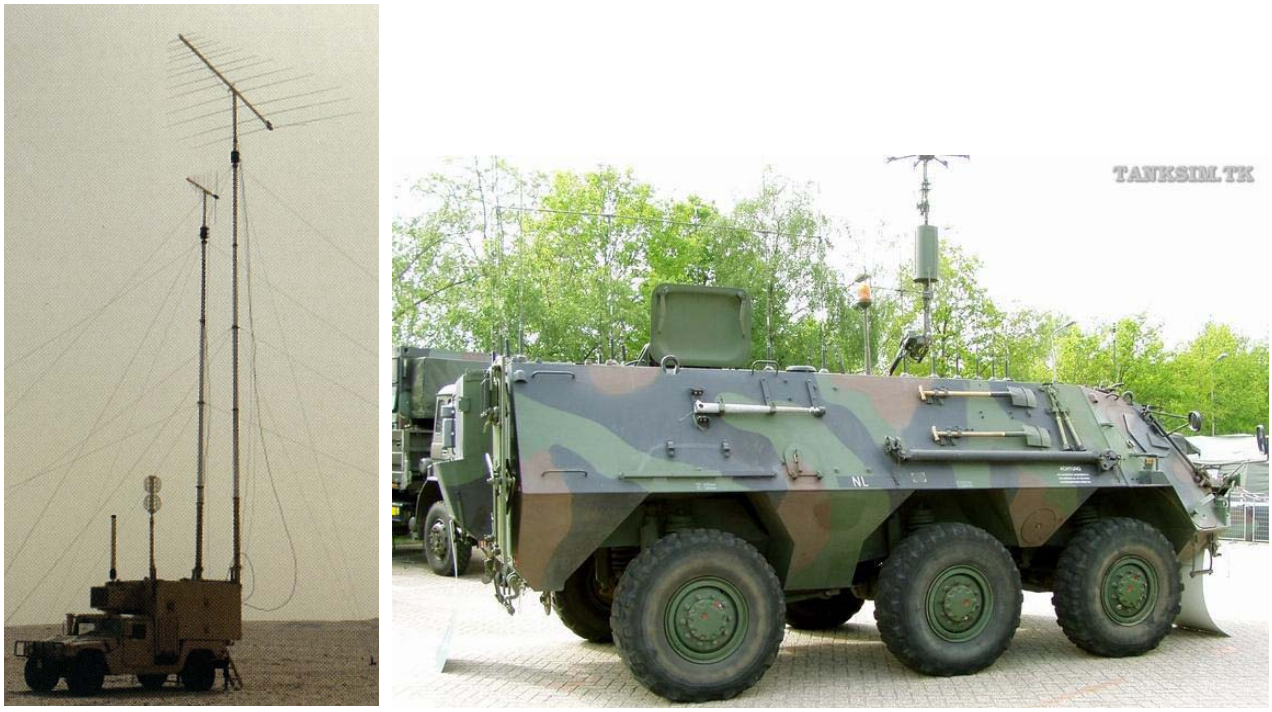

Figure 29: Tactical communication jammers.

Figure 30: General Atomics MQ-9 UAV with jamming pod.

Interoperability between own forces (and coalition forces) is crucial, and needs to be well planned and coordinated (this includes Emission Control – EMCON) to ensure mission success. It can easily happen that own sensors and data-links being jammed, or even that the one jammer jams the other jammer instead of the actual sensors.

2.7 Anti-Radiation Missiles

Anti Radiation Missiles (ARM) home-in on the transmissions from radar or communication signals. Radar ARMs need to be able to detect the antenna sidelobes since the target radar will probably be directed away from the missile most or all of the time. Most ARMs are designed to home in on surface emitters, although surface to air missiles do exist. This is the hard-kill part of Suppression of Enemy Air Defences (SEAD). Various developments are currently ongoing to give ARMs a HPM capability (instead of a High Explosive warhead). This will mitigate the homing accuracy requirements.

The new generation Advanced Anti-radiation Guided Missiles (AARGM) have the following typical features:

- Supersonic speed (mach 2+) and a range of more than 60 nm.
- GPS and inertial navigation system.
- Active millimeter wave (MMW) radar seeker.
- Digital anti-radiation homing seeker.
- An Integrated Broadcast Service Transceiver - allows the missile to receive targeting information from various platforms while it is still on the aircraft, and reports fusing status just prior to impact.

Countermeasures against ARMs are:

- Low power transmissions will not allow the ARM seeker to detect and lock on to the emitter.
- Bi/multi-static or networked emitters do not have the transmitter and receiver co-located. So at least the damage is localized to the transmitter and not the receiver, where the operators are normally positioned.
- Transmit intermittently (this has radar tracking filter implications) or use short-burst transmissions for communications.
- Use synchronised but geographically spaced dummy transmitters to confuse the homing missile's tracking loops.

Figure 31: USA's new generation Advanced Anti-radiation Guided Missiles (AARGM).

2.8 Directed Energy Weapons (DEW).

DEW can be divided into Lethal and non-Lethal weapons, as well as into RF and Electro-Optical systems. See the chapter 3 (DEW) for more information.

The only protection measures against EMP and HPM weapons is that of RF screening (Faraday cage). The problem comes where the RF energy couple into antennas, power-lines and communication cables. Batteries and fibre-optic communication cables can solve this partly, but if the system require antennas, this remains the main vulnerability point.

Another solution is that of redundancy. Keep a spare system (e.g. unconnected radio) in a Faraday cage, and replace the damaged unit after the HPM/EMP attack.

To counter Laser Guided Bombs (LGB), the defender can release smoke, which obscures the target, whilst manoeuvring away. This is obviously a time critical process and solution for a land vehicle or naval vessel. A faster response solution for these surface based targets is to use a DIRCM to illuminate the surface next to the target, conceptually creating a more lucrative (stronger) target for the LGB to home-in on.

Beam riding missiles track or follow the designator's laser beam until it hits the target. Although a LWR will be able to detect the laser, obscuration smoke is the only countermeasure. To prevent even this countermeasure, missile designers developed Off-Boresight beam-riders, where the laser illuminates a space next to the target, so the LWR cannot detect the laser, and the missile flies in with this known offset.

Lasers are active devices – transmitting energy – and hence can be detected by a Laser Warning Receiver (LWR) and therefore needs to be part of the EMCON planning.

High Power Acoustic devices used as non-lethal means to do crowd control, either by broadcasting a message, or by transmitting loud irritating sounds. The main counter to these type of acoustic devises is proper ear protection. With this in mind, these devices are seldom used as weapons, but mostly as propaganda/voice command devices.

2.9 Decoys

The aim of decoys is to present the aggressor with a more attractive target than the actual target, and thus either get the radar/missile to lock onto it, or break the lock if it was locked on. Decoys can be passive (e.g. chaff, corner reflectors, replicas, etc.) as well as active (flares, jammers, etc.) that gets deployed by or used instead of a platform. They are typically used in the EO/IR/Radar domain. are used in the self-protection role.

Although mostly used in the defensive role (chaff, flares and towed decoys), flying decoys can also be used offensively in the Suppression of Enemy Air-Defences (SEAD) role (for example the Miniature Air-Launched Decoy - MALD), where they would entice the enemy's radars to become active, and hence make themselves vulnerable to anti-radiation missile attacks.

Figure 32: A typical airborne chaff cartridge & chaff (left), and the Gripen's chaff/flare dispensers (1 to 4) shown on the right.

Figure 33: A Miniature Air-Launched Decoy (MALD) on an USAF F-18 (left), with an AN/ALE-55 Fibre-Optic Towed Decoy (FOTD) being launched from an USN F-4 (right).

Figure 34: Mirage dispensing IR Flares (left) and a visual decoy with IR properties (right).

Figure 35: LWR fitted to an Amphibious Assault Vehicle (AAV) – integrated to the smoke launchers.

The main counter for the self-protection decoys is to improve the victim sensor's resolution. Range and Doppler for the radars and spatially (imaging) for the EO sensors. On the other hand, from the protector's point of view, to make the platform requiring the protection as stealthy as possible – to give the decoys the best possible change to be more attractive.

2.10 SIGINT Systems

Signals Intelligence (SIGINT) is intelligence-gathering by interception of signals, intentionally or unintentionally transmitted, whether between people or computers - Communications Intelligence (COMINT), whether involving electronic signals not directly used in communication, Electronic Intelligence (ELINT), or combinations of the two. As sensitive information is often encrypted, signals intelligence often involves the use of cryptanalysis. Also, traffic analysis - the study of who is signalling whom and in what quantity - can often produce valuable information, even when the messages themselves cannot be decrypted.

The main advantage of SIGINT is that it is completely passive, and the originator of the information (Radar, communication system etc.) is not aware that the signal has been intercepted. Except for the Electronic Support Measures (ESM) case where the main purpose is to warn of an immediate threat or to control an Electronic Attack system, the main functions of SIGINT systems is that of Situational Awareness (SA) and to obtain the Electronic Order of Battle (EOB).

Much of the hardware and software required for the detection, identification, and location of threats in any EW battle management system comes from the world of spectrum management. Spectrum analyzers are best suited for making very accurate measurements of signals – but is not suitable for wide instantaneous frequency coverage, real-time and jammer control applications. Monitoring receivers make rapid measurements of signals in real-time (including demodulation) and monitor them either locally or remotely and can account for signals variations over time. Depending on the architecture, this type of receivers can result in a high probability of intercept.

Direction finding (DF) systems are an essential component, as they use special antennas that can provide bearing information for the signal of interest. Software combines bearings from multiple networked DF receivers (triangulation), automatically calculating and plotting transmitter location and displaying the information in variety of ways, including on a digital map. These DF stations can be fixed, mobile, or portable to provide maximum flexibility. Many instruments can be combined into a single system with a unified interface and automated measurement capabilities. The result is the ability to deploy a system on any scale, from locally to regionally, or even nationally.

Examples of ESM systems are Radar Warning Receivers (RWR) and Laser Warning Receivers (LWR).