DOI 10.5162/ettc2018/6.2

Sabotage and Disclosure of Flight Test and other reasons & methods to intercept, jam or spoof telemetry

Michael Niewöhner
COMPLETER.NET Sales & Engineering GmbH,
www.completer.net,
Michael.Niewoehner@completer.net

Abstract

The paper deals with the reasons for jamming and spoofing telemetry and GPS, but also with methods from the world of electronic warfare, which may not (yet) be relevant or known in the domain of flight test. The lecture will also give a closer look at and deeper insight in the possibilities of intercepting and evaluating telemetry data and the possibilities that arise from this, even if the contents are encrypted. FISINT (Foreign Instrumentation Signals Intelligence) is an area of signals intelligence (SIGINT), that plays a subordinate role in electronic warfare and military intelligence but is very interesting to intelligence agencies and beneficial to other organizations.

Key words: Jamming, Spoofing, Telemetry, GPS, FISINT

The world of Electronic Warfare (EW) and Signals Intelligence (SIGINT)

Electronic warfare (EW) is any action involving the use of the electromagnetic spectrum or directed energy to control the spectrum, attack of an enemy, or impede enemy assaults via the spectrum. The purpose of electronic warfare is to deny the opponent the advantage of and ensure friendly unimpeded access to the EM spectrum.

EW can be applied from air, sea, land, and space by manned and unmanned systems, and can target humans, communications, radar, or other assets. Electronic Warfare has several subdivisions.

Electronic Attack (EA)

EA involves the use of electromagnetic energy, directed energy, or anti/radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability. In the case of electromagnetic energy, this action is referred to

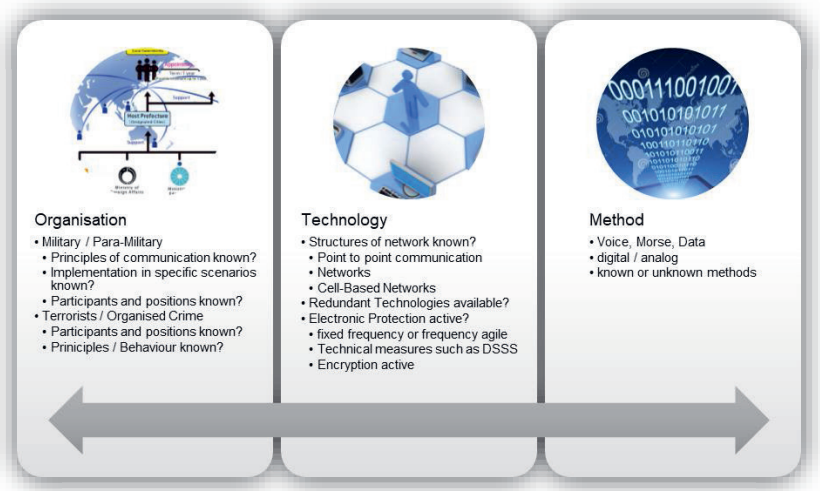

Figure 1: Taxonomy for Electronic Attack Measures

as jamming and can be performed on communications systems or radar systems.

Electronic Protection (EP)

EP involves actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability.

Electronic Warfare Support (ES)

ES is involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for immediate threat recognition, targeting, planning, and conduct of future operations.

These measures begin with systems designed and operators trained to make Electronic Intercepts (ELINT) and then classification and analysis broadly known as Signals intelligence from such detection to return information and perhaps actionable intelligence to the commander.

The purpose of ES tasking is threat recognition and other tactical actions such as threat avoidance and homing. However, the same assets and resources that are tasked with ES can simultaneously collect intelligence that meets other collection requirements.

Signals Intelligence (SIGINT)

SIGINT is derived from the direction finding, processing, and analysis of intercepted enemy communications, electronics and foreign instrumentation signals. It provides the commander valuable, near-real-time intelligence on enemy intentions, readiness status, and disposition by intercepting and locating enemy command, maneuver, fire support, reconnaissance, and logistic emitters.

Any nation has a political interest to gain information superiority against its potential threats. Therefore, most of them operate strategic intelligence systems with monitoring and locating capabilities as well as evaluating and reporting functions.

The vital interest of nations is formation of strategy, policy, and military plans and operations at the national and theatre levels. Strategic intelligence concentrates on the national political, economic, and military considerations of states or nations. It identifies the support for governments, the ability of states or nations to mobilize for war, the national political objectives, and the personalities of national leaders. It predicts other nations' responses to own theatre operations.

Intercepting and Locating Telemetry emissions

Foreign instrumentation signals intelligence (FISINT) was formerly known as TELINT or telemetry intelligence. FISINT entails the collection and analysis of telemetry data from a missile or aircraft tests.

Telemetry communication is mainly one-directional transmission from instrumented device to a telemetry receiver in a control station (mobile/fixed). Different applications are Meteorology, Oil and gas industry, Motor racing, Transportation, Agriculture, Water management, Swimming pools, Energy monitoring, Resource distribution, Medicine/Healthcare, Fishery and wildlife research and management, Retail, Energy providers, Falconry, Law Enforcement and Mining. All of those are of minor interest for intelligence authorities. Of more interest are the usage in the Aerospace, Defense and Space Domain.

Telemetry is used in complex systems such as missiles, RPVs, spacecraft, oil rigs, and chemical plants since it allows the automatic monitoring, alerting, and record-keeping necessary for efficient and safe operation.

Space agencies such as ISRO, NASA, ESA and other agencies use telemetry and/ or tele-command systems to collect data from spacecraft and satellites. Telemetry is vital in the development of missiles, satellites and aircraft because the system might be destroyed during or after the test. Engineers need critical system parameters to analyze and improve the performance of the system. In the absence of telemetry, this data would often be unavailable.

Space Science

Telemetry is used by manned or unmanned spacecraft for data transmission. Distances of more than 10 billion kilometers have been covered, e.g., by Voyager 1.

Rocketry

In rocketry, telemetry equipment forms an integral part of the rocket range assets used to monitor the position and health of a launch vehicle to determine range safety flight termination criteria. Problems include the extreme environment (temperature, acceleration and vibration), the energy supply, antenna alignment and (at long distances, e.g., in spaceflight) signal travel time.

Flight testing

Today nearly every type of aircraft, missiles, or spacecraft carries a wireless telemetry system

as it is tested. Aeronautical mobile telemetry is used for the safety of the pilots and persons on the ground during flight tests. Telemetry from an on-board flight test instrumentation system is the primary source of real-time measurement and status information transmitted during the testing of manned and unmanned aircraft.

Intercepted telemetry was an important source of intelligence for the United States and UK when Russian missiles were tested. Telemetry was also a source for the Russians, who operated listening ships in Cardigan Bay to eavesdrop on UK missile tests performed in the area.

Telemetry communication in aircraft / missile testing is according to IRIG 106 standard an FQPSK / SOQPSK signal with a PCM signal encoded. Such telemetry mainly operates in L-Band, S-Band and C-Band. Nowadays it moves more and more in the direction of C-Band. Due to the fact, that transmission is one-directional, there is no possibility for error-correction. Consequently, the requirements for the quality of the signal are high.

The users of this sort of telemetry are Air Force Bases, Aircraft Industry and general defense industry.

Evaluating Telemetry emissions

Telemetry emissions are mainly encrypted. This should secure the content of the transmitted data. What is not known widely is, that this does not protect against interception, analysis and evaluation. Putting together several intelligence sources, a clear picture of the monitored emitter could be put together.

By triangulation, the position of an emitter can be identified very accurate. By comparing different positions over time, the flying speed can be calculated and tracked. With some intelligence systems, even the flying height (elevation of the signal compared to position) can be found out.

The fact, that a telemetry emission is sending continuously makes it easy to track the exact flying route of the aircraft. If communication is bi-directional, the structure and setup of ground stations could be disclosed. As transmitted power is relatively high, and the object is transmitting from a high position, the interception station can be far away from the aircraft.

Coming back to the encryption, the content is relatively safe against real-time decryption. Nevertheless, all traffic can be recorded and decrypted with high performance computers later.

Finally, all such information helps enemy forces to plan jamming and spoofing procedures for future flight tests.

Electronic Attack (EA) for telemetry and GPS

Jamming is the deliberate radiation, re-radiation, or reflection of electromagnetic energy for disrupting enemy use of electronic devices, equipment, or systems. It degrades communications by reducing or denying the enemy's ability to pass key information at critical times and can cause enemy operators to become irritated, confused, or misled during offensive, defensive of retrograde operations. When applied successfully, jamming can contribute to the failure of those actions which depend on communication using the electromagnetic spectrum.

ES is the primary source of information used to identify and develop jamming targets. It helps to

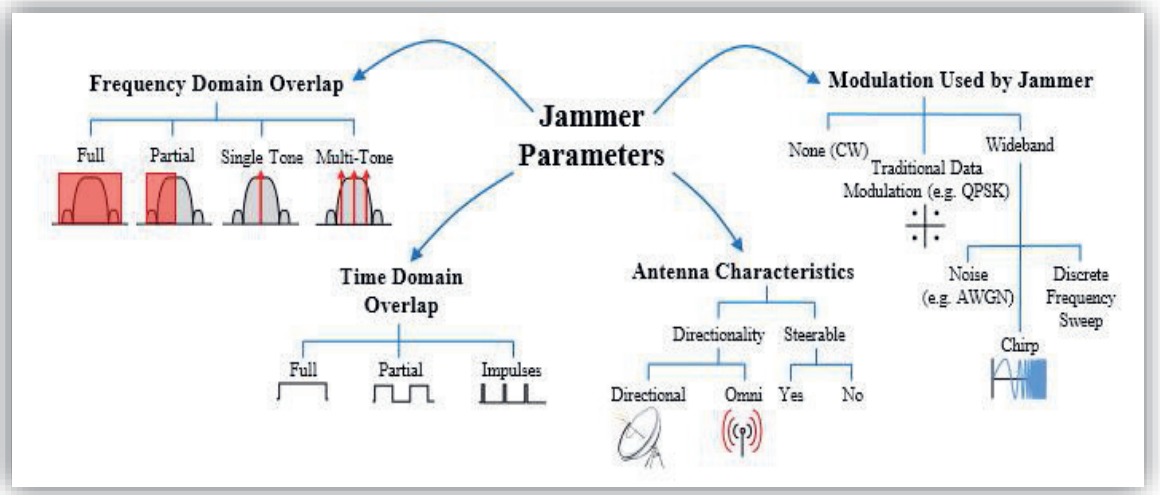

Figure 2: Jammer Parameters

identify the enemy's locations and intentions and thereby identify valuable jamming targets. Indiscriminate jamming wastes resources could impede friendly communications or could attract countermeasures such as artillery fire. Consequently, jamming operators/ systems need to know exactly who, what frequency, where and when to jam.

Enemy nets, which routinely pass information of intelligence value, should be identified and monitored, other nets, such as those having a highly tactical value to the enemy but little or no intelligence value to friendly forces, could be attacked with jammers. Enemy secure communications may also be jammed with the intention of drawing the enemy into clear voice communication.

The process may be along the following lines. An intercept DF network picks up a transmission that is determined not to be from own forces or from neutral operators. Analysis identifies specific parameters for the situation such as:

- transmission central frequency
- 3-dB and IO-dB bandwidth
- modulation scheme in use
- signal strength at the detecting receiver(s)
- direction or localization position if known
- times of transmissions
- how frequently the channel is used
- duration of transmissions
- association with other systems (activity analysis)

This is where the behavior of an enemy network is studied to determine its structure specific identifying features such as frequency instability, operator Morse behavior, the same voice on successive intercepts or transmission of formatted messages.

These factors can be analyzed with the benefit of knowledge already known, such as association with known weapon systems and technical parameters of known enemy systems. The detected transmission may for example be associated with a specific air defense command system or be of a type known to be used for command and control. Transmission behavior may also reveal the relative importance of the channel. If is frequently used, then it may be an important command and control channel. If it is noticed before artillery shells arrive, then it may be the artillery command network. If troop movements are correlated with the transmissions, then again it may be a command net. If other transmissions on other frequencies follow on quickly after the initial transmission, then again it might be part of the command network and so on.

For effective jamming operations, the planning function needs all information about function, position in a net, position on the battlefield and ability to affect the combat plan. For those reasons, the planning of jamming operations shall be in responsibility of the tactical leader.

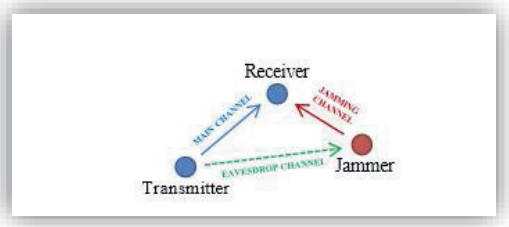

Figure 3: Jamming Principles

One main principle that regularly gets forgotten is that it is possible to deny the interception of a signal by jamming, but not the transmission.

Different methods of jamming are briefly explained in the following section.

Spot Jamming

Spot jamming occurs when a jammer focuses all its power on a single frequency. While this would severely degrade the ability to track on the jammed frequency, frequency agile radar would hardly be affected because the jammer can only jam one frequency. While multiple jammers could possibly jam a range of frequencies, this would consume a great deal of resources to have any effect on frequency-agile radar and would probably still be ineffective. Spot jamming is used to jam a pre-selected frequency that has been determined as a target of interest.

Once the transmission is determined to be a high priority target, an EW tasking mission may be issued to the spot jammer. This will include the technical parameters and any other pertinent information, such as the duration of the jamming task. The actions of the jammer detachment will be to tune the jammer to the required frequency and bandwidth if this is adjustable. The antenna will be pointed in the direction of the enemy receiver. Before jamming, the channel can be listened on to determine whether it is still transmitting (there is no point in jamming an unoccupied channel). If it is still in use, then jamming can commence. The jamming can consist of un-modulated or modulated noise. Un-modulated noise will raise the noise floor of the enemy receiver, preventing them being able to communicate. Modulated noise does the same thing but also disrupts audio reception of the

transmission signal making it impossible for the receiving operator to hear the message. Periodically, the jamming signal will be turned off so that the jammer operators can listen to determine whether the enemy is still using the channel or have changed to a different one.

Sweep Jamming

Sweep jamming is when a jammer's full power is shifted from one frequency to another. While this has the advantage of being able to jam multiple frequencies in quick succession, it does not affect them all at the same time, and thus limits the effectiveness of this type of jamming. Although, depending on the error checking in the device(s) this can render a wide range of devices effectively useless

Barrage Jamming

Barrage jamming is the jamming of multiple frequencies at once by a single jammer. The advantage is that multiple frequencies can be jammed simultaneously; however, the jamming effect can be limited because this requires the jammer to spread its full power between these frequencies, as the number of frequencies covered increases the less effectively each is jammed.

Barrage jamming is the simplest form of jamming and is usually defined as a jammer which transmits noise-like energy across the entire portion of spectrum occupied by the target with 100% duty cycle in time. Thus, it is non-correlated and non-protocol-aware. Barrage jamming has been shown game theoretically and information theoretically to be the best a jammer can do in the absence of any knowledge of the target signal.

Barrage jamming is used to deny the enemy of the use of a portion of spectrum. This can be because enemy forces are frequently changing channels or that they are using full frequency hopping systems. Compared to spot jammers, barrage jammers need to supply jamming power into many channels rather than just one. On the rather simplistic assumption that the barrage jammers deliver the same jamming power into each jammed channel and that the effective jamming power has the same effect as the spot jammer, it is easy to calculate the power reduction for the number of channels jammed.

Partial Band Jamming

When jamming a single-carrier signal, it has been shown that jamming gains can be achieved by not jamming the entire signal in the frequency domain, but rather jamming a fraction of the signal. This is known as partial-band jamming, and it is usually considered a non-correlated jamming attack because the jammer transmits continuously in time. Performing partial-band jamming against an Orthogonal Frequency-Division Multiplexing (OFDM) waveform does not make sense because strong forward error correction could allow the data to be reconstructed from the unjammed subcarriers.

Responsive Jamming

Responsive jammers have an RF detection capability that allows them to scan for threats and jam those of interest.

Adaptive Jamming

Adaptive jamming is an extension of responsive jamming but with the potential to jam several targets at the same time. It provides an improved method to achieve the same effects as barrage jamming but in a far more focused manner.

Repeater Jamming (Follower Jamming; Responsive Jamming; Reactive Jamming)

Repeater jamming is the simplest form of correlated jamming when the jammer has no knowledge of the protocol. In repeater jamming, the jammer transmits when it senses energy on the channel. This may be in the form of the jammer re-transmitting what it receives with noise added or sensing a series of subchannels and transmitting noise when it senses energy on one or more subchannels.

Smart Jamming (Pilot jamming; Equalization Jamming)

Smart jamming is the term used to describe jamming aimed at network vulnerabilities rather than simply raising the noise floor or causing unacceptable audio or data performance. Methods of smart jamming are aimed at types of network such as GSM, UMTS, paging systems and many others.

A smart jammer designed to attack GSM will have less or even no effect against other networks that may be present, so it is important to be able to identify the exact type of network for it to work. Some network vulnerabilities include: pilot channels; synchronization channels, time slots or data; paging channels or time slots; error correction checksums; acknowledgement or Not Acknowledged messages.

The purpose of smart jamming is to prevent normal performance of a network. This may be by denying subscribers the ability to log on to the network by causing base station overload, disrupting signals telling subscribers that they have a call, preventing successful call initiation or disrupting communications once a link is established by causing the system to successively re-send packets of data due to Not Acknowledged or error checksum faults. This

type of jamming is relatively new compared to the other methods.

Equalization jamming involves targeting any mechanism related to equalization. Known data symbols (reference symbols) are inserted into the transmitted waveform to estimate the channel's frequency response and equalize the effect of the channel at the receiver prior to demodulation. These known symbols are called pilot symbols in multicarrier communications such as OFDM or single-carrier frequency division multiple access (SC-FDMA) and channel sounding symbols in multiple-input and multiple-output (MIMO) systems. For example, in OFDM, pilot tone jamming is simply the process of jamming pilot tones, which may reside on certain subcarriers (in the case of 802.11) or may be multiplexed in time and frequency with data (in the case of LTE).

Pilot jamming is protocol-aware because the jammer must know where the pilots are located. If the pilots occur on a dedicated subcarrier then the attack is non-correlated, but if they are multiplexed in time then it must be correlated to surgically jam the pilots. It was found that pilot jamming can be energy efficient and similar degradation in target receivers Bit Error Rate (BER) can be achieved using roughly one-tenth of the energy.

The pilot jamming process is similar in the case of SC-FDMA, which is the single-carrier variant of OFDM and used in the uplink of the LTE air-interface. In MIMO systems, known reference signals are used for channel sounding and thus can be jammed if they are known by the jammer a priori. Another special kind of equalization jamming attack involves jamming the cyclic prefix (CP) of a multicarrier waveform such as OFDM or SC-FDMA. These waveforms use a CP to mitigate inter-symbol interference (ISI) and inter-channel interference (ICI). CP also ensures that the convolution of the channel impulse response with the modulated symbols has the form of a circular convolution, which is essential for simple one-tap equalization in the receiver. These crucial roles played by the CP make SC-FDMA particularly vulnerable to jamming attacks through CP.

Synchronization Jamming

For a communications link to function, the receiver must synchronize to the incoming signal in both time and frequency. To aid in this task, a synchronization signal, or synchronization symbols, are usually designed into the PHY layer protocol. For example, in LTE there are two different synchronization signals that each appear every 5ms. Synchronization jamming is simply the process of surgically jamming one or more synchronization signals. This jamming technique is unique in the sense that it may only prevent radios from establishing a communications link, and thus it won't cause immediate Denial of Service (DOS).

However, synchronization signals tend to be very sparse with respect to the entire signal, thus providing a significant jamming gain. Synchronization jamming must be protocol-aware, to know where the synchronization signal is located. It must be time-correlated, assuming the synchronization signal is multiplexed in time with data and other signaling.

AGC Jamming

The automatic gain control (AGC) mechanism in a receiver adjusts the input gain in such way that the received signal comes in at a proper level to best utilize the range of the analogue-to-digital converter(s).

A jamming attack that targets the AGC mechanism is one that uses a very low duty cycle (e.g.,2%) but with extremely high instantaneous power. By not transmitting continuously, the jammer can save power and remain harder to detect in some situations. AGC jamming is non-correlated, although the specific period and duty cycle used are important parameters. Aside from the assumption/knowledge that the target receiver uses AGC, it is non-protocol-aware.

Protocol-Aware Jamming

The term protocol-aware simply means the jammer is aware of the protocol of the target signal. Information about the signal's protocol is obtained during the Signal Awareness step and used in the Attack Selection decision-making. For example, the jammer may identify that a signal is a Wi-Fi or LTE signal, which due to the open nature of specifications allows the jammer to know almost everything about the PHY and MAC layers.

A jammer could use a priori knowledge of the protocol to exploit weaknesses in the protocol and launch a jamming attack that is more effective and may be harder to detect than non-protocol-aware jamming. For example, the jammer may only know a signal uses OFDM with pilots in certain locations, which would be considered protocol-aware if it knew exactly where the pilots were placed.

In most wireless protocols, the data takes up the largest portion of time and frequency resources. Thus, when targeting something besides the data, it will likely result in an attack that uses less power and is harder to detect (if the targeted mechanism is essential for communications). Possible mechanisms that could be targeted in a

protocol-aware attack (taken from open literature) include Control channels/subchannels, Control frames or packets (e.g., ACKs), Pilots (reference symbols), Synchronization signals and Cyclic prefix in OFDM.

Possible protection measures

There are different possibilities to protect own flight tests against jamming and spoofing. First, the level of confidentiality should be very high. As explained, jamming should be planned and if planning time is reduced by missing a priori knowledge like flight plans, the probability of being jammed is reduced significantly. But this is probably not new knowledge.

Technically it is most beneficial to have alternative communication means on board, as every military unit should do. If one is jammed, the system can take evasive measures and switch to another communication means.

Also, it is helpful to raise own power of the received signal. As explained, the jammer can deny receiving but not transmitting. So, if the original signal is much stronger than the jamming signal, the probability of being jammed is lower. This could be done by high power emitters, but on other hand, this would make it easy to intercept and thereby evaluate your flight test. Another possibility is, to operate a receiver network in the flight test area, so that the aircraft has a short distance to the receiver station. Therefore, you would need more small, remote controlled and transportable receivers/ antennas for reasonable prices.

Resume

Military intelligence and intelligence agencies are interested in monitoring telemetry communication, as they gain insight on new weapon system development, the structure and capabilities of foreign forces and generate target knowledge at a very early state. Jamming and Spoofing are methods to deny beneficial usage of the electromagnetic spectrum.

In Flight Test Surrounding, currently the risk of being jammed is much smaller than the risk of being intercepted and analyzed. However, sometimes you have malfunctioning in your flight test campaigns it might also be a smart, protocol-aware jammer and you will be wondering what happened. Especially as the occurred problem is not reproduceable in the lab.

Expressions

[1] **Intelligence collection management (ICM)** is the process of managing and organizing the collection of intelligence from various sources. The collection department of an intelligence organization may attempt basic validation of what it collects but is not supposed to analyze its significance.

[2] **Signals Intelligence (SIGINT)** results from collecting, locating, processing, analyzing, and reporting intercepted communications and non-communications (for example, radars) emitters. SIGINT provides the commander with valuable, often NRT intelligence and targeting information on enemy intentions, readiness status, and dispositions by intercepting and locating enemy command, maneuver, fire support, reconnaissance, air defense, and logistics emitters. SIGINT operations require efficient collection management and synchronization to effectively overcome and exploit enemy efforts to protect his critical communications and weapons systems through emissions control, communications operating procedures, encryption, and deception. SIGINT is subdivided into: communications intelligence (COMINT); electronic intelligence (ELINT); and Foreign instrumentation signals intelligence (FISINT).

[3] **FISINT (Foreign instrumentation signals intelligence)** is a sub-category of SIGINT, monitoring primarily non-human communication. Foreign instrumentation signals include (but not limited to) telemetry (TELINT), tracking systems, and video data links. TELINT is an important part of national means of technical verification for arms control.

[4] In military telecommunications, the terms **Electronic Support (ES)** or Electronic Support Measures (ESM) describe the division of electronic warfare involving actions taken under direct control of an operational commander to detect, intercept, identify, locate, record, and/or analyze sources of radiated electromagnetic energy for the purposes of immediate threat recognition (such as warning that fire control RADAR has locked on a combat vehicle, ship, or aircraft) or longer-term operational planning. Thus, Electronic Support provides a source of information required for decisions involving Electronic Protection (EP), Electronic Attack (EA), avoidance, targeting, and other tactical employment of forces. Electronic Support data can be used to produce signals intelligence (SIGINT), communications intelligence (COMINT) and electronics intelligence (ELINT).