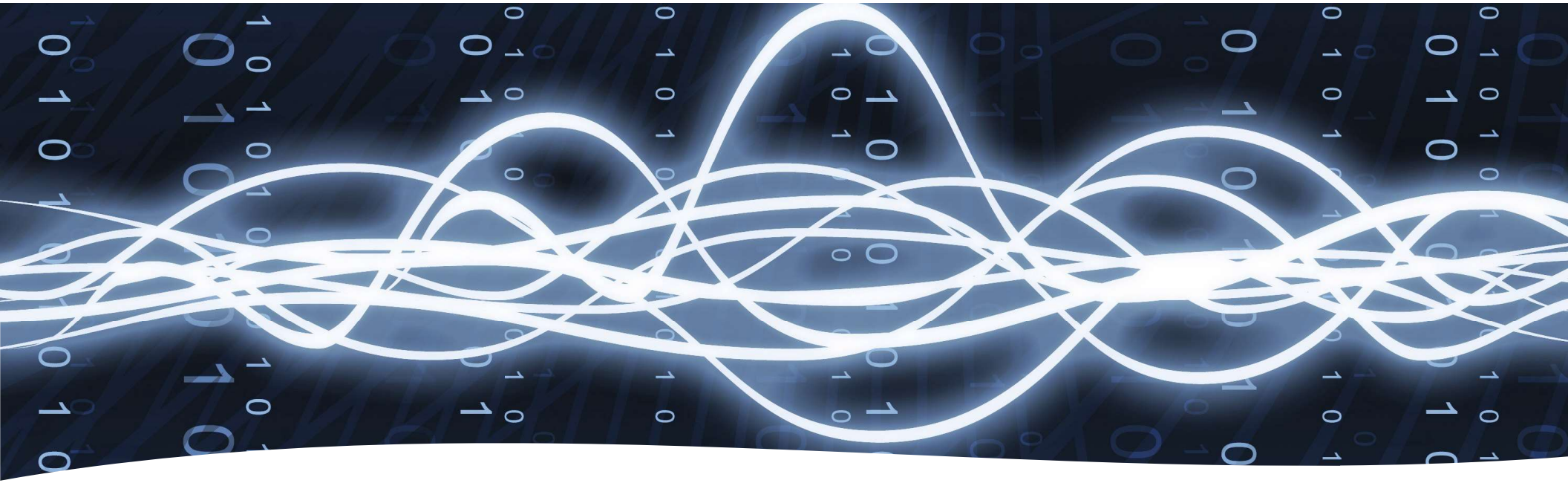


Part 3

Signals Intelligence (SIGINT) Technical Principles

TONEX

Targeting

SIGINT is conducted in response to requirements for intelligence from different agencies and policy makers.

Based on these priorities, agencies in the Intelligence Community (IC) , design and develop mechanisms for collecting information in different locations, information that will meet the wide variety of policy maker requirements.

To the extent possible, collection mechanisms are consolidated for greater efficiency between the various intelligence agencies.

Thus, a given collection mechanism may provide information that is useful for a variety of different topics. This process seeks to avoid the development and deployment of collection mechanisms individually for each target, an approach that would be inefficient and expensive.

SIGINT Targeting

SIGINT supports targeting by providing key operational and locational intelligence on enemy C2 operations and facilities, weapons systems, force compositions, and dispositions.

Information provided through SIGINT can identify high value and high payoff targets and help develop options for attacking these targets.

SIGINT also supports all-source intelligence gain and loss assessments of potential enemy targets.

Example of Targeting: Military Targeting Based on Cellphone Location

- Signals Intelligence (SIGINT) including cellphone and SIM card data – to locate and kill suspected militants in Afghanistan, Iraq, Pakistan, Somalia, and Yemen.
    - It has long been public knowledge that US operations use cell phone SIGINT in this way to carry out military strikes (since at least 2004)

ELINT Targeting

- ELINT is information derived primarily from electronic signals that do not contain speech or text (which are considered COMINT).

Intercept Management

- Modern SIGINT systems
- Larger intercept aircraft
- Target analysis and planning
- Once the decision to target is made, the various interception points need to cooperate, since resources are limited.
- Knowledge of physics and electronic engineering further narrows the problem of what types of equipment might be in use.
- Long-range search radars
- Short-range fire control radars

Signal Detection

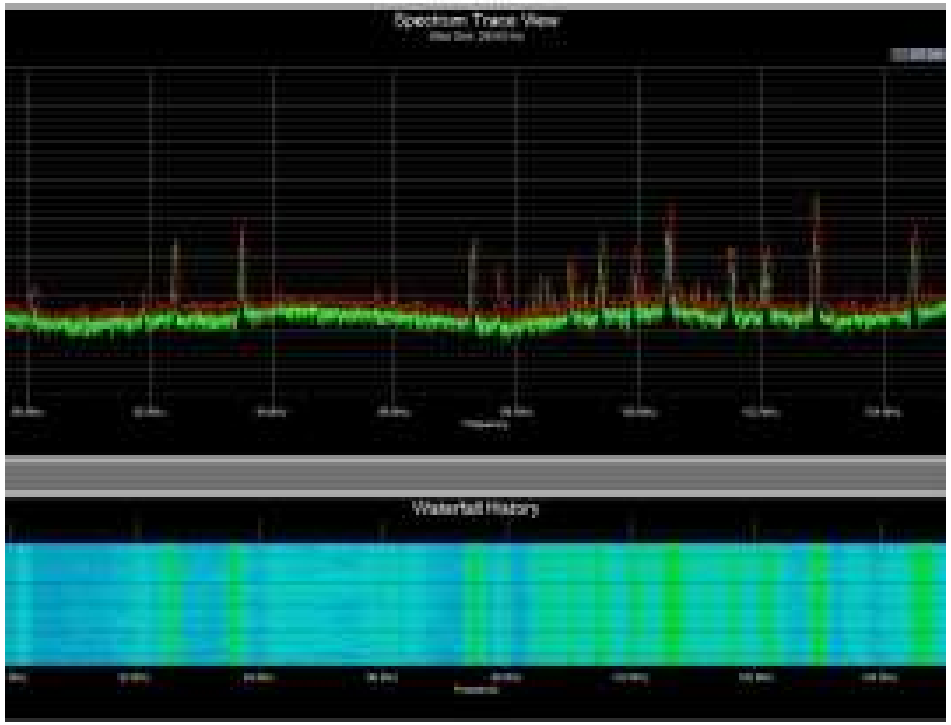
- Even if a signal is human communications (e.g., a radio), the intelligence collection specialists must know it exists.
- If the targeting function described above learns that a country has a radar that operates in a certain frequency range, the first step is to use a sensitive receiver, with one or more antennas that listen in every direction, to find an area where such a radar is operating.

- Once the radar is known to be in the area, the next step is to find its location.

- Simplified spectrum analyzer display of superheterodyned, amplitude modulated signals.

Simplified Spectrum Analyzer

- If operators know the probable frequencies of transmissions of interest, they may use a set of receivers, preset to the frequencies of interest.
- These are the frequency (horizontal axis) versus power (vertical axis) produced at the transmitter, before any filtering of signals that do not add to the information being transmitted.
- Received energy on a particular frequency may start a recorder and alert a human to listen to the signals if they are intelligible (i.e., COMINT).

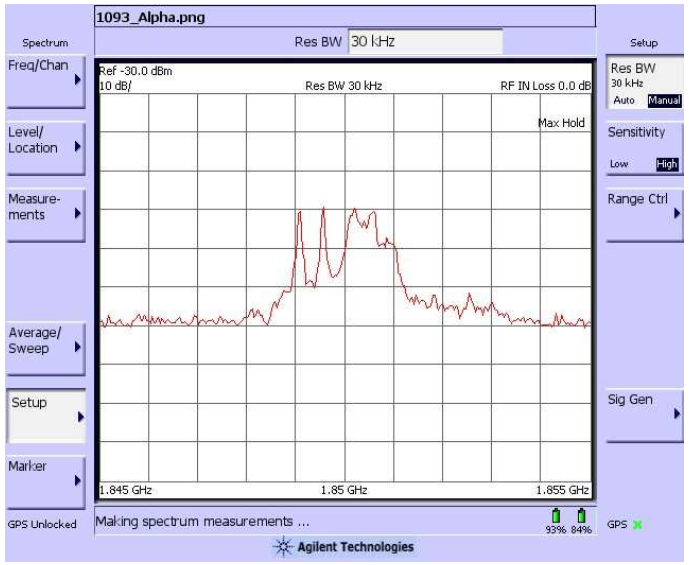


Introduction to Spectrum Analyzers

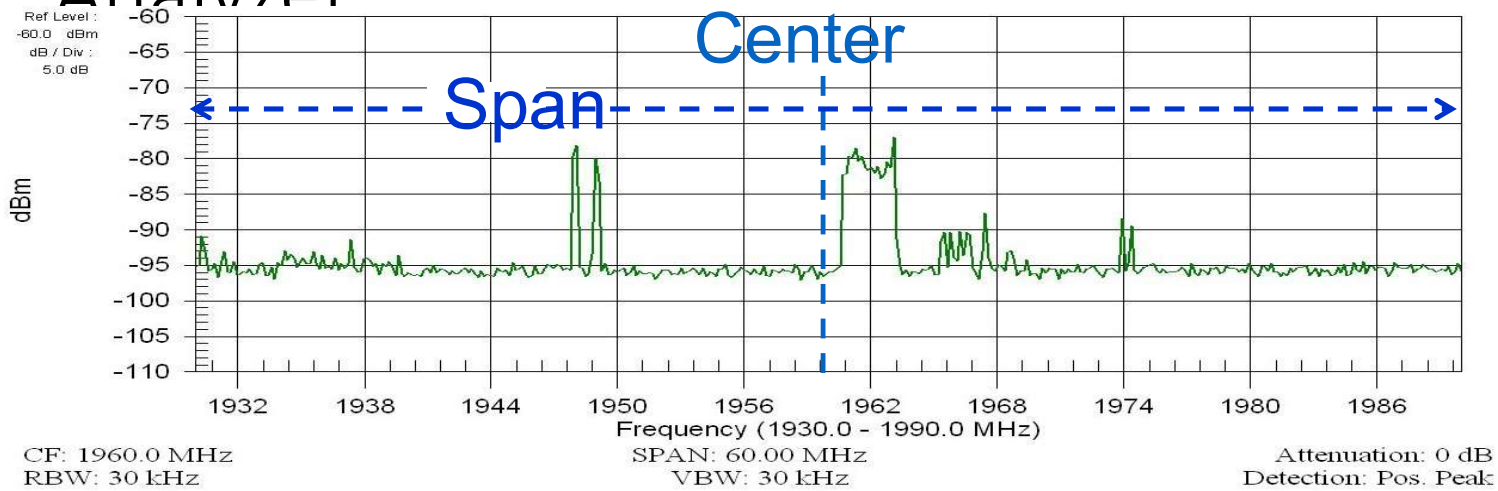
- There are two main test tools that allow us to “see” radio signals
  - Oscilloscopes display a living graph of signal strength (vertical) vs time (horizontal) – our window into the world of signals in the time domain
  - Spectrum Analyzers display a living graph signal strength (vertical) vs frequency (horizontal) – our window into the world of signals in the frequency domain
- Spectrum analyzers are especially valuable for measuring many key characteristics of radio signals
  - Frequency
  - Power
  - Occupied bandwidth
  - Noise, harmonics, intermodulation products, spurious signals
  - Frequency response of filters and networks

The Display of a Spectrum Analyzer

- The job of a spectrum analyzer is to show a plot of signal amplitude against frequency
  - The vertical scale usually has ten major divisions (amplitude), with adjustable db per division
  - The horizontal scale usually has ten major divisions (frequency), low frequency on the left and high on the right, with adjustable center frequency and MHz. per division

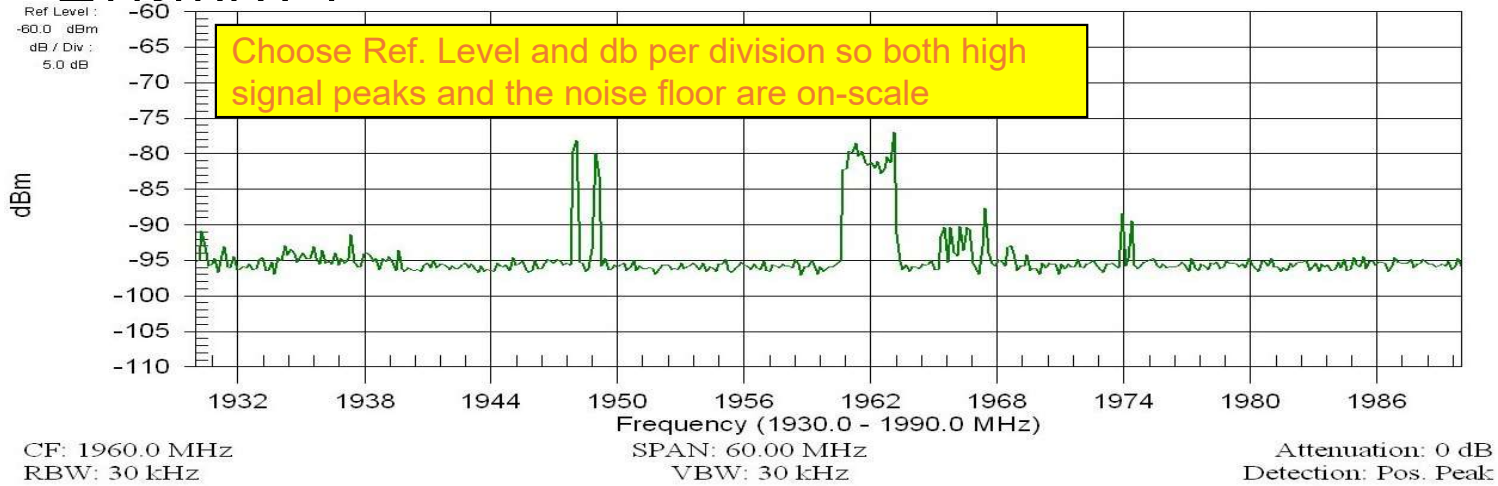


Setting the Frequency of a Spectrum Analyzer



- To set the frequency of a spectrum analyzer, two independent selections must be made.
  - Center Frequency – normally the frequency of the signal
  - Frequency Span – the width of frequencies to be monitored
- Normally the span should be set wide enough to see all the sidebands of the signal you are watching
  - In interference cases, you may want to watch a wider range
- Many spectrum analyzers also allow an alternative way to set the frequencies – just set the two “edge” frequencies between which you want to monitor – the “start” and “stop” frequencies.

Adjusting the Gain of a Spectrum Analyzer



- The gain setting of a spectrum analyzer must be appropriate for the strength of the signal you are trying to see
  - For strong signals, lower gain is needed, and it may be necessary to switch in attenuation to prevent overloading of the spectrum analyzer and possible internal intermodulation
  - For weak signals, higher gain is needed so that the desired signal will be visible on the scale
  - To see a weak signal in the presence of very strong signals, an external bandpass filter may be needed ahead of the spectrum analyzer to keep the strong signals from overloading the analyzer

Setting Scan Rate on a Swept Spectrum Analyzer

- A swept spectrum analyzer is really a narrow-band radio receiver whose frequency rapidly scans through the selected span of frequencies while the received power displays on the vertical axis.
- The speed of scanning is very important
  - The faster the scan, the faster the measurement can be made
- However the feasible rate of the scan is limited by two other factors inside the spectrum analyzer
  - the IF bandwidth of the analyzer's internal swept receiver
    - Sometimes called "IF bandwidth"
  - the bandwidth of the baseband filter used to drive the display
    - Sometimes called "video bandwidth"
- Many analyzers automatically select scan rate and the two bandwidths for the user, taking into account the width of the frequency span being displayed
  - For most measurements, these default values are fine

Setting Filter Bandwidths of a Spectrum Analyzer

- The IF filter governs the frequency resolution of the spectrum analyzer
  - a narrow bandwidth will allow resolving close-together signals
  - However narrow filters don't respond to signals as quickly as wide ones, making it necessary to scan slower
- The video filter provides some "averaging" of the signal, helping to reduce the effects of noise and let weaker signals be noticed.
  - However, video filtering also limits the speed at which the spectrum analyzer can scan.
- When using narrow bandwidths the scan rates can be objectionably slow.
  - In this case, reconsider how wide a span really needs to be scanned. If you can reduce the span width, the time per scan speeds up accordingly.

Advanced Features: Markers and Counters

- Some spectrum analyzers allow setting up “markers”
  - A marker is a visible line or label to mark a certain frequency and the power level on it
    - The marker can be manually adjusted to get a very precise reading of frequency and strength of a signal being watched
    - Some analyzers also provide automatic “marker to peak” settings, to reveal power and frequency of a signal quickly without the user having to manually tune the marker
    - Many spectrum analyzers also provide “marker to center” features which automatically change the center frequency of the analyzer to the current position of the marker
    - Many analyzers have multiple-marker capability
    - Many analyzers also allow marker settings to be stored for future use
- Some analyzers also provide accurate frequency-counter measurements for the marker positions

Advanced Analyzer Features: Storage

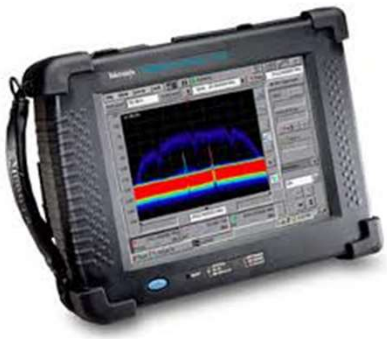
- Display Storage
  - Most modern analyzers allow digital storage of complete displays including signal, markers, and labels for all settings
  - This is very helpful in documenting what has been seen, and for before-and-after evaluation
  - The displays can be downloaded to PC and saved as relatively small files for archiving purposes

- Settings Storage
  - Most modern analyzers also allow digital storage of complete measurement setups including center frequency, frequency span, amplitude settings, scan rate, IF and video bandwidths, marker settings, and any other advanced features
  - This is very convenient for repetitive measurements under the same conditions: no tedious settings, just recall setup #3 and you're ready to measure.

- Many times you will want to measure
  - The amount of coupling between nearby antennas
  - The loss of a transmission line or gain of an amplifier
  - The frequency response of a filter
- A basic spectrum analyzer only receives and displays how much energy is at each frequency
  - It does not make signals; it only displays existing signals
- A Tracking Generator connects to a spectrum analyzer and operates in sync with it. It produces a signal of precise strength with a frequency that “tracks” right along with the frequencies the spectrum analyzer is displaying
- By feeding the tracking generator into a device under test and looking at the output with a spectrum analyzer, its gain or loss, passband, distortions, and many other characteristics can be seen

The Most Advanced Spectrum Analyzers for Signal Detection and Identification

- Currently the most effective spectrum analyzers in the world are actually DSP-based receivers using advanced A-D converters
- They're able to analyze whole 20 MHz. spectrum blocks in real time to capture pulsed signals as short as 125 microseconds.
- The Rohde & Schwarz PR100 ($55,000)
  - GPS in the antenna handle and excellent automatic mapping
- The Tektronix SA2600 ($43,000)
  - The H600 variation, has a catalog of many different types of signals and can identify most types immediately
- Both these devices are sensitive enough to spot local oscillators of cell phones buried with IEDs
- Both export restricted on US munitions list



Electronic Order of Battle (EOB)

- An electronic order of battle (EOB) is a listing of noncommunications electronic devices, including site designation, nomenclature, location, site function, and any other pertinent information obtained from any source that has military significance when related to the devices.
- The Electronic Order of Battle (EOB) details known combinations of emitters and platforms in a particular operator in the form of paper-based products, sometimes Area of Responsibility, for both Blue and Red force data.
- Data on emitters, platforms, threat systems, and signatures etc.

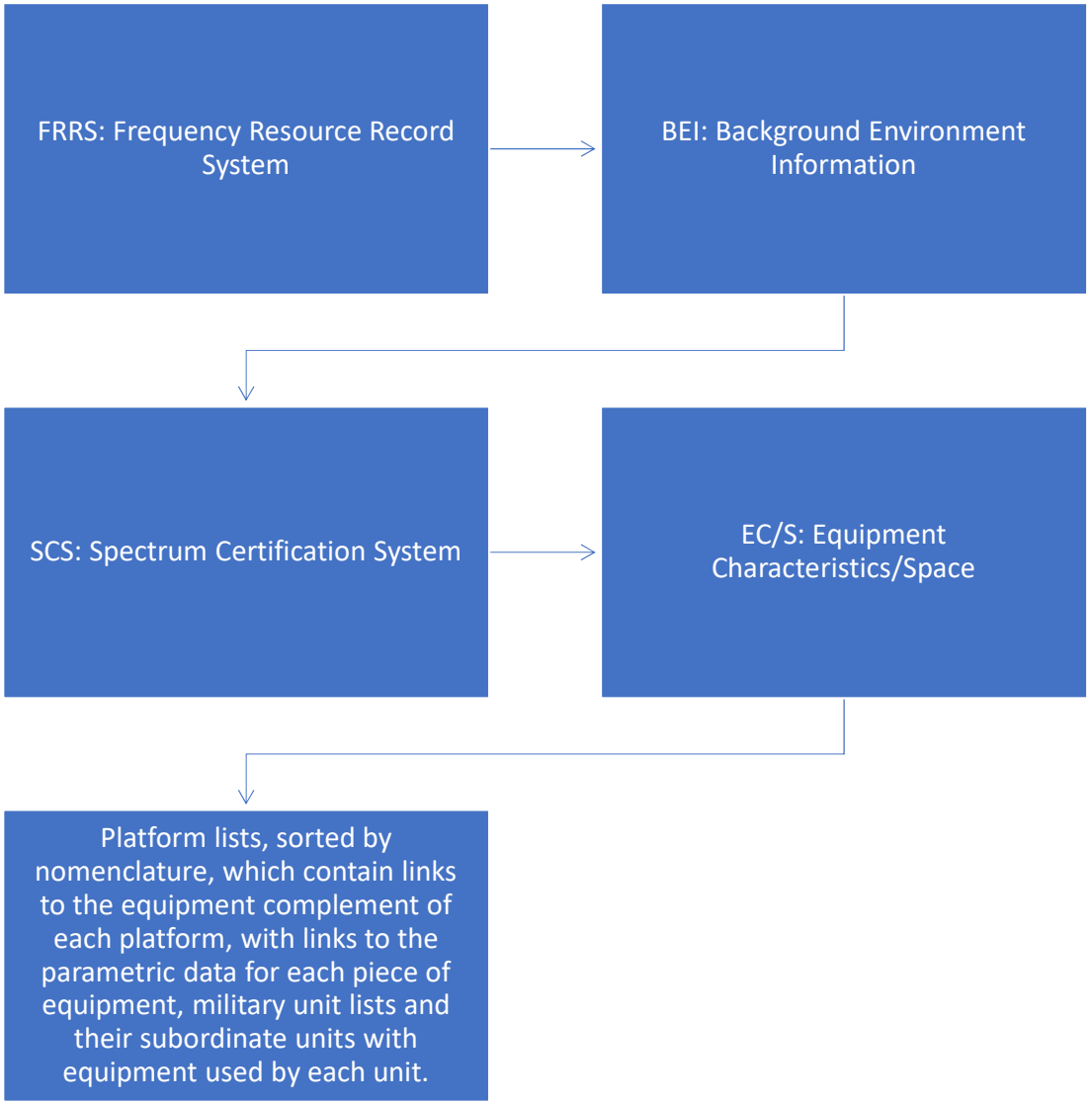
Generating the Electronic Order of Battle (EOB)

- Airborne Signals Intelligence (SIGINT) has long been a tactical and strategic asset for the Operational Commander in multi-domain electronic warfare (EW).
- This electronic support measure (ESM) discipline continues to grow in importance with the evolving radar and communication technology.
- Generating the Electronic Order of Battle (EOB) by intercepting the signals of both adversaries and the friendly forces and determining their role in the broader organizational order of battle is critical for the war fighters.

Electronic Order of Battle (EOB)

- Generating an electronic order of battle (EOB) requires identifying SIGINT emitters in an area of interest, determining their geographic location or range of mobility, characterizing their signals, and, where possible, determining their role in the broader organizational order of battle.

- EOB covers both COMINT and ELINT.



Intelligence and Maintaining an EOB

Example of location technical databases

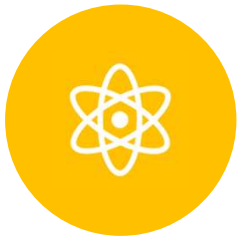
EOB and related data flow

- For example, several voice transmitters might be identified as the command net (i.e., top commander and direct reports) in a tank battalion or tank-heavy task force. Another set of transmitters might identify the logistic net for that same unit.
- An inventory of ELINT sources might identify the medium- and long-range counter-artillery radars in each area.
- Signals intelligence units will identify changes in the EOB, which might indicate enemy unit movement, changes in command relationships, and increases or decreases in capability.
- Using the COMINT gathering method enables the intelligence officer to produce an electronic order of battle by traffic analysis and content analysis among several enemy units. For example, if the following messages were intercepted:

The EOB Buildup Process

Signal separation

Measurements optimization



Data Fusion

Networks build-up

Countermeasures to Interception

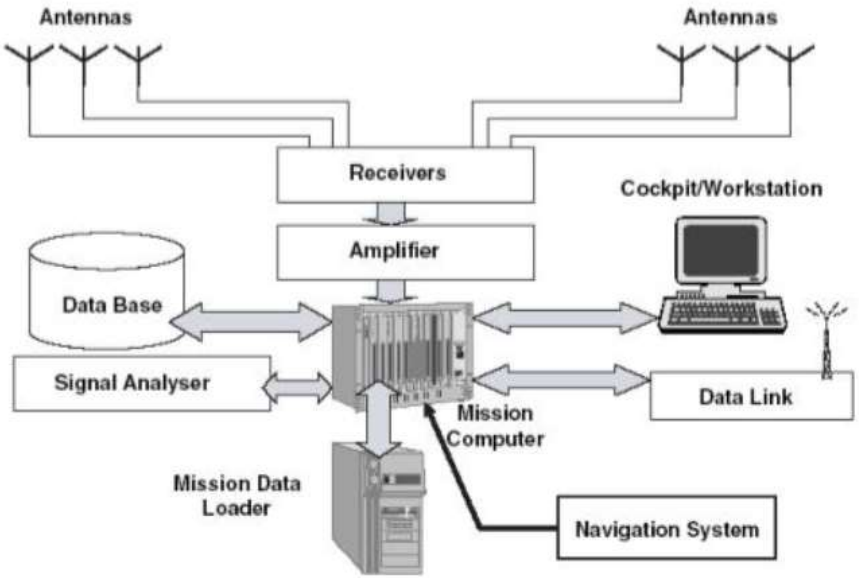
- Spread-spectrum communications is an electronic counter-countermeasures (ECCM) technique to defeat looking for frequencies. Spectrum analysis can be used in a different ECCM way to identify frequencies not being jammed or not in use.

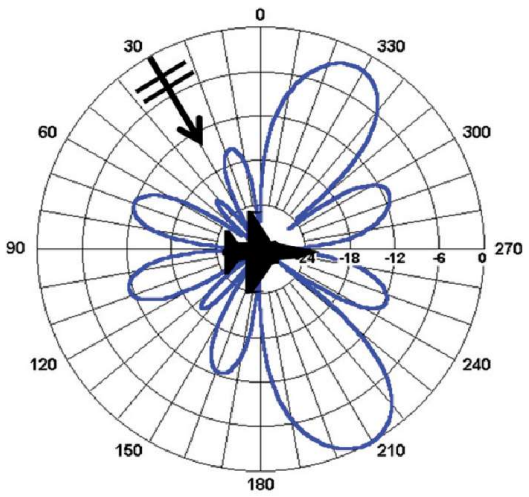
COMINT and ELINT Collections

- COMINT Collection
  - The locations and numbers of specific communication transmissions
  - Their signal characteristics
  - Their messages
  - Any communication patterns

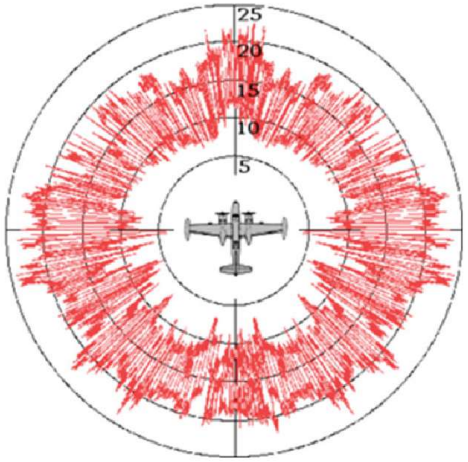
- ELINT
  - Collection of the source and direction of arrival (DOA) of a broad range of radar emitters and other electrnoic systems
  - Signals are analyzed for
  - Frequency (f)
  - Pulse and pulse repetition frequency (PRF)
  - Signal Strength
  - Modulation schemes
  - Scan parameters
  - Usage pattens

Typical Architecture of COMINT/ELINT





Radar cross section (RCS) measurements



Technical ELINT

- Technical ELINT then deals with interception, collection, analysis identification and recording, and documentation of emitter radiations or signatures.

- Although often non-real time in the past it is becoming forced to be more real-time to keep pace with the modern battlefield.

Operational ELINT

- The term Operational ELINT is used by some in the community to describe actions taken to search, intercept, locate, and identify radiated electromagnetic energy for the purpose of real-time exploitation of such radiations in support of military actions.

- This definition is often used to describe the same functions as Electronic Support (ES), whereas ES was more often applied to tactical platforms and Operational ELINT to more strategic or national platforms.

- Overviews of signal data bases and information provided to users will be reviewed at a high level.

Use of Electromagnetic Spectrum

- All military forces use the electromagnetic spectrum to command-and-control operating forces acquire targets, guide weapons, and direct supporting arms.

- These military forces also use the electromagnetic spectrum to collect, process, and report intelligence and to support other administrative and logistics operations.

SIGINT Direction-Finding

- Advanced threat representative Signal Intelligence and Direction Finding (SIGINT/DF) capabilities for collection and reporting of Direction Finding (DF) to support threat command decisions and optimize the use of threat force assets.
- Signal survey, search, detection, visualization, collection, wideband recording, DF/geolocation, analysis and reporting.
- Scan the RF spectrum, detect and catalog all signal activity.
- Direction Finding (DF) for Communications Intelligence (COMINT) and Electronic Warfare (EW) applications.

Integrated products for spectrum monitoring, direction finding, adaptive beamforming and geolocation of High Frequency (HF) signals

- Signals Intelligence (SIGINT) and geolocation
- Detection, interception and collection of Signals of Interest (SOIs)
- Monitoring of interference
- Estimation of spectrum occupancy
- Tasking of array systems for radio Direction Finding (DF) and beamforming
- Spectrum policing
- Enhanced signal reception to increase link availability
- Research into High Frequency (HF) propagation to enhance ionosphere models

SIGINT Direction-Finding Product Example

- The product range includes antennas, receivers and processing software which can be combined to create a system designed for specific application.
- Super-Resolution Direction Finding (SRDF)
- Adaptive Digital Beamforming (ADBF) technology

Direction-Finding

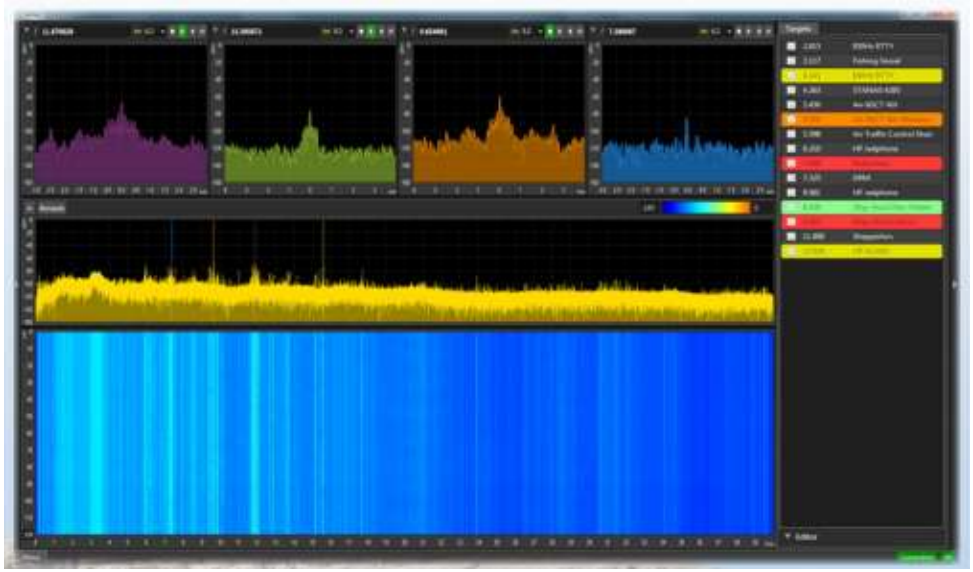
Name	Frequency
Direction Finding System	20 MHz – 6 GHz
HF Direction Finding System	1.5 MHz – 30 MHz
VHF Super Resolution Direction Finding Antenna	20 MHz – 300 MHz
VHF - UHF Super Resolution Direction Finding Antenna	20 MHz – 6 GHz

Super-Resolution Direction Finding (SRDF)

- SRDF Conventional DF systems can only estimate the direction of arrival of a single signal within a given frequency band.

- Super-resolution provides the ability to resolve two or more signals whose angular separation is less than the natural beamwidth of the array.

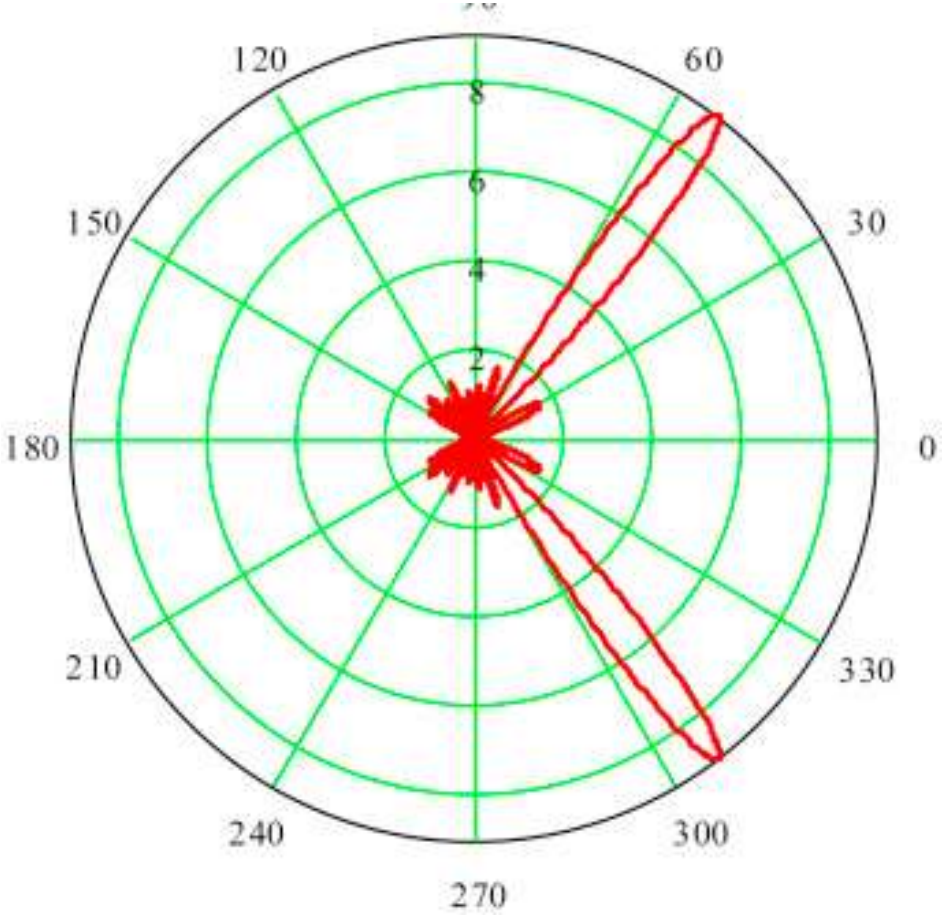
- An order of magnitude increase in spatial resolution
- Increased Direction Finding (DF) accuracy
- Simultaneous azimuth and elevation DF
- Operation with short duration signals
- No requirement for a particular array geometry

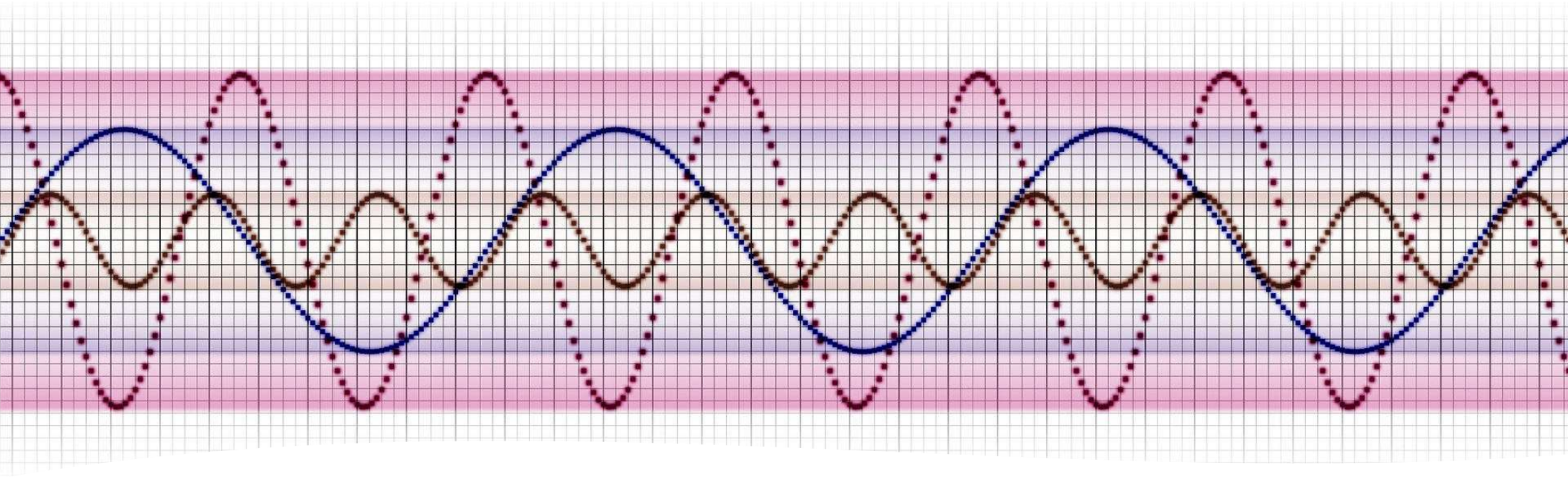


ADAPTIVE DIGITAL BEAMFORMING (ADBF)

- The enhanced output from ADBF allows a Signal of Interest (SOI) to be detected and demodulated regardless of the presence of other signals.

- Advantages of ADBF over single antenna reception include:
- For an N antenna array, a signal to noise improvement of up to 10log(N) dB
- Signal to interference improvement of up to 40 dB, when in the presence of strong interference
- Discrimination between signal propagation via groundwave and multiple skywave modes

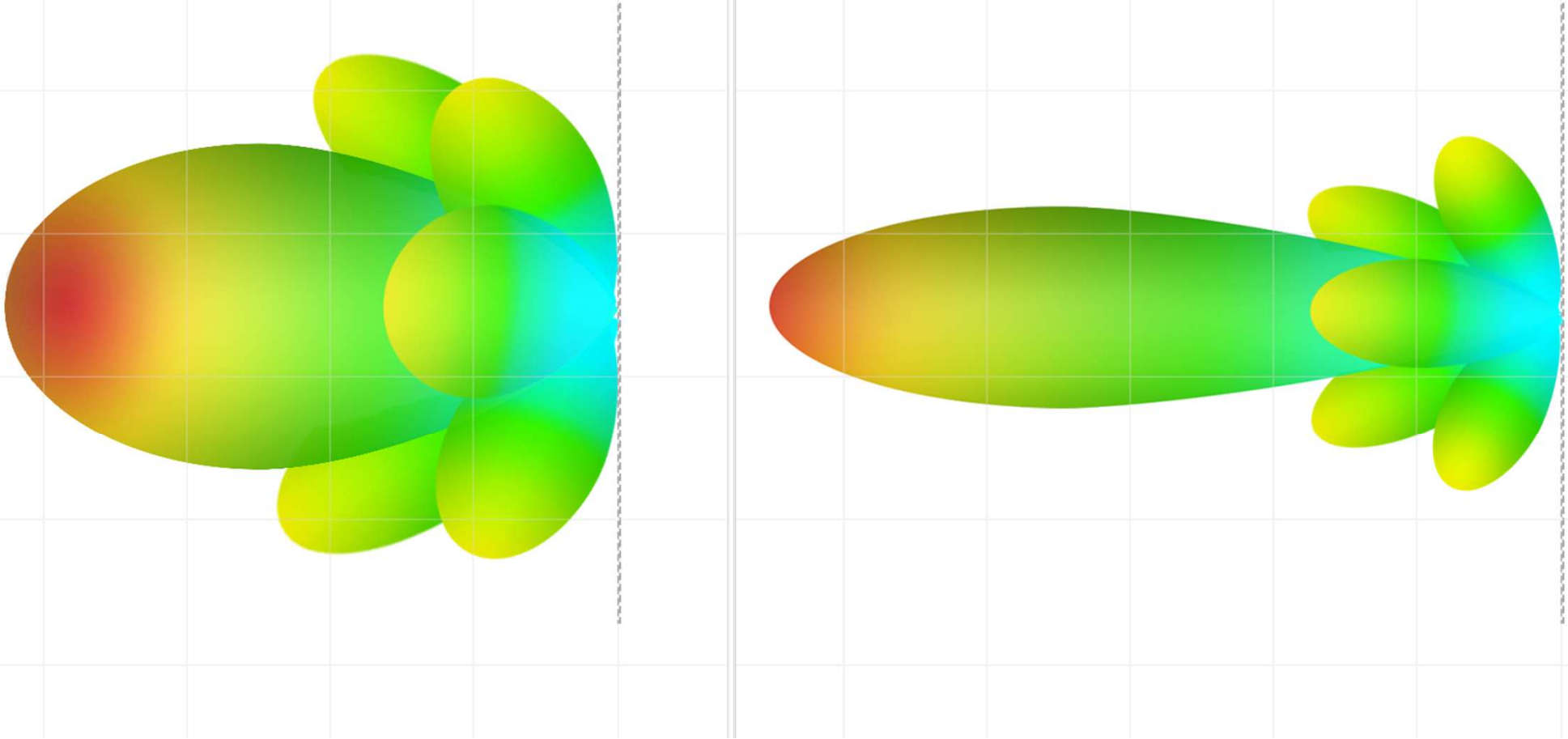


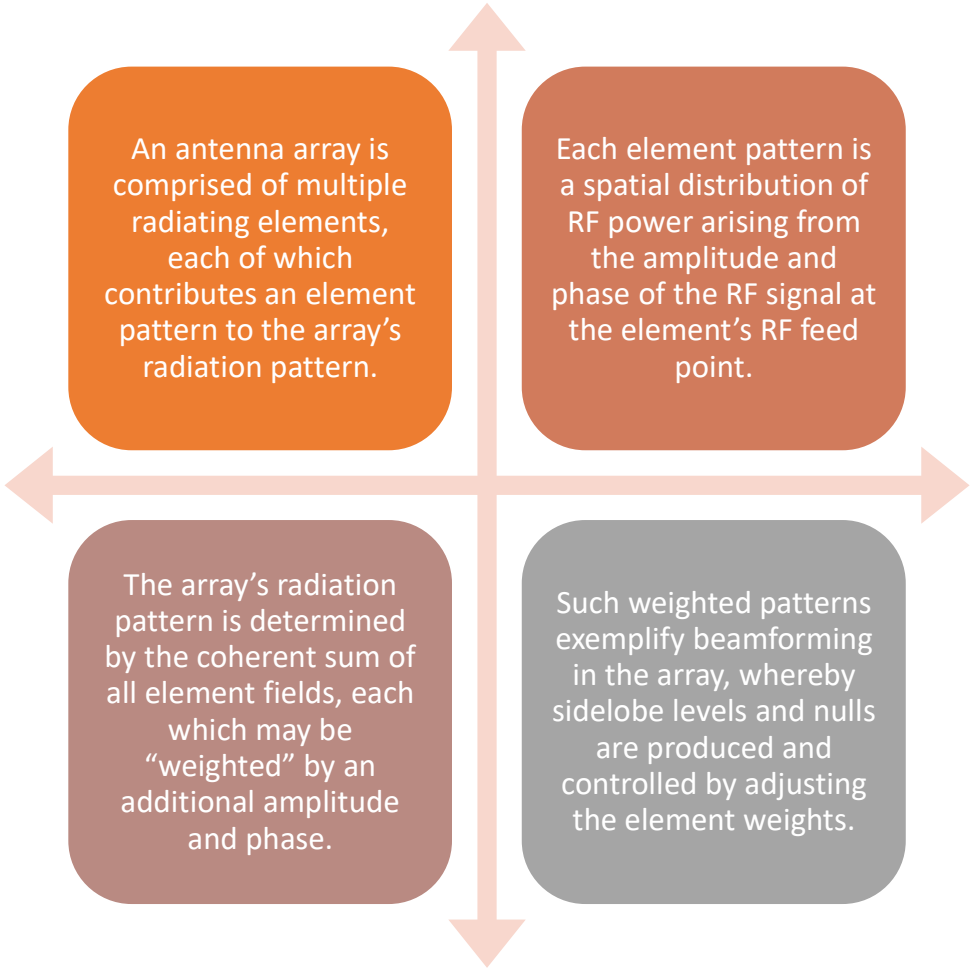


Beamforming

- The term ***beamforming*** refers to a method of directing a RF signal towards a specific receiving device, whereas the alternative would be allowing the signal to spread in all directions from a transmitter the way it naturally would.
- By focusing a signal on a specific direction, **beamforming delivers higher signal quality to a receiver**. This means information is transmitted faster and more accurately. Furthermore, this accuracy can be reached **without boosting power**.

Example of Radiation Pattern with a Fixed Beamformer and an Adaptive Beamformer





Beamforming techniques loosely fall into two categories: conventional and adaptive

Fixed Beamforming vs. Adaptive Beamforming

Fixed beamforming generally describes a conventional technique where the antenna array pattern is obtained from fixed element weights that do not depend on the signal environment.

Conversely, adaptive beamforming element weights that do depend on and can adapt to the signal environment via some feedback mechanism.

Adaptive beamforming, which was initially developed in the 1960s, uses a digital signal processor (DSP) to compute the complex weights using an adaptive algorithm, which then generates an array factor for an optimal signal-to-interference-plus-noise ratio (SINR).

Basically, adaptive beamformers are designed to adjust to differing situations in order to maximize or minimize SINR, which helps measure the quality of wireless communication.

GEOLOCATION

The geographical position of a transmitter can be determined by using both single or multiple arrays.

For a single array system the location is estimated using DF results in conjunction with measurements or modelling of the ionosphere.

More accurate position fixes can be achieved using triangulation techniques on DF results from multiple arrays.

Processing and Exploitation

SIGINT processing consists of converting and formatting raw signals data to a form that is usable in follow-on SIGINT and all-source intelligence analysis.

The processing and exploitation phase is usually not a discrete function, but rather one that is accomplished during collection.

Once the collected information has been processed, analysis must determine its significance. Other intelligence information may also be fused together with the processed SIGINT to give a comprehensive picture and to show how the information can be used by the commander to gain an advantage.

Processing and Exploitation

The following processing and exploitation functions are used to convert collected raw information into a form suitable for SIGINT production

Traffic Analysis

Linguistic Analysis

Signal Analysis

ELINT Analysis

Traffic Analysis

- Traffic analysis is the study of all characteristics of communications except encrypted texts.
- Call signs, frequencies, times of transmission, cryptographic indicators, precedence, and message lengths are examples of these characteristics.
- These characteristics are called externals and are compiled and sorted primarily for the purpose of reconstructing the adversary's communication structure and organization.
- This information yields valuable electronic order of battle data and other information. With on-line communication encryption systems becoming widely used by potential adversaries, traffic analysis becomes an increasingly difficult function.

Traffic Analysis

When locations are known, usage patterns may emerge, from which inferences may be drawn.

Traffic analysis is the discipline of drawing patterns from information flow among a set of senders and receivers, whether those senders and receivers are designated by location determined through direction finding, by addressee and sender identifications in the message, or even MASINT techniques for "fingerprinting" transmitters or operators.

Message content, other than the sender and receiver, is not necessary to do traffic analysis, although more information can be helpful.

Traffic Analysis Example

For example, if a certain type of radio is known to be used only by tank units, even if the position is not precisely determined by direction finding, it may be assumed that a tank unit is in the general area of the signal.

The owner of the transmitter can assume someone is listening, so might set up tank radios in an area where he wants the other side to believe he has actual tanks.

Traffic analysis need not focus on human communications

Example:

- if the sequence of a radar signal, followed by an exchange of targeting data and a confirmation, followed by observation of artillery fire, this may identify an automated counterbattery system.
- A radio signal that triggers navigational beacons could be a landing aid system for an airstrip or helicopter pad that is intended to be low-profile.
- Patterns do emerge. Knowing a radio signal, with certain characteristics, originating from a fixed headquarters may be strongly suggestive that a particular unit will soon move out of its regular base. The contents of the message need not be known to infer the movement.
- There is an art as well as science of traffic analysis. Expert analysts develop a sense for what is real and what is deceptive.

Cryptanalysis

- Cryptanalysis is the study of encrypted signals, data, and texts to determine their plain language equivalents.

- The capability to read the adversary's encrypted communications is obviously valuable.

- Cryptanalysis capability depends on the sophistication of the target's encryption system and the availability of specialized equipment and software resources availability.

Note

Cryptanalysis is the study of methods for obtaining the **meaning** of encrypted information, without access to the secret information that is typically required to **do** so.

Typically, this involves knowing how the system works and finding a secret key.

Cryptanalysis is also referred to as codebreaking or cracking the code.

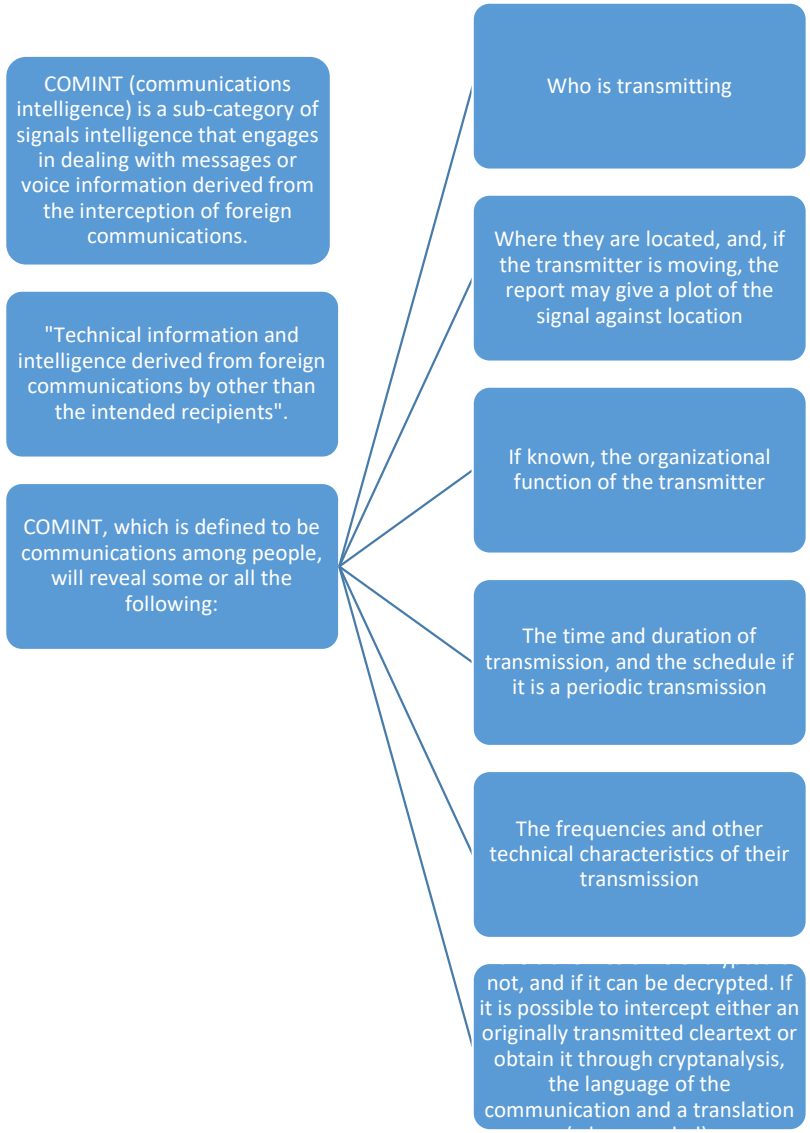
Linguistic Analysis

- Linguistic analysis is the transcription and translation of foreign language intercepts into for example English, German or Japanese.

- This analysis starts at the collection site upon interception. Messages of considerable length require more time and are usually transcribed and translated.

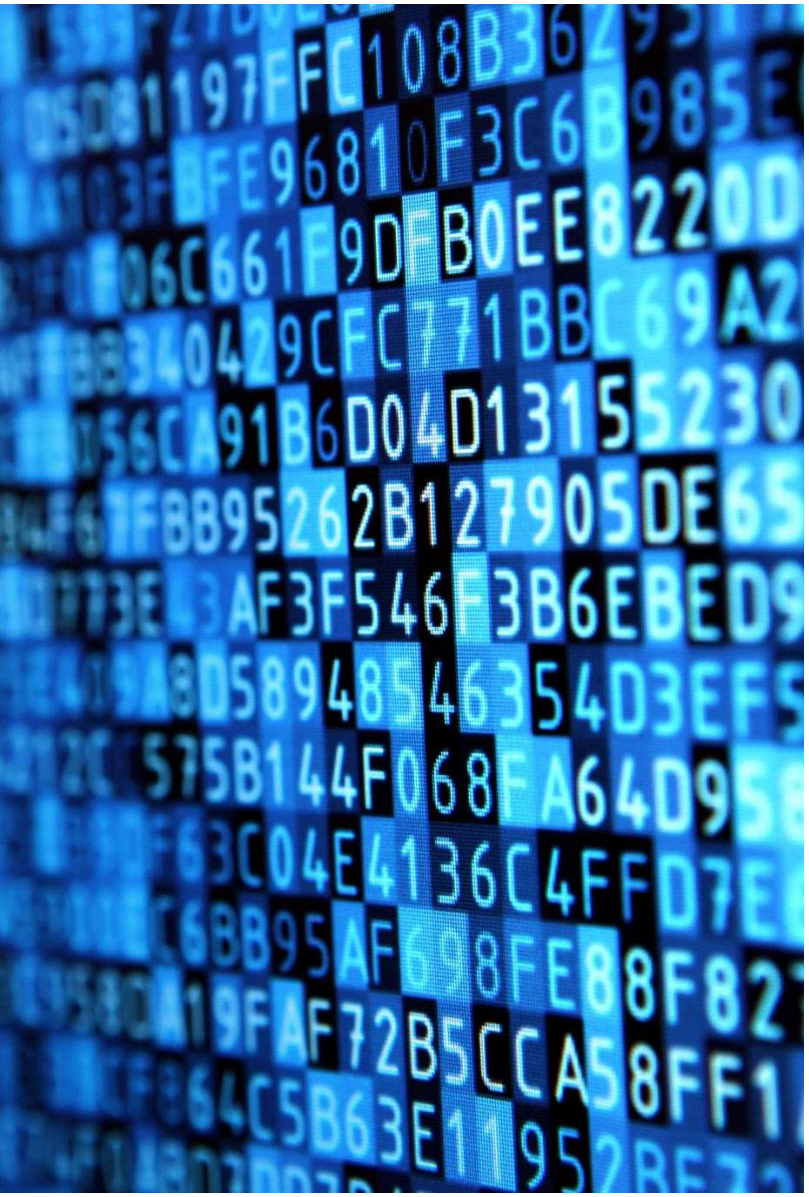
- SIGINT specialists are trained in a wide variety of languages for this task, but augmentation by external sources (e.g., native and/or contract linguists) may be required in order to satisfy all requirements.

Communications Intelligence



Voice Interception

- A basic COMINT technique is to listen for voice communications, usually over radio but possibly "leaking" from telephones or from wiretaps.
- If the voice communications are encrypted, traffic analysis may still give information.
- While modern electronic encryption does away with the need for armies to use obscure languages, it is likely that some groups might use rare dialects that few outside their ethnic group would understand.
- Retrospective analysis of old telephone calls can be made from Call detail record (CDR) used for billing the call.



Call Detail Record (CDR)

- **Call Detail Record (CDR)** - or Telephony Metadata include comprehensive communications routing information, specifically, originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, Mobile Subscriber Integrated Services Digital Network Number (MSISDN), International Mobile station Equipment Identity (IMEI) number, also trunk identifier, telephone calling card numbers, and the time and duration of call.

- Telephony metadata does NOT include substantive content of any communication, or the name, address, or financial information about a subscriber or customer.

Mobile Evolution of 1G to 5G

1G to 4G Mobile last 30 years interconnecting people
5G interconnecting people with machines, IoT, AI, ML, DL, SDN/NFV and SOA

5Gs (5G System) IDs

- 5G-GUTI 5G Globally Unique Temporary Identifier
- 5G-S-TMSI 5G S-Temporary Mobile Subscription Identifier
- GUAMI Globally Unique AMF Identifier
- GUTI Globally Unique Temporary UE Identity
- NCGI NR Cell Global Identity
- NCI NR Cell Identity
- PEI Permanent Equipment Identifier
- SUCI Subscription Concealed Identifier
- SUPI Subscription Permanent Identifier
- UUID Universally Unique Identifier

5G Identifiers

- 5G Globally Unique Temporary Identifier (GUTI)
  - The 5G-GUTI is used in 5G as a means to keep the subscriber's IMSI confidential. At the time of network registration, the AMF (Core Access and Mobility Management Function) will allocated the 5G-GUTI, which is comprised of the GUAMI (Globally Unique AMF ID) and the 5G-TMSI (5G Temporary Mobile Subscriber Identity).
- 4G IMSI
  - 5G→ Subscription Permanent Identifier (SUPI)
  - In 5G, all subscribers will be allocated a globally unique 5G SUPI. Example SUPI formats include the IMSI and NAI (Network Access Identifier).
- 4G P-TMSI
  - 5G→ Subscription Concealed Identifier, the SUCI
  - SUCI contains the mobile country code and mobile network code
  - The SUCI is a partially encrypted SUPI (Subscription Permanent Identifier), used during procedures associated with the 5G System when the device has not been assigned a 5G-GUTI (5G Globally Unique Temporary Identity). The SUCI is created by encrypting the MSIN (Mobile Subscriber Identification Number) component of the subscriber's IMSI.
- 4G IMEI
  - 5G→ Permanent Equipment Identity or PEI
- Subscriber Identity De-concealing Function (SIDF)
  - The SIDF is a functional element of the UDM (Unified Data Management), responsible for decrypting a SUCI (Subscription Concealed Identifier) to reveal the subscriber's SUPI (Subscription Permanent Identifier). The Subscription Identifier De-Concealing Function (SIDF) is responsible for de-concealing the SUPI from the SUCI. The SIDF uses the private key part of the privacy-related home network public/private key pair that is securely stored in the home operator's network. The de-concealment shall take place at the UDM. Access rights to the SIDF shall be defined, such that only a network element of the home network is allowed to request SIDF

SUBSCRIPTION PERMANENT IDENTIFIER (SUPI)

A globally unique 5G Subscription Permanent Identifier (SUPI) shall be allocated to each subscriber in the 5G system and provisioned in the UDM/UDR.

The SUPI is used only inside 3GPP system

Valid SUPI types:

- IMSI
- Network Access Identifier (NAI)
  - By using the NAI, it will be possible to also use non-IMSI-based SUPIs

Depending on the protocol used to convey the SUPI, the SUPI type can take different formats.

5G Identifiers

- Each subscriber in the 5G system shall be allocated one 5G Subscription Permanent Identifier (SUPI) for use within the 3GPP system. The Subscription Concealed Identifier (SUCI) is a privacy-preserving identifier containing the concealed SUPI.

  - The 5G system supports identification of subscriptions independently of identification of the UE. Each UE accessing the 5G system shall be assigned a Permanent Equipment Identifier (PEI).

  - The 5G system supports allocation of a temporary identifier (5G-GUTI) in order to support user confidentiality protection.

3GPP TS 23501: 5G system various identifiers at subscriber level and the equipment level

- SUPI-Subscription Permanent Identifier
- At Subscriber level
  - It is valid only in the 3GPP system, provisioned in the UDM/UDR.
  - It is based on IMSI (TS 23003) + Network specific identifier (TS 22261). In this way, UE can present its IMSI to the network (EPC) in inter-working scenarios.
  - For roaming cases, it may take the form of MCC+MNC of IMSI.

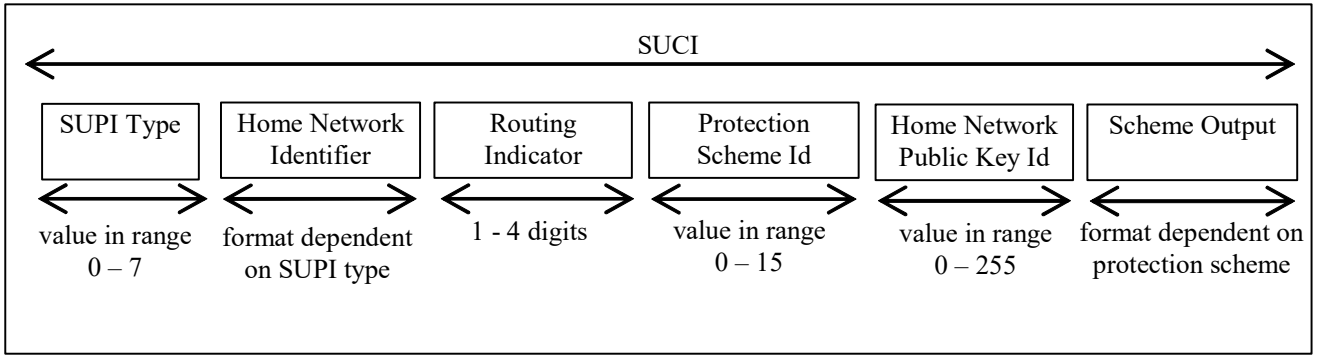
SUCI - Subscription Concealed Identifier

At Subscriber level

The SUCI is a privacy preserving identifier containing the concealed SUPI

It is to preserve the privacy and more details can be found in

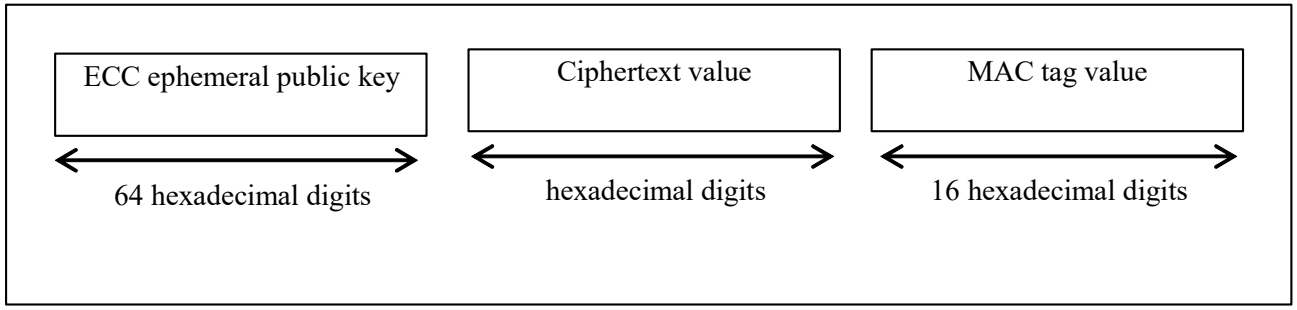
Decoding of SUCI



Structure of SUCI

- The SUCI is composed of the following parts:
- 1) SUPI Type, consisting in a value in the range 0 to 7. It identifies the type of the SUPI concealed in the SUCI. The following values are defined:
  - 0: IMSI
  - 1: Network Specific Identifier
  - 2 to 7: spare values for future use.
- 2) Home Network Identifier, identifying the home network of the subscriber.
- When the SUPI Type is an IMSI, the Home Network Identifier is composed of two parts:
- Mobile Country Code (MCC), consisting of three decimal digits. The MCC identifies uniquely the country of domicile of the mobile subscription;
- Mobile Network Code (MNC), consisting of two or three decimal digits. The MNC identifies the home PLMN of the mobile subscription.
- When the SUPI type is a Network Specific Identifier, the Home Network Identifier consists of a string of characters with a variable length representing a domain name as specified in clause 2.2 of IETF RFC 7542.
- 3) Routing Indicator, consisting of 1 to 4 decimal digits assigned by the home network operator and provisioned in the USIM, that allow together with the Home Network Identifier to route network signalling with SUCI to AUSF and UDM instances capable to serve the subscriber. If no Routing Indicator is configured on the USIM, this data field shall be set to the value 0.
- 4) Protection Scheme Identifier, consisting in a value in the range of 0 to 15 (see Annex C.1 of 3GPP TS 33.501).
- 5) Home Network Public Key Identifier, consisting in a value in the range 0 to 255. It represents a public key provisioned by the HPLMN and it is used to identify the key used for SUPI protection. In case of null-scheme being used, this data field shall be set to the value 0;
- 6)Scheme Output, consisting of a string of characters with a variable length or hexadecimal digits, dependent on the used protection scheme, as defined below. It represents the output of a public key protection scheme specified in Annex C of 3GPP TS 33.501 or the output of a protection scheme specified by the HPLMN.

Scheme Output for Elliptic Curve Integrated Encryption Scheme Profile A

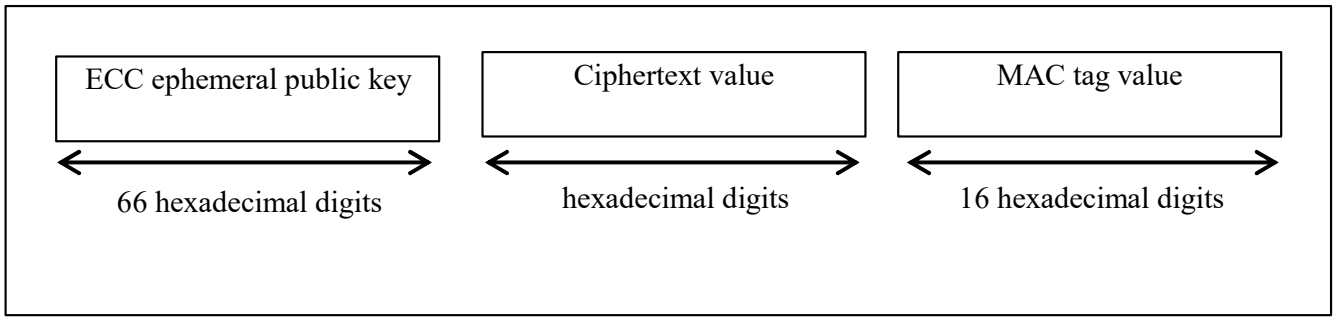


The Mobile Subscriber Identification Number (MSIN) or the username identifies the mobile subscription within the Home Network. The scheme output is formatted as a variable length of characters as specified for the username in clause 2.2 of IETF RFC 7542 .

If the null-scheme is used, the NFs can derive SUPI from SUCI when needed. The AMF derives SUPI used for AUSF discovery from SUCI when the Routing-Indicator is zero and the Protection Scheme is null-scheme.

The ECC ephemeral public key is formatted as 64 hexadecimal digits, which allows to encode 256 bits. The ciphertext value is formatted as a variable length of hexadecimal digits. The MAC tag value is formatted as 16 hexadecimal digits, which allows to encode 64 bits.

Scheme Output for Elliptic Curve Integrated Encryption Scheme Profile B

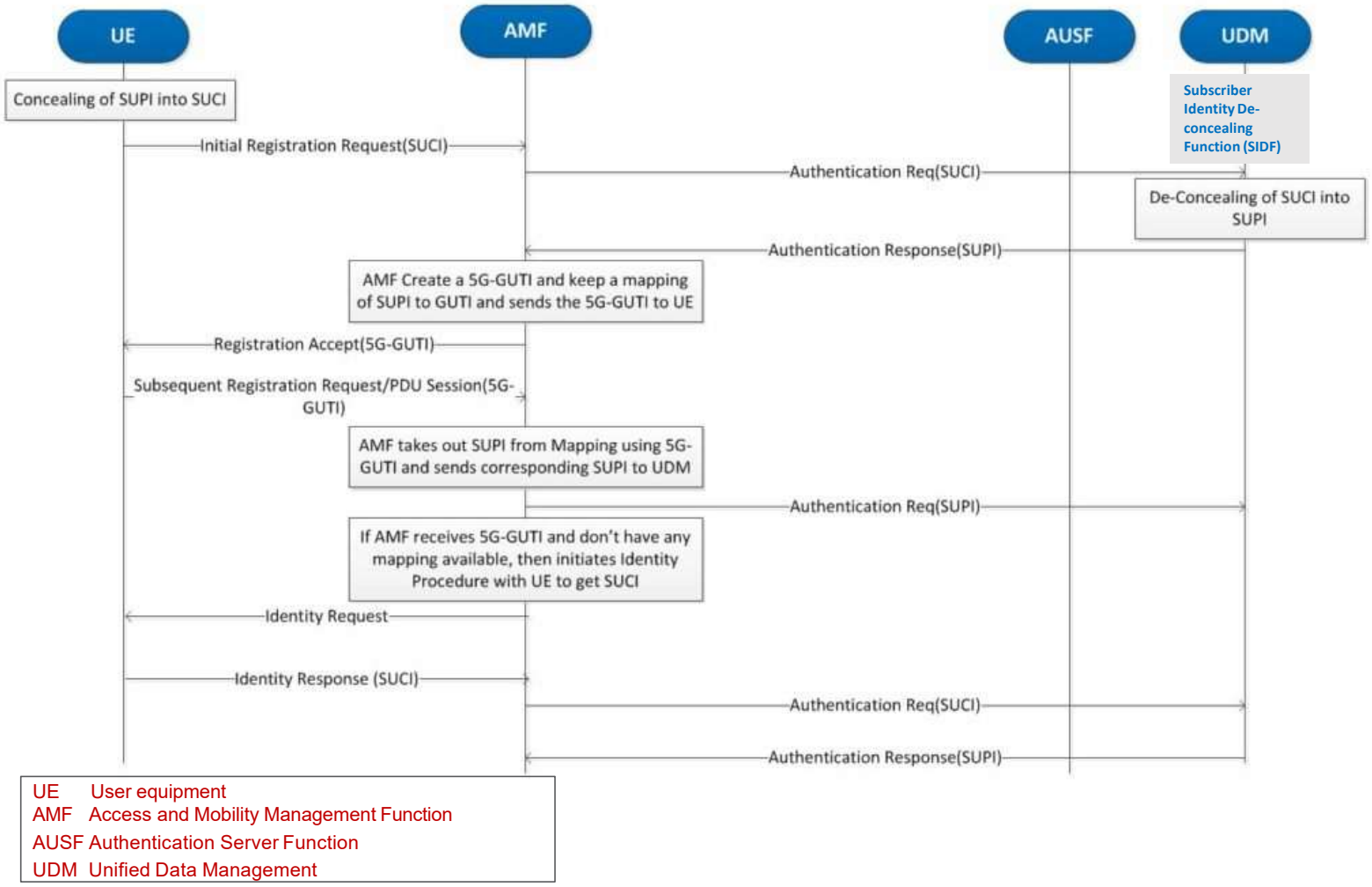


The ECC ephemeral public key is formatted as 66 hexadecimal digits, which allows to encode 264 bits.

The ciphertext value is formatted as a variable length of hexadecimal digits.

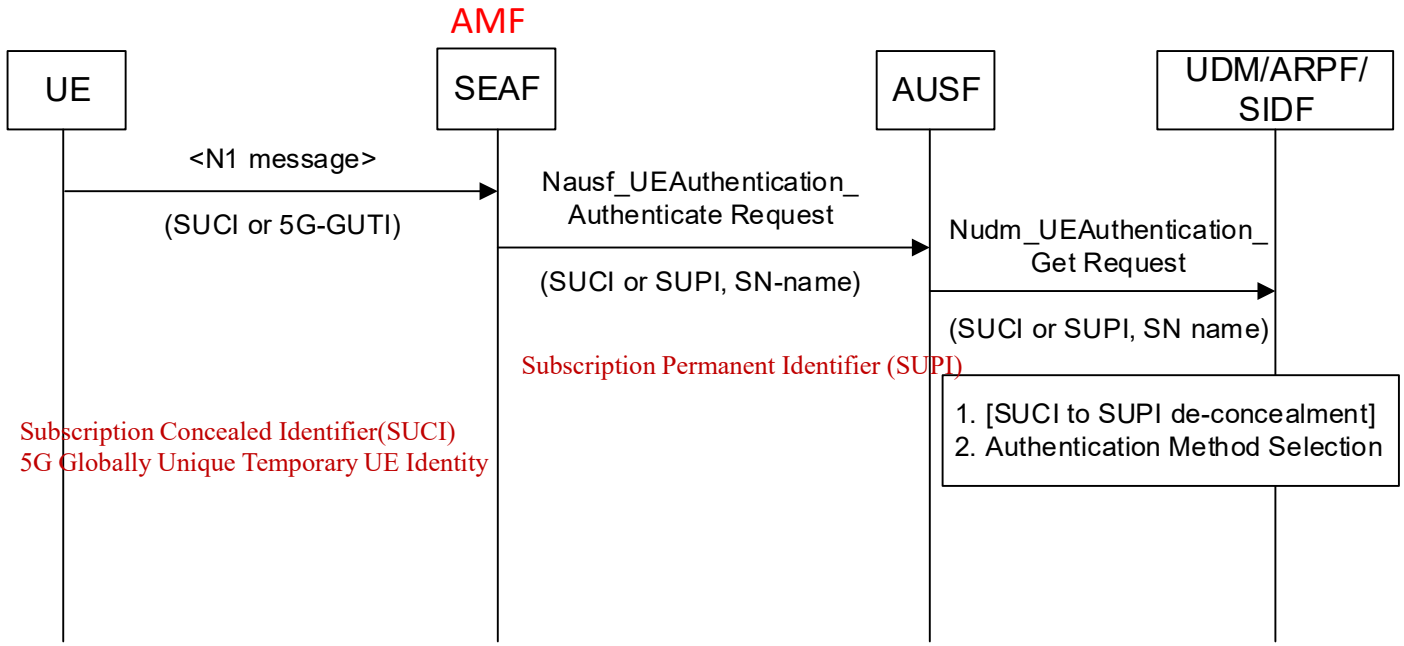
The MAC tag value is formatted as 16 hexadecimal digits, which allows to encode 64 bits.

Identity flow between UE and Network



UE User equipment
AMF Access and Mobility Management Function
AUSF Authentication Server Function
UDM Unified Data Management

Initiation of authentication and selection of authentication method



AUSF: AUthentication Server Function
ARPF: Authentication credential Repository and Processing Function
SIDF: Subscription Identifier De-concealing Function
SEAF: SEcurity Anchor Function
UDM: Unified Data Management

5G Authentication Frameworks

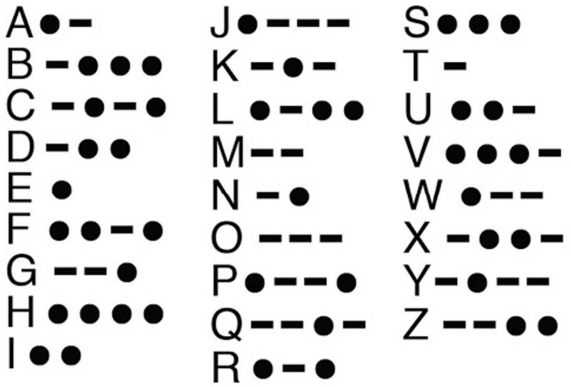
1. 5G AKA (Authentication and Key Management)
   -Mobile Phones and Tablets
2. EAP-AKA’
   -Accessing from a non 3GPP environment (WiFi and Cable)
3. EAP-TLS (PKI)
   -IoT
   -Non-USIM

Signaling Channel Interception

- A given digital communications link can carry thousands or millions of voice communications, especially in developed countries.
- Without addressing the legality of such actions, the problem of identifying which channel contains which conversation becomes much simpler when the first thing intercepted is the signaling channel that carries information to set up telephone calls.
- In civilian and many military use, this channel will carry messages in Signaling System 7 (SS7) protocols in traditional telephony, SIP in VoIP and Diameter in 4G/5G.

Text Interception

- Morse code interception was once very important, but Morse code telegraphy is now obsolete in the western world, although possibly used by special operations forces.
- Such forces, however, now have portable cryptographic equipment.
- Morse code is still used by military forces of former Soviet Union countries.
- Specialists scan radio frequencies for character sequences (e.g., electronic mail) and fax.

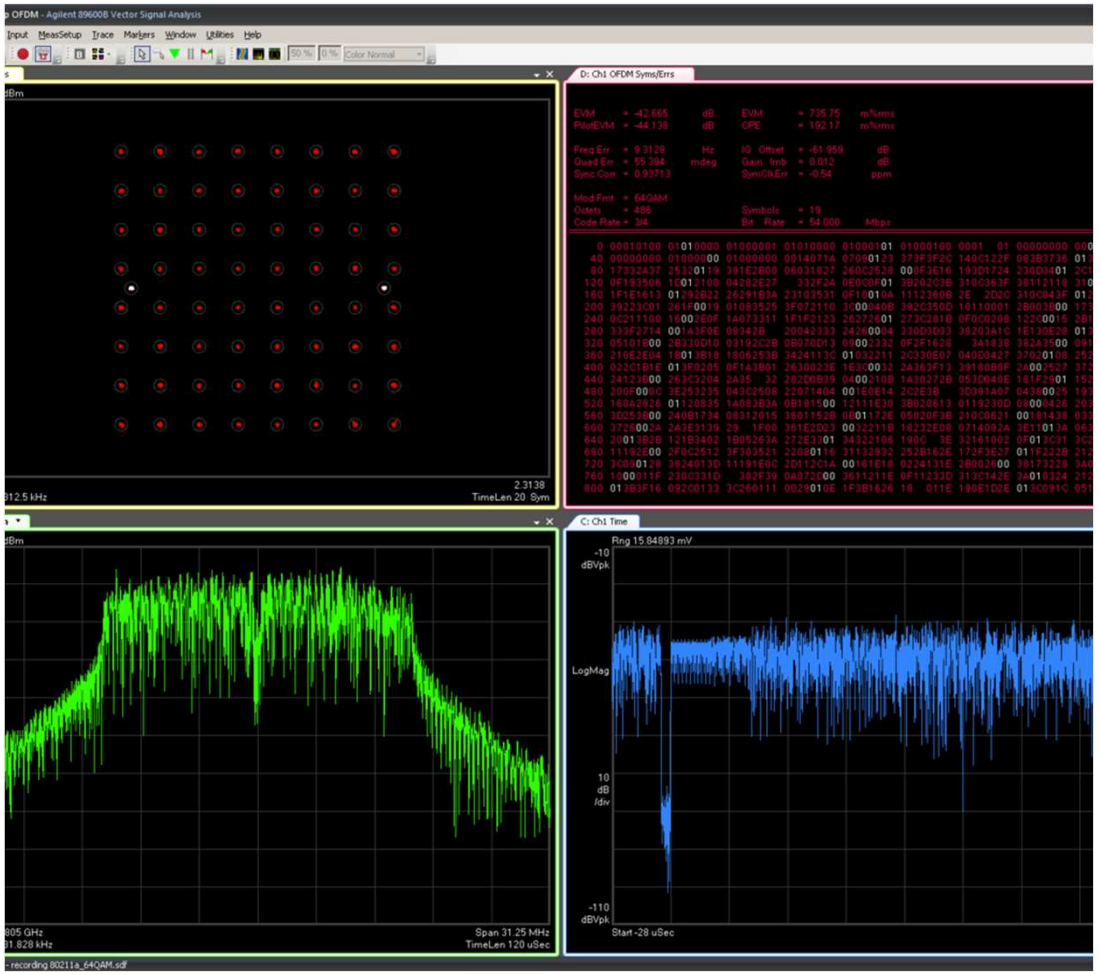


Signal Analysis

- Signal analysis consists of working with all types of signals (e.g., COMINT, ELINT, pro forma) to identify, isolate, reduce to pure form, and exploit acquired SOIs.

- The signal analyst must be well trained and possess the proper electronic and software support tools to be effective.

SOI=signals of interest



SIGINT and Electronic Warfare

- Electronic warfare (EW) is “any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy”.

- EW denies the enemy use of the electromagnetic spectrum for command and control and protects it for friendly command and control. There are three divisions of EW.

SIGINT and EW

- Electronic Warfare Support
- Electronic Attack
- Electronic Protection

Electronic Warfare Support (ES)

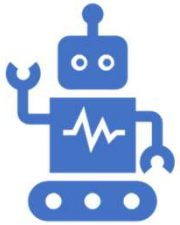
- Electronic Warfare Support Electronic warfare support (ES) includes actions tasked by or under the direct control of an operational commander to search for, intercept, identify, and locate sources of intentional and unintentional radiated enemy electromagnetic signals for the purpose of immediate threat recognition.

- ES provides information required for immediate tactical decisions and operations such as the identification of imminent hostile actions, threat avoidance, targeting, or electronic attack.

SIGINT and ES

Both SIGINT and ES involve searching for, intercepting, identifying, and locating electronic emitters.

The primary differences between the two are the information's intended use, the degree of analytical effort expended, the detail of information provided, and the timeliness required.



SIGINT is used to gain information concerning the enemy, usually in response to a priority intelligence requirement (PIR), an intelligence requirement (IR), or other means.

Electronic Attack (EA)

01

Electronic attack (EA) is action taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum. The objectives of SIGINT may conflict with those of EA.

02

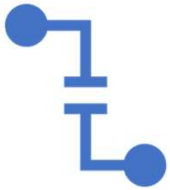
For example, EA may be conducted to interfere with the adversary's use of an emitter the same time as SIGINT operations are designed to exploit the adversary's use of the same emitter.

03

Furthermore, EA operations against one target may disrupt or otherwise interfere with friendly SIGINT collection against the same or different targets.

SIGINT and EA

The objectives of SIGINT may conflict with those of EA.



For example, EA may be conducted to interfere with the adversary's use of an emitter the same time as SIGINT operations are designed to exploit the adversary's use of the same emitter.

Furthermore, EA operations against one target may disrupt or otherwise interfere with friendly SIGINT collection against the same or different targets.

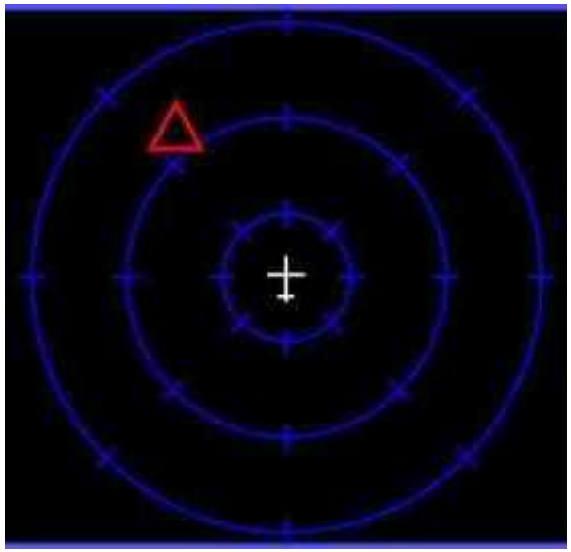
Threats and Enemy Capabilities

- The more a combat unit relies on the electromagnetic spectrum, the more vulnerable it is to the enemy's signals intelligence and electronic warfare actions.

- The enemy can
  - Detect a unit's devices which radiate electromagnetic energy to reveal its identity and location.
  - Monitor a unit's communications to reveal its intentions, combat capabilities, logistics and personnel status, and other critical operational and tactical information.
  - Inject false information into communications and information systems (CIS) to confuse and mislead a unit.
  - Interrupt a unit's use of the electromagnetic spectrum, thereby degrading its ability to receive and process intelligence, plan operations, and execute C2 functions.

Indications and Warning

- SIGINT is often the principal provider of indications and warning (I&W) because adversaries often reveal their intentions, locations, and movements in their communications and other electronic emissions.



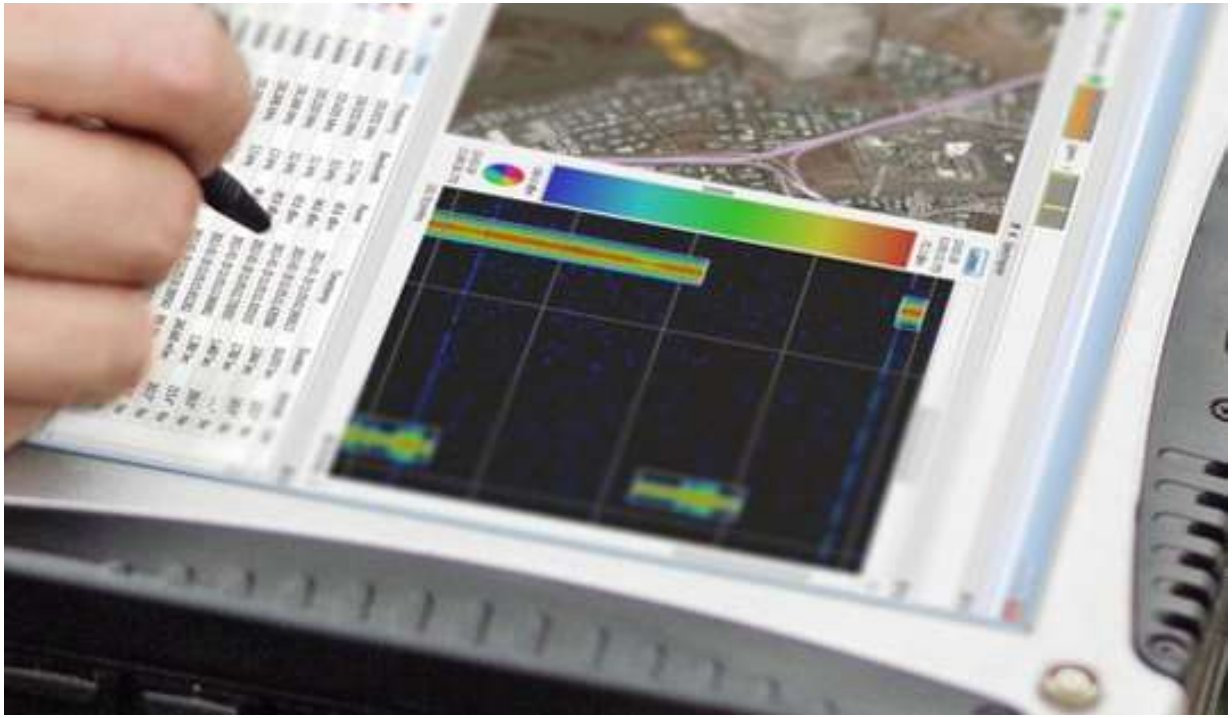
Targeting

SIGINT supports targeting by providing key operational and locational intelligence on enemy C2 operations and facilities, weapons systems, force compositions, and dispositions.

Information provided through SIGINT can identify high value and high payoff targets and help develop options for attacking these targets.

SIGINT also supports all-source intelligence gain and loss assessments of potential enemy targets.

Discussions



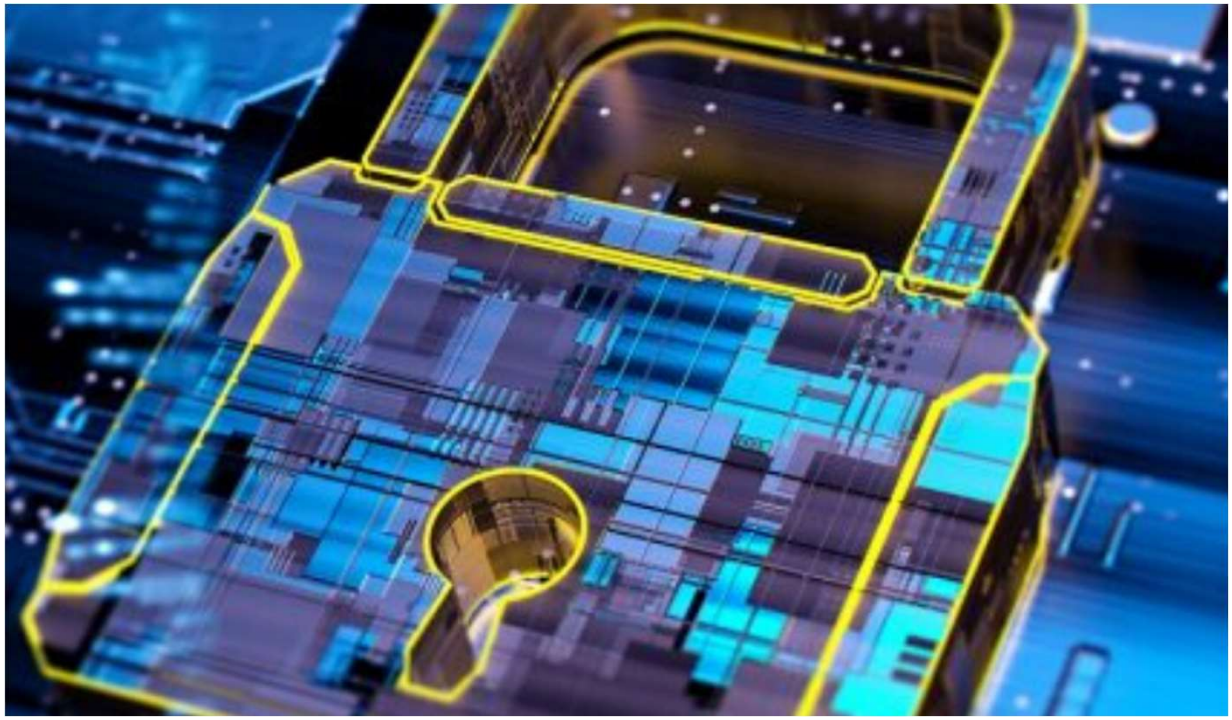
Signal Intelligence System Capabilities

- Today's new and emerging threats are driving the need for updated signal intelligence system capabilities that not only can detect, collect and analyze the newest signal threats, but geolocate them as well.
- SIGINT system combines precision RF, SDR and Direction Finding (DF) hardware with the next generation of the software.

COTS Signals Intelligence Capability

- COTS signals intelligence capability to provide unparalleled signal survey, search, detection, visualization, collection, wideband recording, DF/geolocation, analysis and reporting

VHF/UHF/SHF Dual Polarized Monitoring Antenna



ELINT

- ELINT includes the interception and analysis of noncommunications transmissions, such as radar.
- ELINT is used to identify the location of an emitter, determine its characteristics, and infer the characteristics of supported systems.

ELINT using Software Defined Radio (SDR)

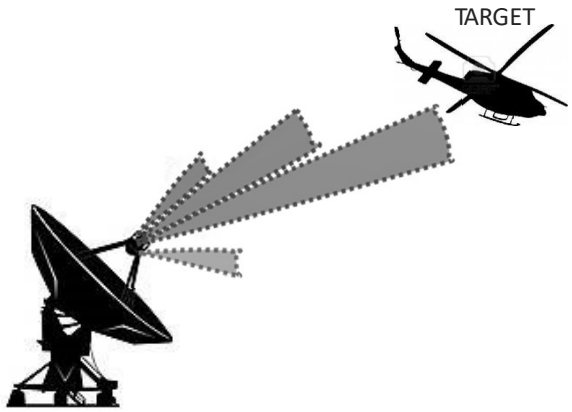
- DSP/FPGA for electronic intelligence
-
- Developing electronic intelligence systems using signal processing hardware: FPGA, DSP and I/O modules
- Mix FPGA with DSP processors, and to integrate that processing power with very fast communications ADCs, capable of sampling IF signals directly
- Most modern governments use electronic intelligence (ELINT) technology to gather information - often used in the fight against terrorism and crime.
- Typically, Electronic Intelligence systems have embraced the concepts of the "Software Radio" - a radio receiver in which as many elements as possible are reprogrammable.
- This allows one system to be used to decode signals from many different sources.

Technical ELINT

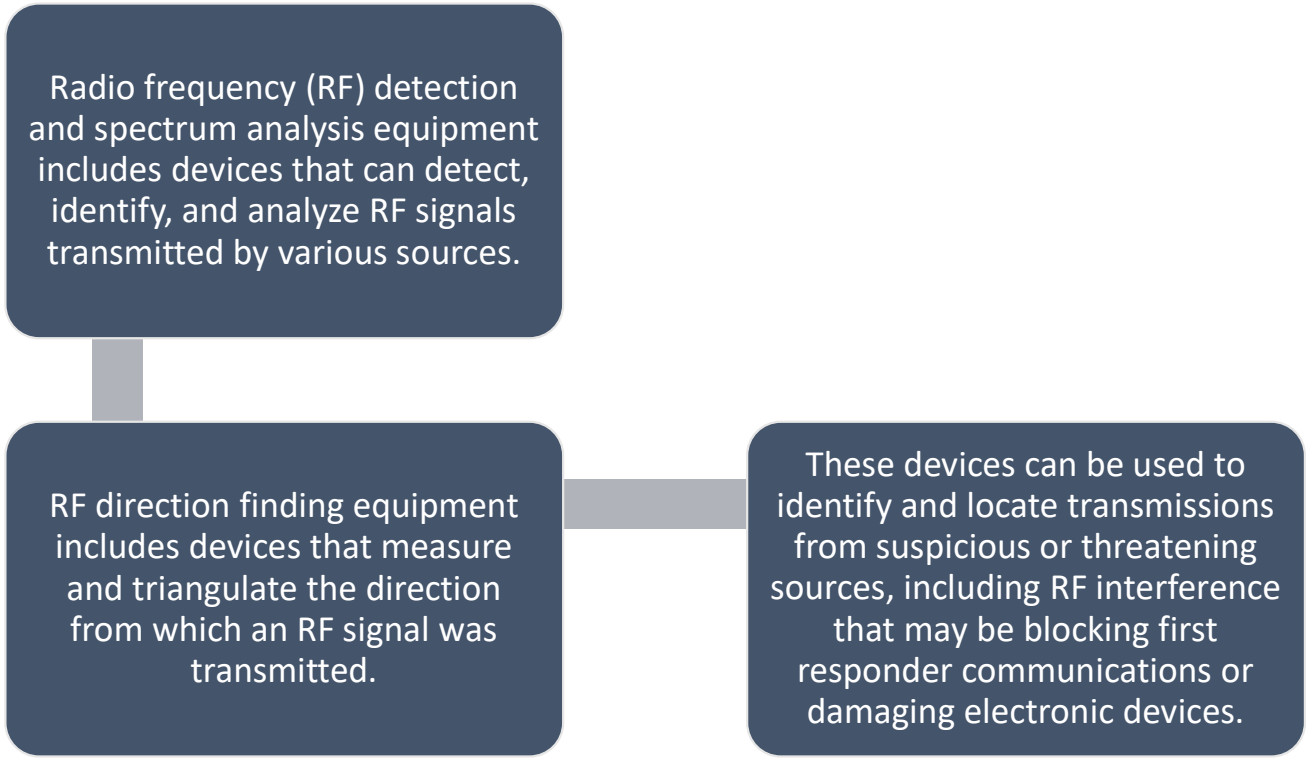
- Technical ELINT focuses on the details of the signals. In the case of a radar, the characteristics of interest can be the transmitted power, the frequency, the pulse repetition timing, or the shape of a pulse.

- The capabilities of a radar can be deduced from these parameters.

- For instance, the detection range of a radar against a given type of aircraft or missile can be computed, or the best ways to jam the radar can be determined.



Radio Frequency Detection, Spectrum Analysis, and Direction-Finding (DF) Equipment



Case Study 1: ALION VERSATILE RF AUTOMATED MONITORING SYSTEM

- The Alion Versatile RF Monitoring System (V-RAMS) is capable of RF detection, spectrum analysis, and direction finding.
- Key spectrum analysis features of the V-RAMS include stored trace, parametric and in-phase and quadrature (I/Q) data; terrain mapping of potential interference sources; editable spectrum masks; and a licensed database of emitters for identification of detected signals.
- The V-RAMS can detect RF signals within the bandwidth of 20 MHz to 6 GHz. An optional range extension to 75 GHz is also available. The scanning bandwidth of the V-RAMS ranges from 10 Hz to 650 kHz.
- The noise floor of the V-RAMS is 22 dB at 2 GHz. An external low noise amplifier (LNA) can increase the sensitivity of the receiver.
- The vendor specifies the entire system weighs less than 30 pounds. The price of the V-RAMS, as quoted by Alion, is $76,270.53.

https://www.alionscience.com/protecting-essential-communication-systems/

Example of Radio Direction Finding (DF) System

- Direction Finder Set is a tactical, man-transportable system that provides search, intercept, and DF on communications signals in the HF/VHF/UHF and other bands.

- **Direction finding** (**DF**), or **radio direction finding** (**RDF**), is the measurement of the **direction** from which a received signal was transmitted. This can refer to **radio** or other forms of wireless communication, including radar signals detection and monitoring (ELINT/ESM).

RF Direction Finding

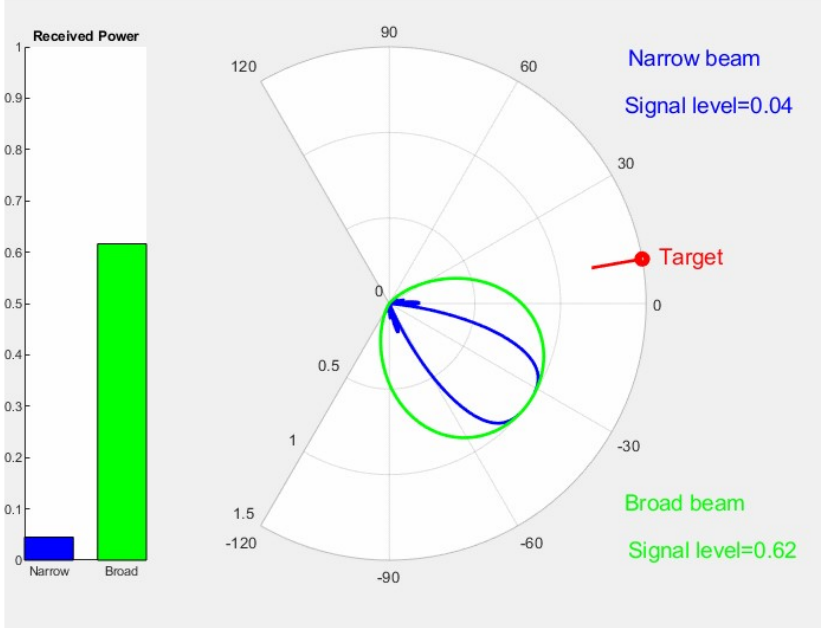
- RF direction finding is used in several applications:
  - SIGINT: such as the direction of a threat, the location and movement of enemy transmitters and the direction of enemy jammers.
  - Radio monitoring: the location of sources of interference and of illicit transmitters
  - Search and Rescue: the location of RF search and rescue beacons.
  - Science: the tracking of animals in their environment.

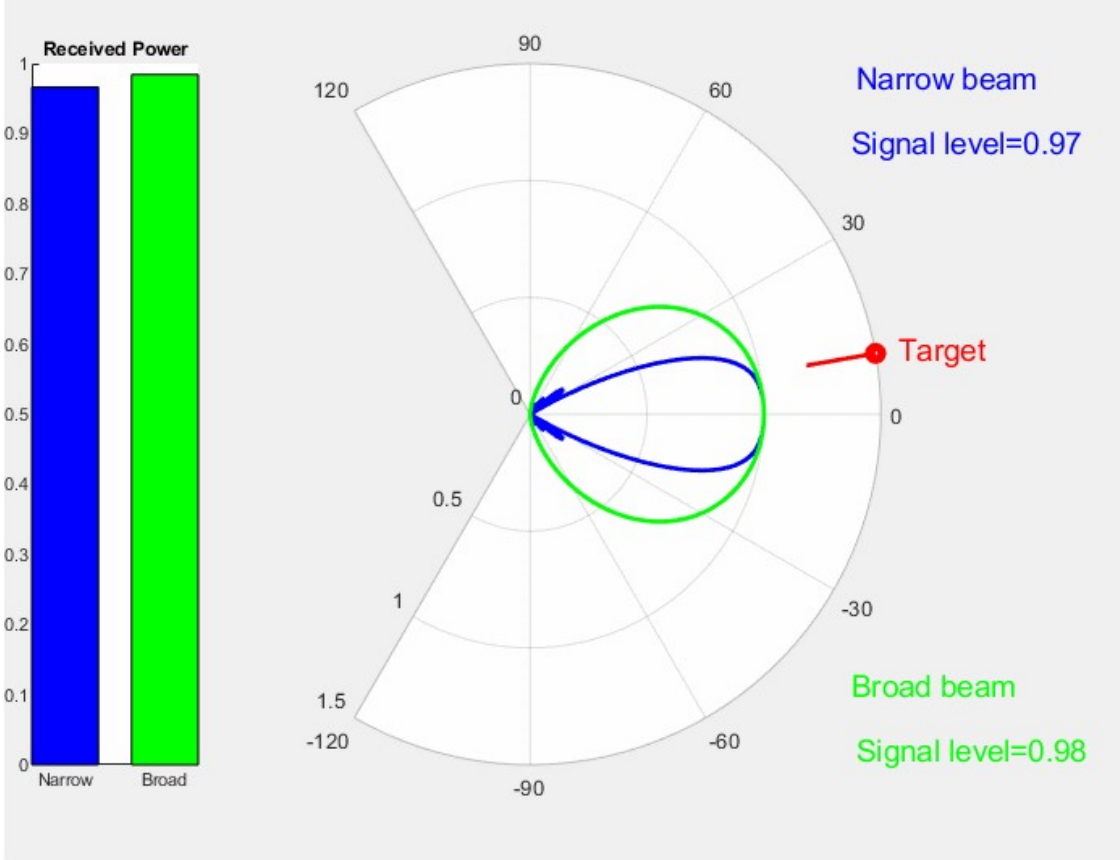
Single Receiver DF Systems: Directional Antenna Technique

- The simplest RF direction finding system consists of a directive antenna and a single receiver. The antenna is pointed in different directions while the receiver indicates the received signal strength. Only the magnitude of the signal is used to determine the direction of a transmitter.
- The accuracy of this technique is dependent on the width of the antenna radiation pattern.
- A narrow beam will improve the accuracy but will increase the time spent scanning all possible directions.
- If the beam is too narrow the target may even be missed especially with intermittent transmission sources.
- A broad beam will decrease the bearing accuracy.

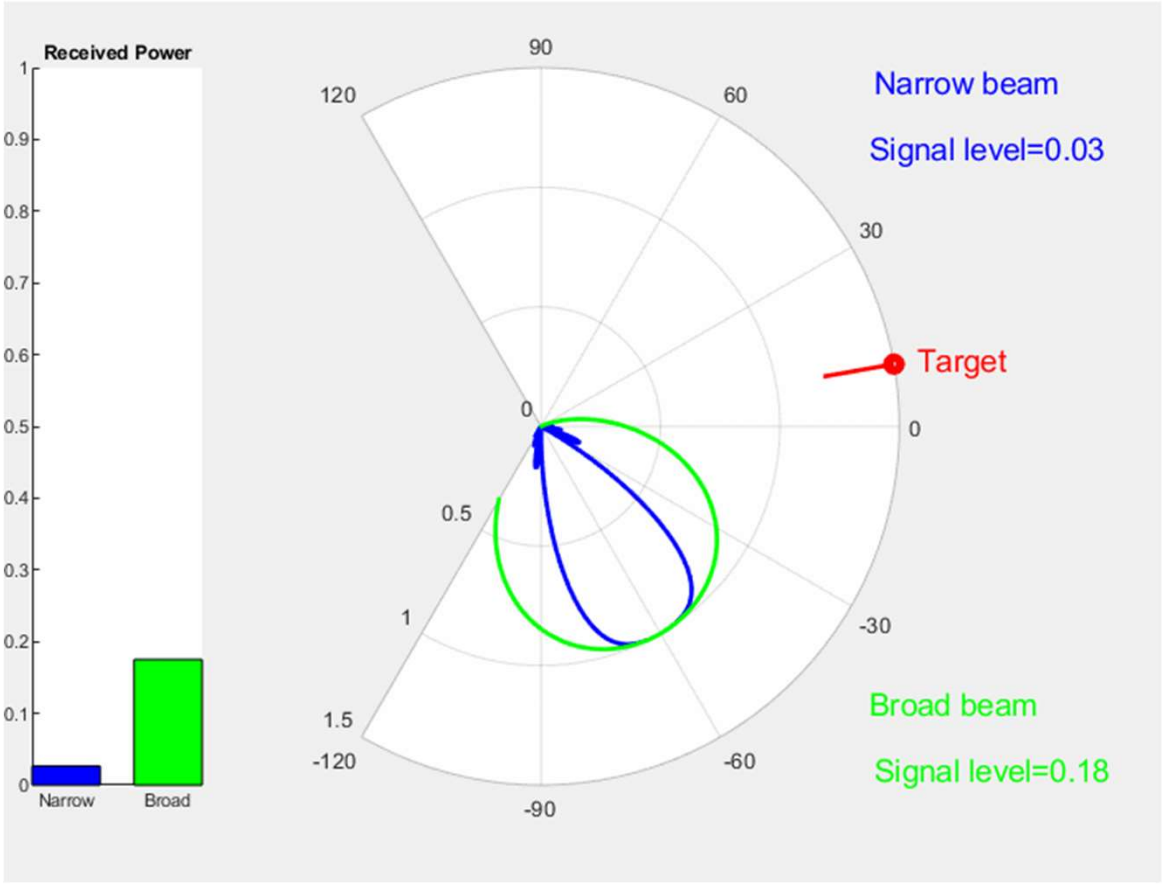
- In SIGINT applications is commonly used for broad band high frequency DF. These systems are fully motorized and use knowledge of the antenna radiation pattern to improve accuracy.

Directional Antenna Technique





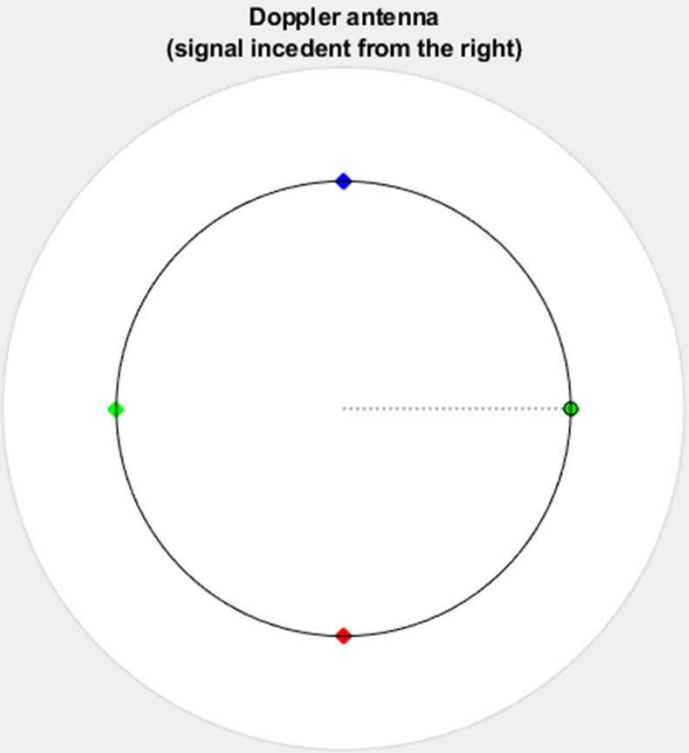
Directional Antenna Technique



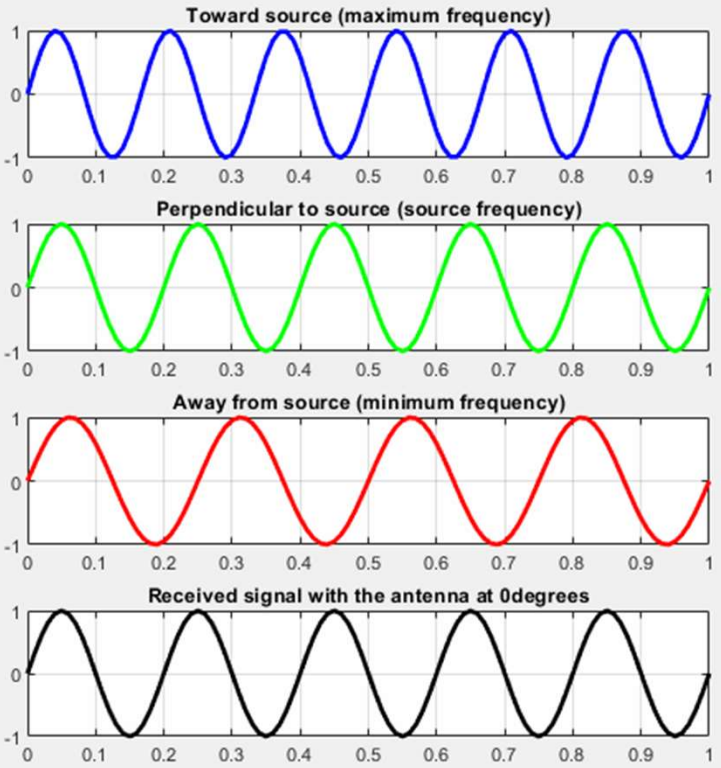
Doppler and Pseudo-Doppler Technique

- The Doppler DF system uses a single receiver connected to an omni directional antenna that is physically rotated on the circumference of a circle.
- As the antenna moves toward the radio source, doppler shift will increase the received frequency and the received frequency will decrease as the antenna moves away from the source.
- The change in frequency (obtained by demodulation) is used to determine the direction of the radio source.
- The modern approach is to successively sample each antenna in a circular array of antennas, removing the need for any moving parts.
- This is referred to as Pseudo-Doppler DF.

Doppler and Pseudo-Doppler Technique



The circular trajectory of a doppler DF antenna. The received signal is incident from the right.

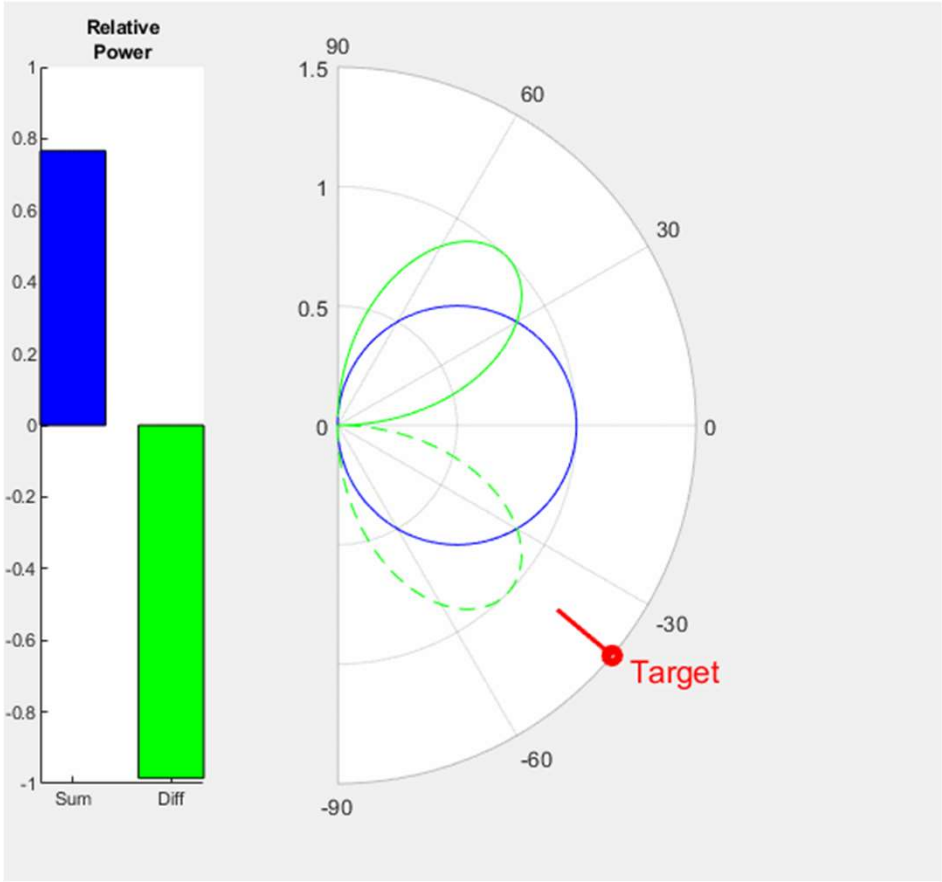


The received frequency at various positions along the trajectory of the antenna is shown in the right image of the figure. As the antenna moves away from the incident signal, the frequency increases (red graph) and as the antenna moves towards the incident signal, the frequency increases (blue graph). The black curve shows the received frequency response at the position indicated by black circle on the antenna diagram.

Two Receiver Systems: Mono-pulse Technique

- The mono-pulse or sum-difference RDF technique uses two antennas. The antennas are connected to a four-port combiner 180° hybrid that generates a sum and difference signal.
- Such sum and difference patterns are generated by means of closely spaced overlapping radiation patterns at boresight.
- These signals form sum and difference radiation patterns.
- The ratio of the sum and difference signals and knowledge of the sum and difference patterns are used to determine the direction of the transmitter.
- Phase information is used to determine on which side of the sum pattern the transmitter is.
- An advantage of this system is in its capability to determine the direction of a transmitter after receiving one pulse. Such pulse could be a mere few microseconds. Accuracies of 10meter over a 100Km distance has been reported.

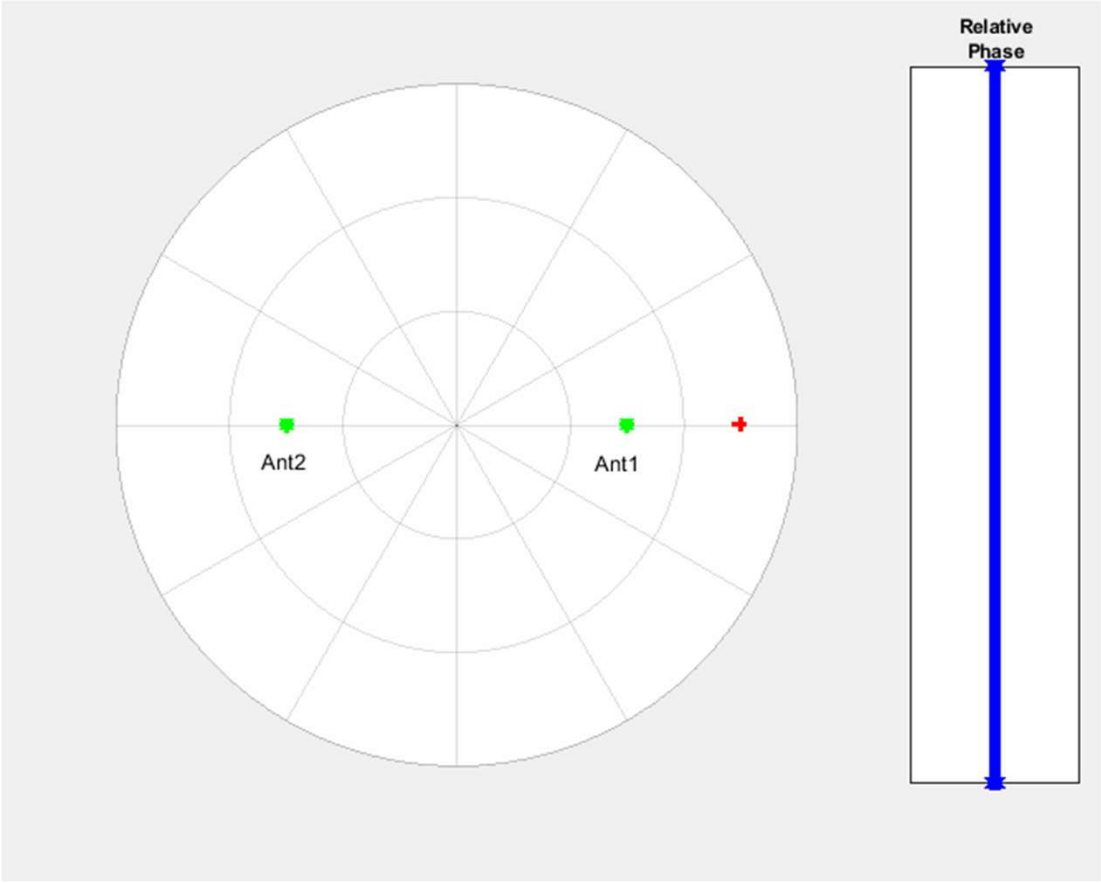
Two Receiver Systems: Mono-pulse Technique



Interferometer

- The relative difference in the phase of the signal received by two omni directional antennas spaced a set distance apart can be used to determine direction or angle of arrival of a RF signal.
- In the omni directional case, the interferometer does not have a way to determine if the signal arrives from the front or the back of the antennas.
- As the frequency increases (or electrical separation increases) ambiguities appear as the phase differences wrap.
- If the antennas are too close (electrical separation very small) then the resulting phase difference will be very small, and the system will not be able to determine the AOA.
- The frequency range of use is thus determined by the separation of the antennas and the noise figure of the receivers.

Interferometer



The image shows two omni directional antennas with the incident signal circulating around them.

The relative phase of the incident signal between the two antennas is shown in the image on the right.

This phase difference is used to determine the direction of the incident signal.

Adcock Antenna, Watson-Watt Method

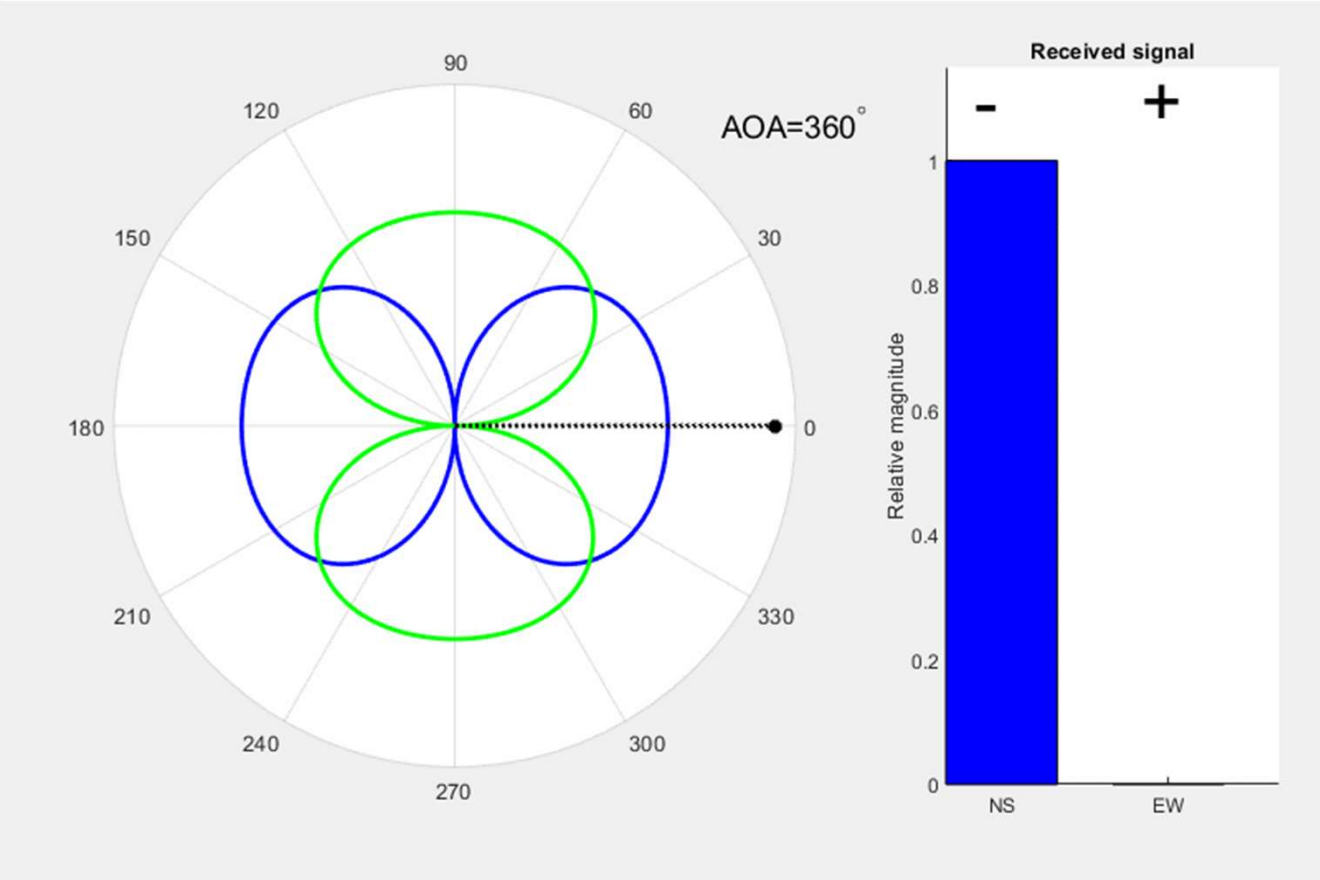
- An Adcock antenna uses two crossed loop antennas.
- The bearing of the RF signal is determined using the level of the signals received at each antenna.
- The method to process the information from a Adcock array is referred to as Watson-Watt.
- This is the best-known method of radio direction finding.

Adcock Array

- In a more general application four closely spaced omni directional antennas positioned in a square can be used to form an Adcock array.
- The opposing antennas are combined using a 180° combiner to form figure-of-8 patterns, which creates a unique set of magnitudes for any bearing direction.
- A Watson-Watt antenna cannot determine if a signal comes from the front or the back without the use of a third omni directional antenna to resolve the 180° ambiguity.

- The figure below shows the typical radiation pattern of an Adcock array. The received signal rotates around the array.
- The relative amplitude of the signal received by the two crossed loop antennas (or combined omni directional antennas) is shown on the right.
- The + and – at the top indicates the relative phase of the two crossed loops with respect to the omni. It is this relative phase that resolves the ambiguity.

Adcock Antenna, Watson-Watt Method



N Receiver Systems – Correlative RDF

With the technological improvements in receivers and digital processors, all the information produced by multiple antenna elements can be used to improve the performance of RDF systems.

Typically, the bearing is calculated using the phase differences of the signals received at the various antennas in the correlative array.

The correlative algorithm compares the phase differences of the incoming RF signals at each antenna to a set of calibration phases stored in the processor to determine the most likely AOA.

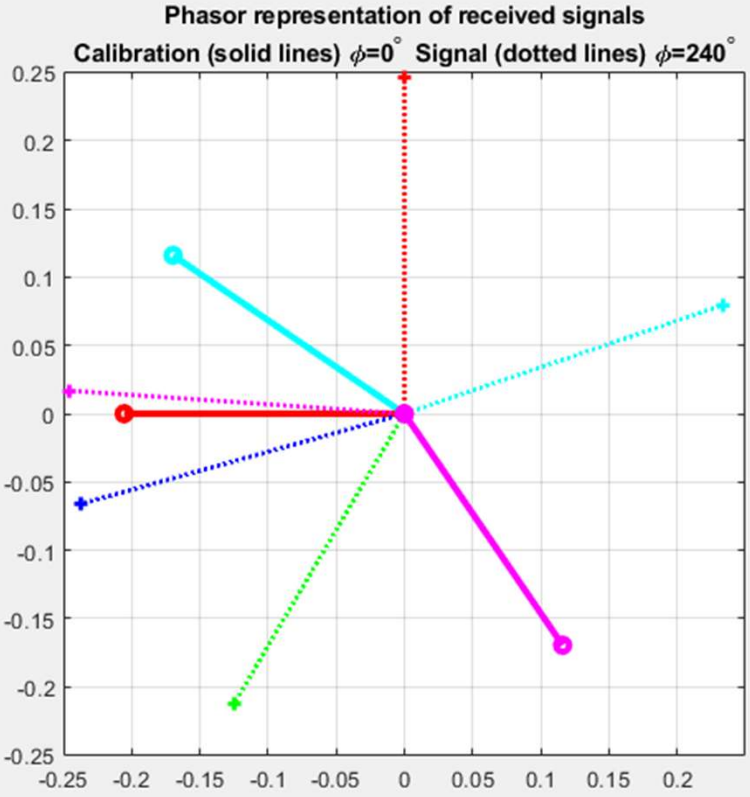
The correction function correlates the relative phases (and magnitudes for some correlators) of the received signals with the correlation table over all possible angles; the maximum of the correlation function indicates the AOA.

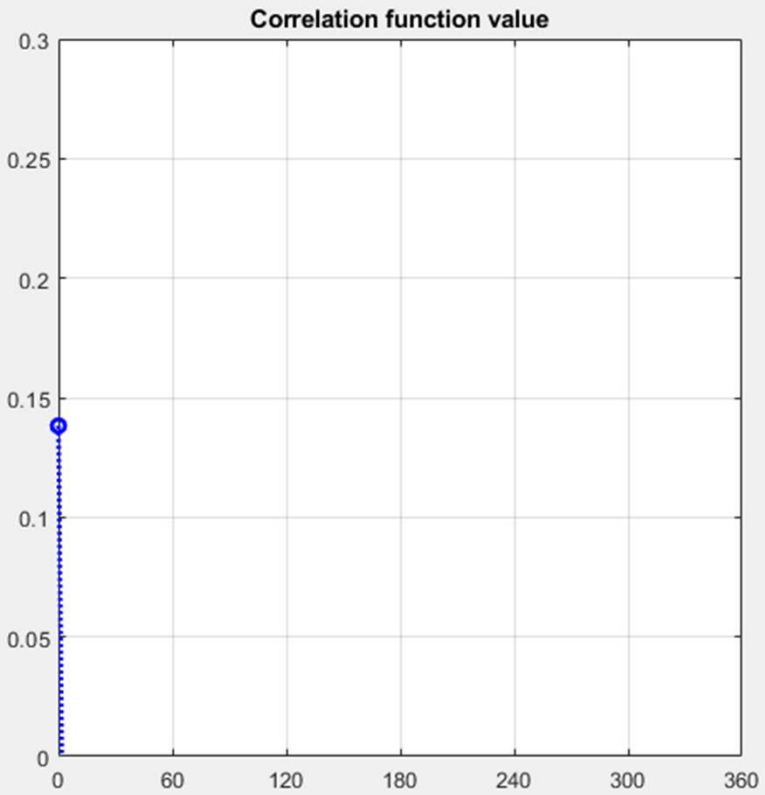
The calibration information can be obtained by calculation or by measurement of the antenna.

Correlative Array

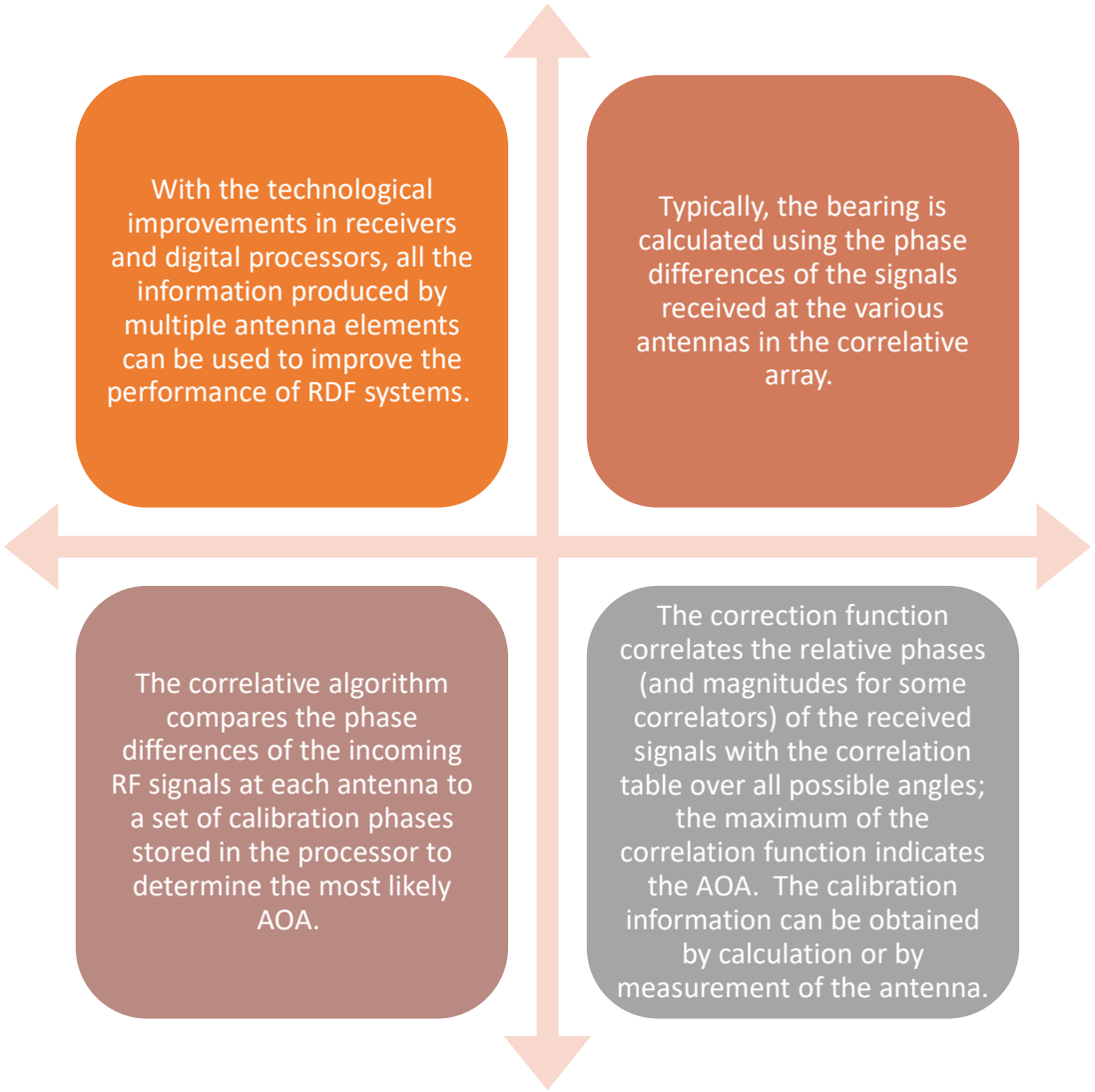
- The most common implementation of a correlative array is to have several omni directional antennas (typically four to nine antennas) in a circular pattern. In this configuration the differences in the phase of the incoming RF signal at each element is used by the correlative algorithm to determine the AOA.
- Cutting edge systems can use both magnitude and phase of an arbitrary number of antennas arbitrarily positioned to determine the AOA in 3D, not just in a horizontal plane.
- The spatial positioning of the antennas in the array is of critical importance to achieve good performance without introducing ambiguities.
- 3D calibration data (not just in azimuth but also in elevation) with elements spatially positioned in atypical configuration is used to determine the AOA in 3D.
- In many practical applications the patterns of the antennas will not be omni directional, clever algorithms can incorporate the magnitude information to improve RDF performance.
- Even an Adcock antenna can be characterized and used in conjunction with a corelative estimator to improve performance of the Watson-Watt method.

N Receiver Systems – Correlative RDF





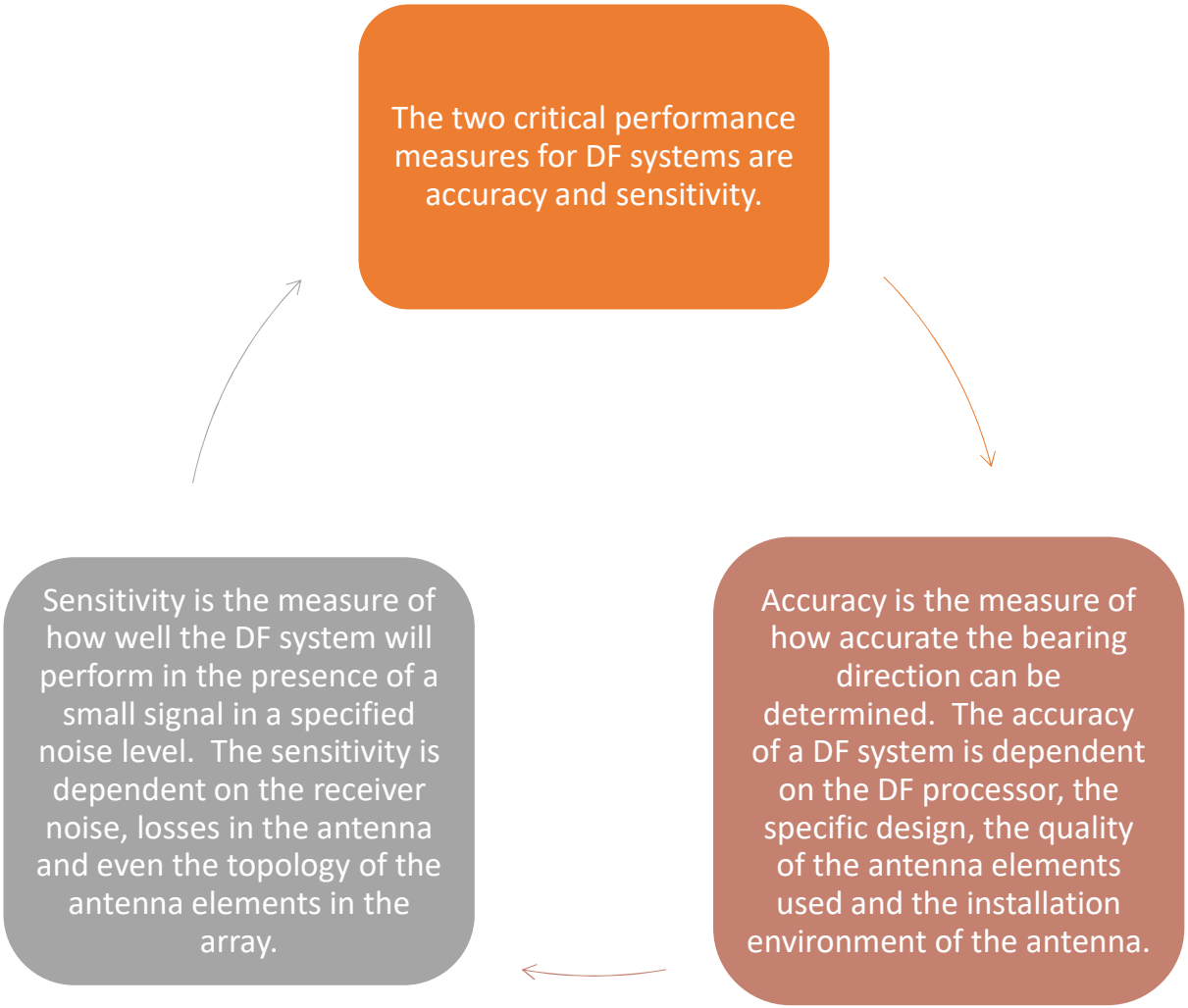
N Receiver Systems – Correlative RDF



Common Implementation of a Correlative Array

- The most common implementation of a correlative array is to have several omni directional antennas (typically four to nine antennas) in a circular pattern. In this configuration the differences in the phase of the incoming RF signal at each element is used by the correlative algorithm to determine the AOA.
- Cutting edge systems can use both magnitude and phase of an arbitrary number of antennas arbitrarily positioned to determine the AOA in 3D, not just in a horizontal plane.
- The spatial positioning of the antennas in the array is of critical importance to achieve good performance without introducing ambiguities. 3D calibration data (not just in azimuth but also in elevation) with elements spatially positioned in atypical configuration is used to determine the AOA in 3D.
- In many practical applications the patterns of the antennas will not be omni directional, clever algorithms can incorporate the magnitude information to improve RDF performance.
- Even an Adcock antenna can be characterized and used in conjunction with a corelative estimator to improve performance of the Watson-Watt method.

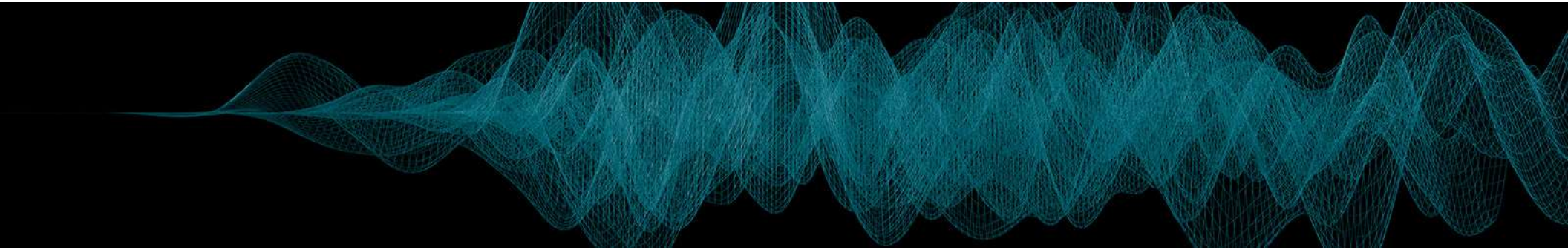
RDF Performance



APPLIED SIGNALS INTELLIGENCE ASI 2020 DF FIXED SITE

- The Applied Signals Intelligence ASI 2020DF Fixed Site is capable of RF detection, spectrum analysis, and direction finding.

- The technology is a fixed site sensor that can intercept and locate analog and digital RF emitters in the high frequency (HF), very high frequency (VHF), and ultra-high frequency (UHF) frequency bands. Application can record audio files, geolocation data, and digital mobile radio metadata, which can be stored on internal or external hard drives.



SIGINT Explained

SIGINT is the interception of signals for the purpose of gathering intelligence.

SIGINT is divided into three sub-disciplines:

Communications Intelligence (COMINT) which is the interception of communication between people and groups

Electronic Intelligence (ELINT) which is the intercepting of electronic signals which are not specifically used for communication

Foreign Instrumentation Signals Intelligence (FISINT), which is the collection of signals created by the testing and use of foreign weapons systems.

SIGINT Functional Planning

- SIGINT Functional Planning
- SIGINT Concept of Operations (ConOps)
- Enemy Characteristics
- Topography
- Planning Responsibilities

SIGINT Operational Planning

- SIGINT planning cycle and activities to enable an understanding and appreciation for the SIGINT effort.

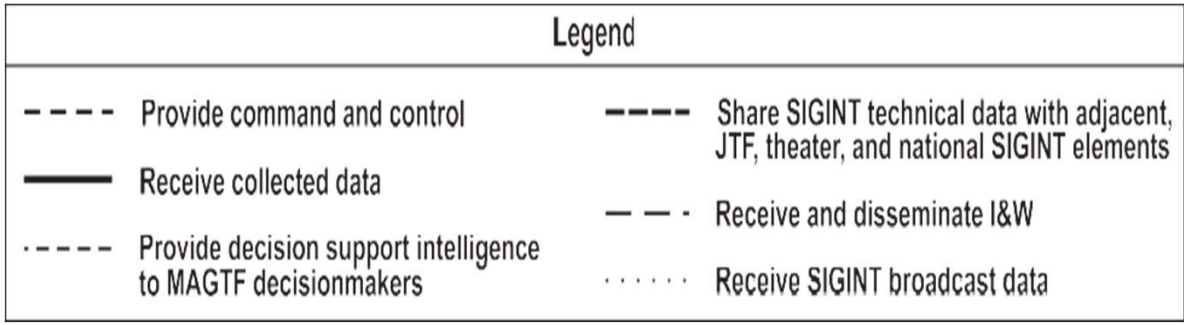
- The SIGINT cycle is in concert with the phases of the intelligence cycle.

SIGINT Operational Planning

- Planning and Direction
- Collection
- Processing and Exploitation
- Production
- Dissemination
- Utilization
- Coordination of SIGINT Operations

SIGINT Operational Architecture

- Provide C2
- Receive Collected Data
- Provide Decision Support Intelligence to Decisionmakers
- Share SIGINT Technical Data with Theatre and National SIGINT Elements
- Receive and Disseminate
- Receive SIGINT Broadcast Data



Planning and Direction

- The planning and direction phase of the intelligence cycle consists of those activities which identify and prioritize pertinent IRs and provide the means for satisfying them. Intelligence planning and direction is a continuous function and a command responsibility.

- The commander directs the intelligence effort; the intelligence officer manages this effort based upon the commander's intent, designation of PIRs, and specific guidance provided during the planning process. The intelligence planning and direction functions are:

- Requirements development.
- Requirements management.
- Collections management.
- Production management.
- Dissemination management.
- Intelligence support structure.
- Supervision of the intelligence effort.

- SIGINT planning is performed in concert with overall intelligence planning. It consists of those activities that identify pertinent IRs which have been tasked to SIGINT units and then provides the means for satisfying those Intelligent Requirements (IRs).

SIGINT planning and direction objectives include:

- Identifying intelligence requirements tasked to SIGINT elements.
- Preparing a SIGINT operations plan, to include integral SIGINT collection, production, and dissemination plans.
- Planning and establishing the SIGINT support system (e.g., CIS, logistics).
- Issuing orders and tasking to SIGINT units.
- Supervising and coordinating the SIGINT operations.

Security of Sensitive Compartmented Information

- SIGINT Special Security Officer
- Personnel Security Program
- Physical Security
- Information Systems Security

Emitter Technical Data

- Effective SIGINT operations require extensive technical information on the enemy's communications and information systems (CIS) resources and operations.

Enemy Command and Control and Supporting Communications and Information Systems

1. What and where are the enemy's critical C2 nodes and what are their vulnerabilities?
2. What types and categories of communications nets and networks are used by the enemy?
3. What echelons of command do the communications nets and networks serve?
4. What are the associated communications and noncommunications electronic emitters?
5. What are the tactics, techniques, and procedures used for enemy CIS operations? How do they relate to various threat functional activities?
6. How is information transferred among the enemy's units and command echelons?
7. Does the enemy employ communications emitters at all levels of command or does it rely on communications means less exploitable by SIGINT (e.g., fiber, wire, wireless, and messenger)?

Effect of Topography

- Terrain, physical obstructions, and vegetation in the area of operations have a major effect on the employment of SIGINT resources and their ability to exploit enemy signals.

- Proper placement of SIGINT collection and DF assets is essential for effective reception of adversary emanations. Several factors affect reception quality

Target Frequencies

- Many of the frequency ranges and power levels in use by the world's military and paramilitary forces require line-of-sight (LOS) or near-LOS paths from transmitter to receiver. Generally, the higher the frequency used, the greater the LOS influence and the more critical the accurate placement of SIGINT collection and DF equipment. Lower frequencies (particularly those below 30 MHz) generally do not require LOS paths. Consequent- ly, the placement of SIGINT collection and DF sites to exploit these frequencies may be located at greater distances from the target transmitters

Power Output

- The power output of a transmitter is an important factor in receiving the signal. To intercept some low-powered signals, SIGINT collection and DF assets must be located closer to the adversary's transmitter, often requiring SIGINT collection and DF teams to either collocate with or closely follow forward MAGTF combat units.

Antennas

- If the targeted adversary's system uses highly directional antennas, as do many multichannel systems, the SIGINT collection and DF site must be placed within the adversary's antenna radiating pattern.

Emitter Technical Data

Aspect	Technical and Operational Characteristics
Communications Operations and Emitters	
Frequency range and use	HF, VHF, UHF, etc.
Transmitter power	Hearability, SIGINT collection, and DF location requirements
Emission type	Single, multichannel, spread spectrum, frequency hopping, burst, etc.
Signal type	Analog or digital
Modulation	Analog and Digital Modulation: AM, FM, PM, ASK, FSK, PSK, PCM, QPSK, QAM etc.
Cryptologic system	Public, private key, none
System type	Voice, data, teletype, facsimile, video, combinations of some or all
Language use	Dialect, written, or voice
Miscellaneous	Communication procedures, emissions control practices, use of deception, security systems, etc.

Emitter Technical Data

Noncommunications Operations and Emitters

Fixed, mobile
Air, ship, vehicle, fixed- installation
Command post, type of weapon system
Band of operation
Pulse duration, pulse repetition frequency, etc.
Effective radiated power, effective range
Jamming, surveillance, targeting, C2, fire control, etc.

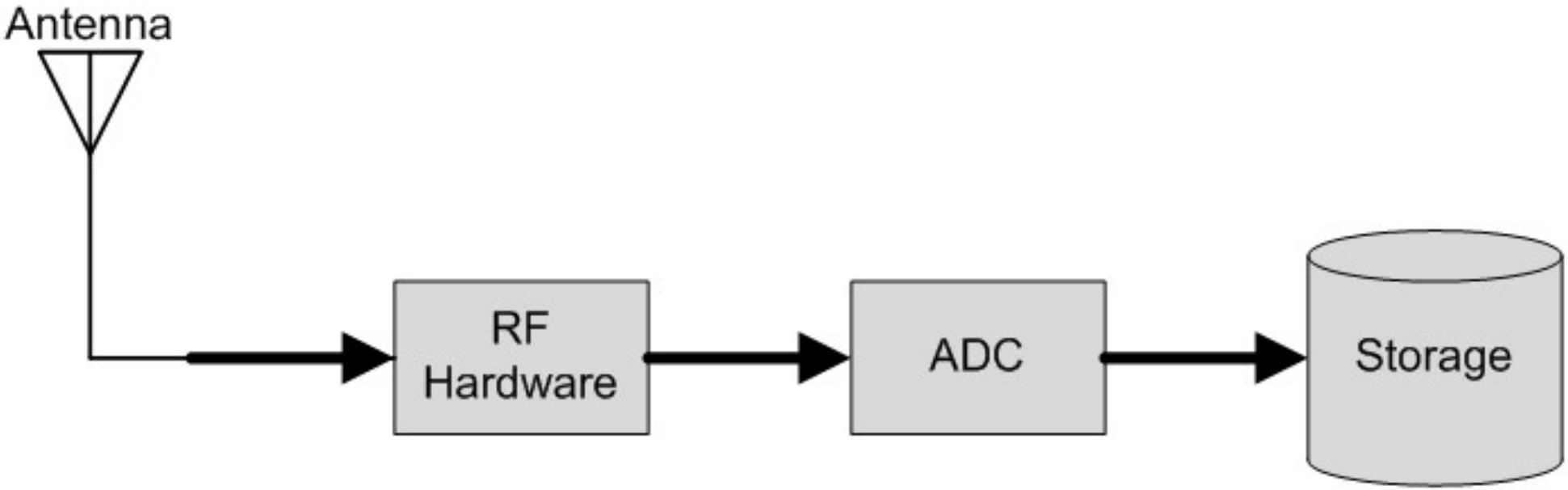
SIGINT / ELINT

- Signals intelligence, or SIGINT, refers to general information gathering via the interception of signals. SIGINT encompasses both the interception of communications-based signals (COMINT) and non-communications-based signals (ELINT).

- A simple but effective SIGINT solution can be comprised of just a few components, including an Antenna, RF Front-End Hardware, an ADC for digitization, and storage for the digitized data.

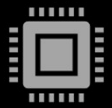
- At small bandwidths and sample rates such a system can be simple, but as signal bandwidths and sample rates increase the link between the ADC and Storage becomes more and more difficult to implement.

A Simple SIGINT Receiver Architecture



FPGA system architecture for high-end data digitization, signal processing, and storage

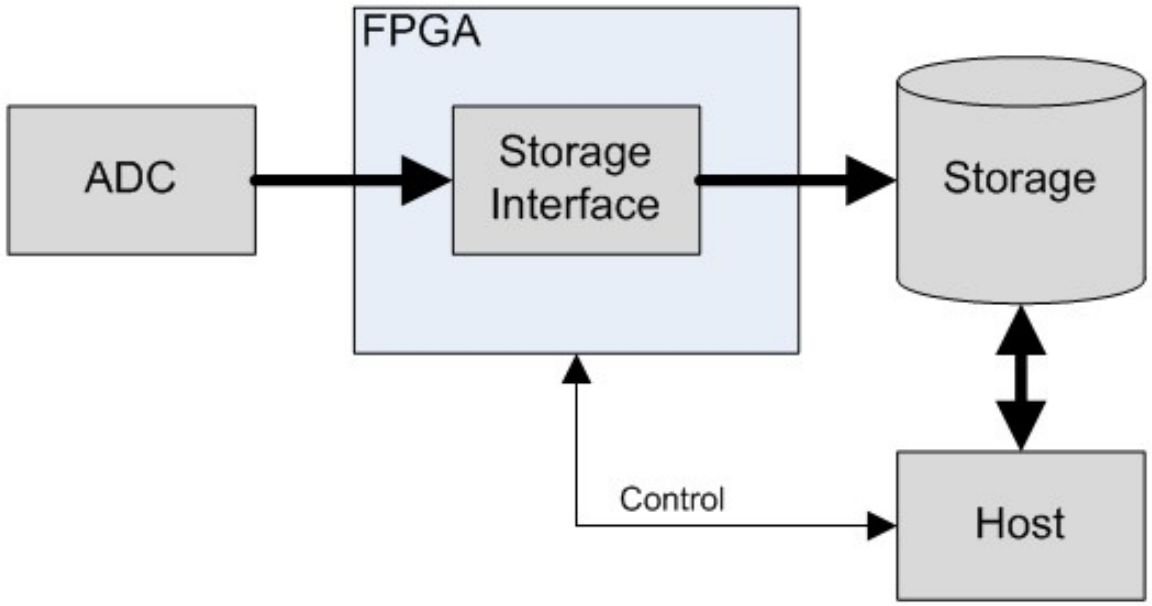
FPGAs are well suited for receiving and transmitting large bandwidths of data and provide an effective bridge between ADC and storage.



An FPGA can receive multiple GHz worth of bandwidth from an ADC and turn it right around to a storage device, presuming you can find storage capable of managing the multi-GB/sec rates coming from the FPGA.

A Host is included for simple storage control and data offloading and analysis, which is often done offline.

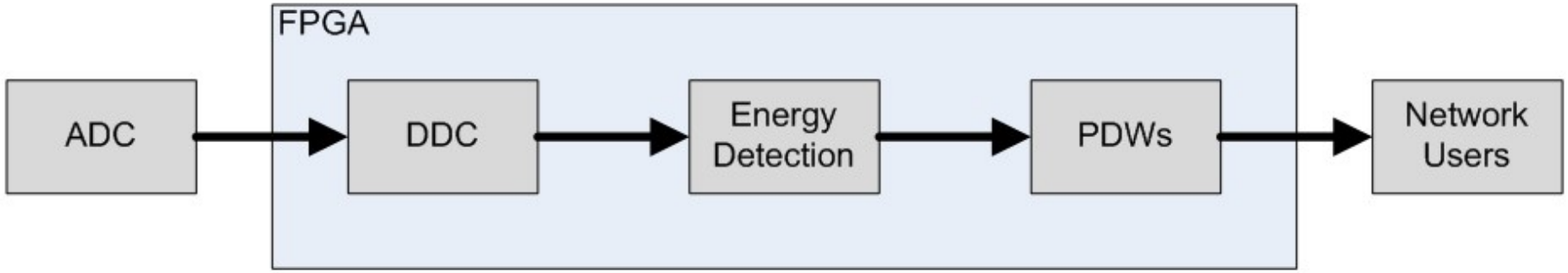
A Simple SIGINT Implementation



Performing SIGINT Functionality in FPGAs

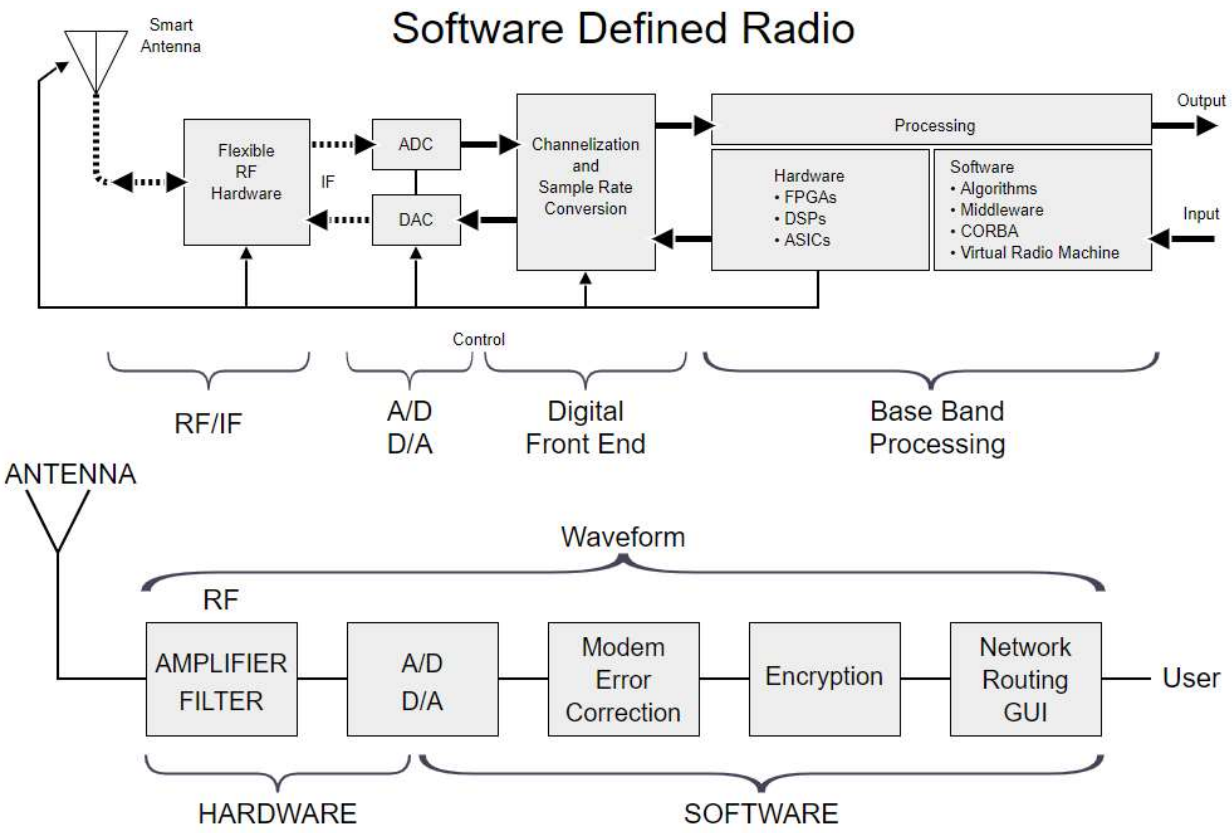
- Consider the block diagram, where instead of simple data storage we're now interested in tuning into a smaller portion of the band with a Digital Down Converter (DDC), implementing an Energy Detector, then generating Pulse Descriptor Words (PDWs) for the detected pulses and disseminating them to users.

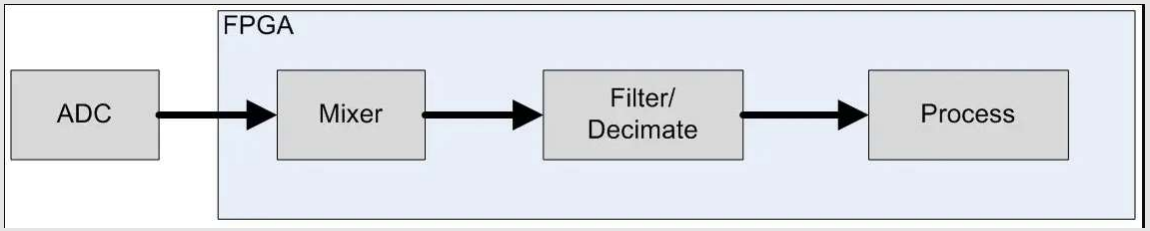
More complicated SIGINT systems



SW Defined Radio

- Software-Defined-Radio (SDR) is a communication system in which radio components including mixers, filters, modulators/demodulators, and detection circuits are implemented in a programmable medium to provide increased flexibility and capabilities. This is shown in block diagram form below.

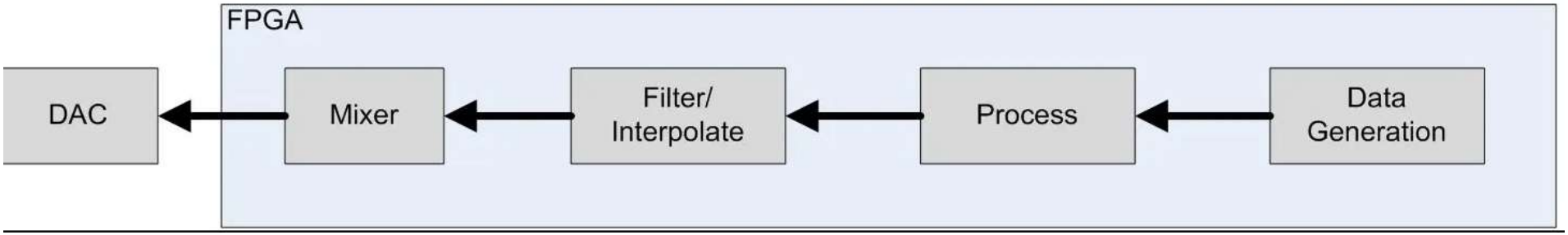




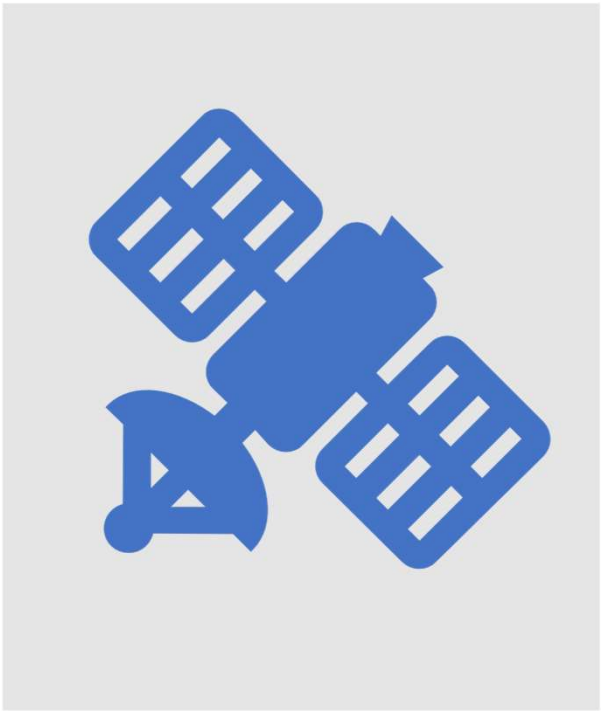
A Typical SDR Receiver

- An idealized SDR would include several “hard” or fixed components including an Antenna, front-end RF Hardware, and an ADC or DAC, while the rest of the functionality would be implemented in a “soft” or programmable medium.
- The most common “soft” device is a general-purpose processor, but processors lack the I/O bandwidth and processing capabilities necessary for implementing SDRs for all but the simplest architectures.
- Thankfully well architected FPGA systems can provide both the I/O bandwidth necessary, and the processing capabilities needed for implementing complex SDRs, and they can do so at multi-GHz sampling rates and GHz-range bandwidths.
- FPGAs are digital devices, so for a receiver the FPGA input would come from an Analog-to-Digital Converter (ADC) as shown below.
- A typical process would start with a mixer that rotates the signal intermediate frequency (IF) to DC, would flow through a filter-and-decimation process to reduce the bandwidth to that of interest, and might conclude with demodulation, energy detection, storage, or other processes.

A Typical SDR Transmitter



Characteristics of SIGINT Satellites



- Active use of equipment for collecting during the First and Second World Wars.

- The first ELINT was put into space on board the experimental p satellite Discoverer-13 in August 1960.
- The Scotop equipment was intended to record the signals of Soviet radars which were tracking the flight of American space objects. The launch of the first specialized ELINT satellites, which received the designation of "Ferret," was begun in the USA in 1962.
- The tasks of space-based SIGINT were subdivided into two groups: ELINT against antiaircraft and ABM radars (discovery of their location, operating modes and signal characteristics) and SIGINT against C3 systems

Example of SIGINT Equipment Types

- Electronic attack (EA) set provides the capability to conduct spot or sweep jamming of single-channel, encrypted or unencrypted, voice or data signals operating in the standard military frequency range of 20-79.975 MHz from selected mobile platforms (e.g., high mobility, multipurpose wheeled vehicles, mobile electronic warfare support system, helicopters and UAVs).

- In addition, it can provide additional channels of high-power VHF voice and/or data communications when not being used as a jamming system.

- When employed as a tactical, general-purpose, low-VHF jamming system, it could have a 250-watt radio frequency linear amplifier that produces a nominal 200 watts of effective radiated power (ERP) using a standard omnidirectional whip antenna.

- To provide required jamming, the system must be employed and operated from a location with an unobstructed signal line of sight to the target enemy's communications transceiver.

Antenna Types for SIGNINT and ISR Applications

- In-Class Activity

- https://www.jemengineering.com/isr-sigint-elint-monitoring-antennas/

SIGINT Equipment Functions

- Intercept
- Collection
- Automated DF (radio direction finding)
- EA
- Spot or sweep jamming
- Target emitter position data
- SIGINT-processing, analysis and reporting system
- Communications Intelligence (COMINT) system: intercept, collection, radio direction finding, analysis, reporting, and collection management support
- Mobile SHF satellite communications (SATCOM) system that uses commercial or military satellites to receive, transmit, and process secure, voice, data, and video teleconferencing (VTC)

Example of SIGINT Equipment Technical Characteristics

Frequency Coverage	Example of Modulation
20-80 MHz (collection and DF expandable to 500 MHz)	AM, FM, ICW, SSB, FSK
0.5 MHz - 40 GHz	conventional, low probability of intercept
.5 - 500 MHz	AM, FM, ICW, SSB, FSK
20 - 79.975 MHz	FM
25 - 550 MHz, 800 - 1300 MHz	AM, FM
1 - 1500 MHz	AM, FM, CW, SSB
5 - 1500 MHz	AM, FM
0.1 - 2036 MHz	AM, FM, CW, SSB
20 - 1000 MHz intercept and DF	AM or FM
.1 - 1900 MHz intercept 25 - 1000 MHz DF	AM, FM, USB, LSB, CW
0.1 - 30 MHz	AM, FM, CW
25 - 1300 MHz	AM, FM, SSB
0.1 - 1999.80 MHz	AM, FM, CW, SSB
.15 - 108 MHz & 115.15 - 223 MHz	AM, FM, SSB
20 - 1000 MHz intercept	AM or FM
0.5 - 29.999 MHz	AM, FM, CW, SSB
1 - 2000 MHz intercept 25 - 1000 MHz DF	AM, FM, USB, LSB, CW
.1 - 1900 MHz intercept 25 - 1000 MHz DF	AM, FM, USB, LSB, CW
0.5 - 29.999 MHz	AM, FM, CW, SSB
20 - 500 MHz	AM, FM, CW, pulse
.5 MHz - 1.0 GHz	AM, FM, CW, pulse

Modulation Types

AM (Amplitude Modulation	Normal mode for CB radios in the US. Works well for voice transmissions, not as well for high fidelity transmissions like music due to a high signal to noise ratio.
USB/LSB aka SSB (Upper/Lower Single Sideband)	Single sideband modulation (SSB) is an efficient mode for radio transmissions, it's especially common in HF frequencies including 10 meters and CB. If you're operating a base station in a frequency range less than 50 MHz, there's a decent chance you'll be operating with single sideband as mode. The reason this mode isn't always used is that it requires extra time to "tune in" by using a clarifier control by each radio operator. With the extra time it takes to clarify the person you're talking to; you can't just pick up the mic and start talking right away.

1. CW is continuous wave: A continuous wave or continuous waveform (CW) is an electromagnetic wave of constant amplitude and frequency.
2. Interrupted continuous wave (ICW): Modulation in which there is on-off keying of a continuous wave.

Case Study: AN/ALQ-218 RWR/ESM/ELINT Sensor System

- Northrop Grumman's AN/ALQ-218 Radar Warning Receiver / Electronic Support Measures / Electronic Intelligence (RWR/ESM/ELINT) Sensor System is the U.S. Navy's choice for airborne situational awareness and signal intelligence gathering.

https://datasheets.globalspec.com/ps/4192/NorthropGrumman/5FA00AFB-E183-4E5C-8A1B-B34F6C581ACF#:~:text=A%20passive%2C%20high%20performance%20SIGINT,8A%20Poseidon%20ASW%2FASUW%20aircraft

AN/ALQ-218 RWR/ESM/ELINT Sensor System

- The AN/ALQ-218 is the world's only receiver system proven to provide high Probability of Intercept (POI) under "Look-Through" operations, enabling DF & Geolocation, parameter measurement and Intentional Modulation on Pulse (IMOP) detection while simultaneously supporting enemy radar threat jamming.
- The AN/ALQ-218 also supports Specific Emitter Identification (SEI) characterization.
- The AN/ALQ-218 utilizes a unique combination of short and long baseline interferometer techniques along with a patented passive ranging algorithm to provide precision Geolocation of all ground-based emitters.
- ELINT signal analysis software is easily provided via the NGC PASS (Parameterizer & Analysis Software System) tool which receives signal data from analog or digital sources and provides measurement tools for analysis in either pre-detected or Pulse Descriptive Word (PDW) domain.

SIGINT EW Support

- EW Support
- EW Attack
- EW Protection

AN/ALQ-218 system features

- Broad Radio Frequency Range: Bands 0, 1, 2 and band 3
- Signal Types: Radar (Pulsed & CW) with optional COMMs support
- High Sensitivity and Dynamic Range
- Dynamic Tuning in sparse signal environment (Jamming)
- Passive Precision Geolocation expandable to targeting accuracies
- Specific Emitter Identification (to USG MISPE standards)
- Commercial Interference Mitigation (in bands 0 & 1)
- Enhanced Fine Frequency Measurement supporting Jamming
- Latest generation Frequency Domain Digital Channelized Receiver
- TRL 9 Technology (Hardware and Software)

Discussions