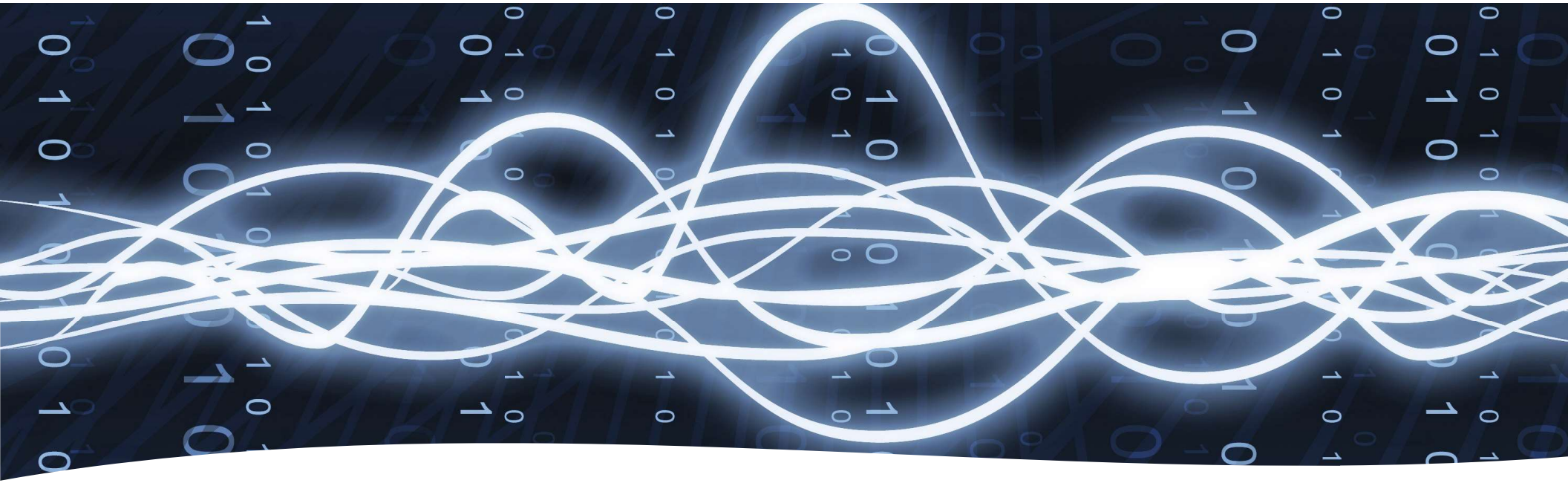
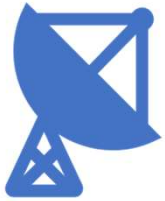


Part 1

SIGINT 101

TONEX

What is SIGINT?



- SIGINT is intelligence derived from electronic signals and systems used by foreign targets, such as communications systems, radars, weapons systems, etc..

- SIGINT provides a vital window for our nation into foreign adversaries' capabilities, actions, and intentions.

SIGINT 101

- What is Signals Intelligence (SIGINT)?
- Component of command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) applications
- Image intelligence (IMINT), signals intelligence (SIGINT), and measurement and signatures intelligence (MASINT) collection systems
- Collection and exploitation of signals transmitted from various communication systems, radars, and weapon systems
- Technical definitions
  - Targeting
  - Intercept management
  - Signal detection
  - Traffic analysis
  - Electronic order of battle
- Communications Intelligence
- Electronic Signals Intelligence
- SIGINT and MASINT
- SIGINT and Electronic Warfare (EW)

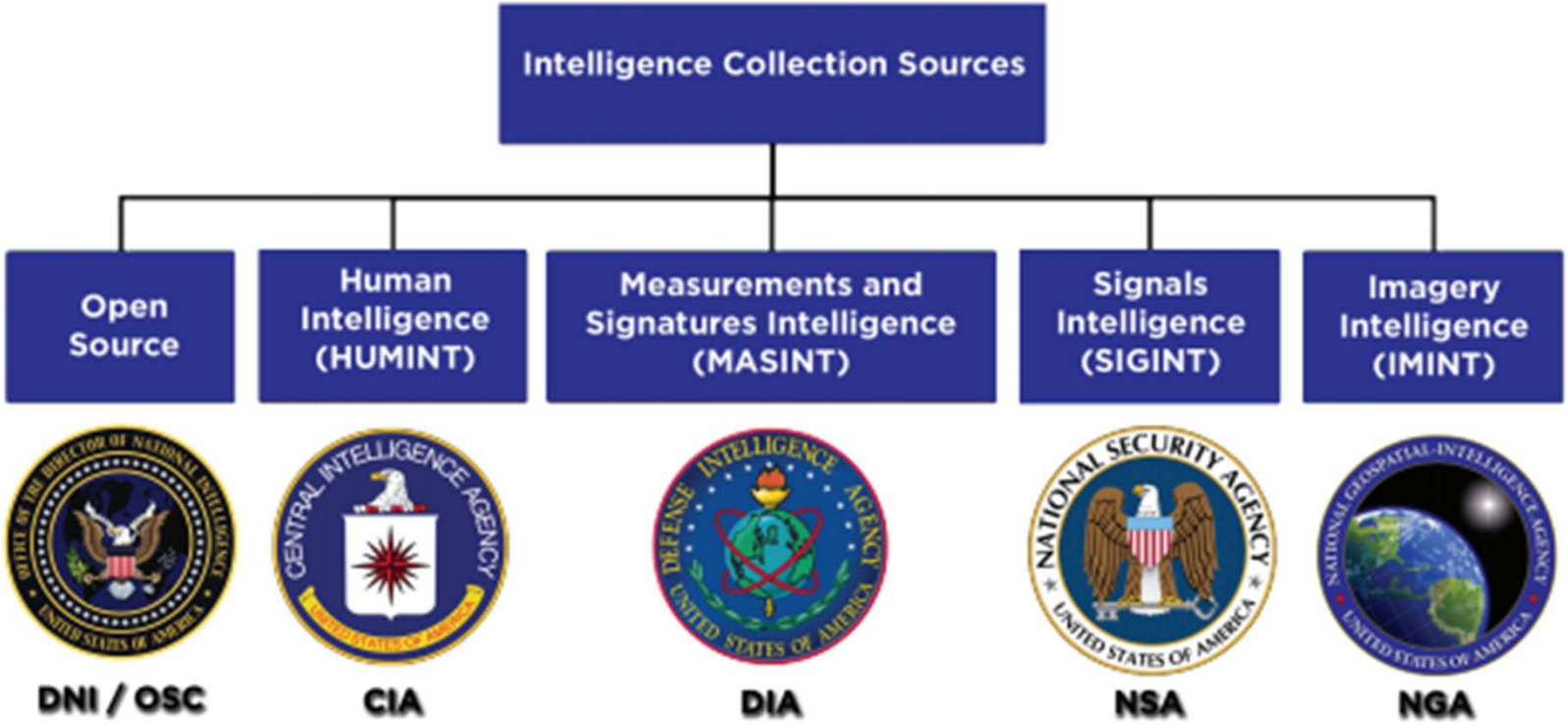
What is Intelligence?

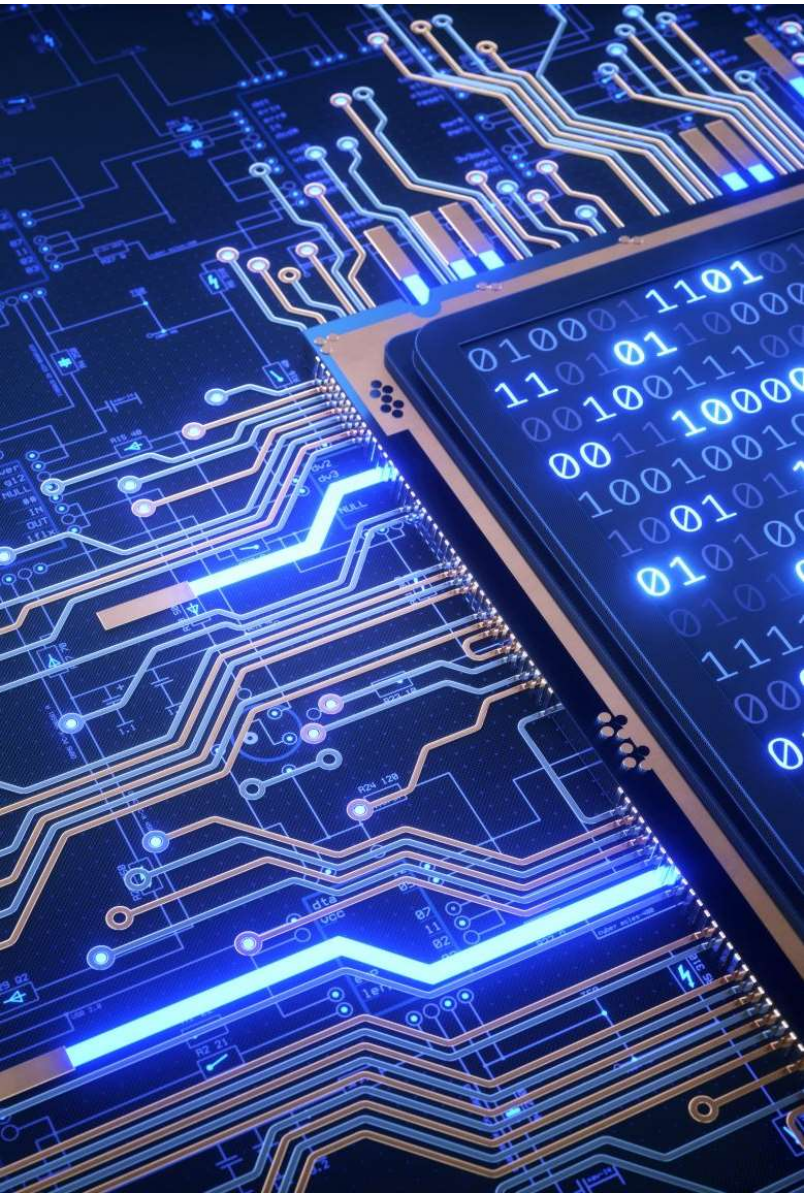
- Intelligence is information gathered within or outside that involves threats to a nation, its people, property, or interests, development, proliferation, or use of weapons of mass destruction, and any other matter bearing on the national or homeland security.
    - Intelligence can provide insights not available elsewhere that warn of potential threats and opportunities, assess probable outcomes of proposed policy options, provide leadership profiles on foreign officials, and inform official travelers of counterintelligence and security threats

Intelligence Collection Disciplines or the "INTs."

Signals Intelligence (SIGINT)	**Imagery Intelligence (IMINT)**	**Measurement and Signatures Intelligence (MASINT)**
Geospatial Intelligence (GEOINT)	**Human Intelligence (HUMINT)**	**Open-Source Intelligence (OSINT)**

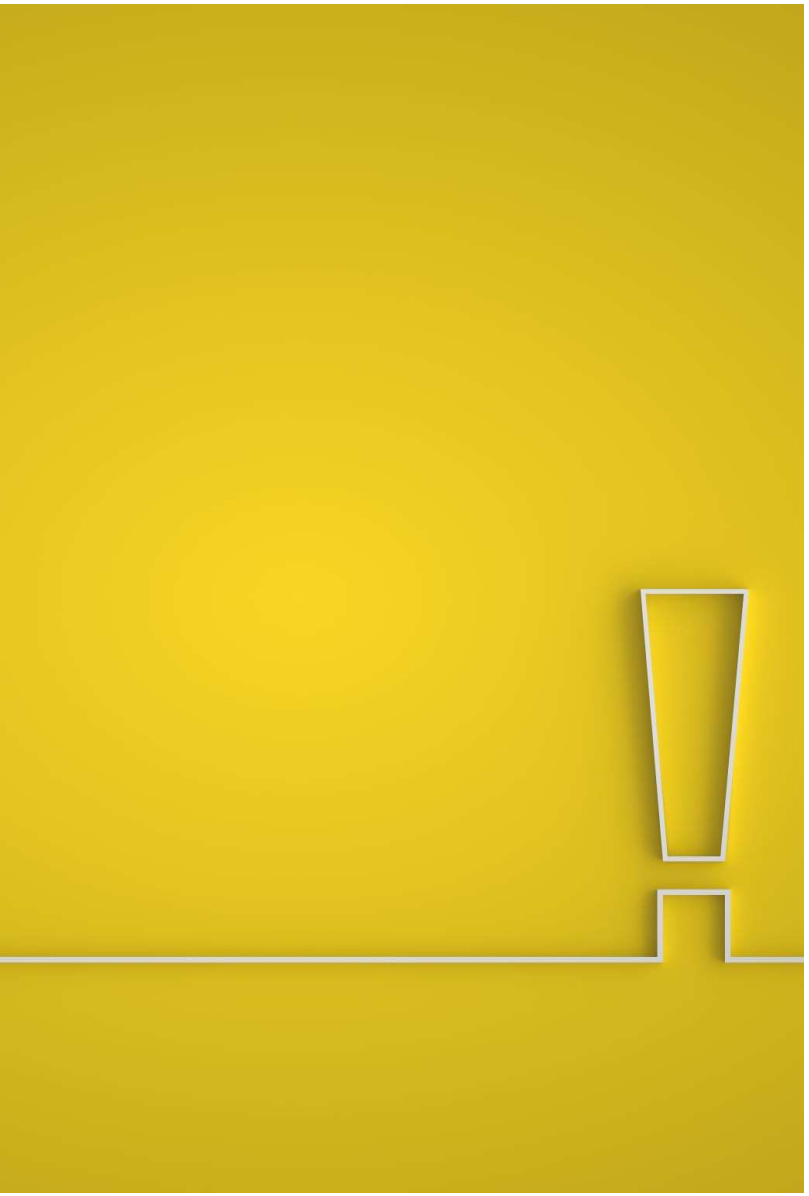
Intelligence Collection Sources (USA)





Signals Intelligence is derived from Signal Intercepts

- Signals intelligence is derived from signal intercepts comprising, either individually or in combination, all communications intelligence (COMINT), electronic intelligence (ELINT), and foreign instrumentation signals intelligence (FISINT), however transmitted.



COMINT, ELINT and FISINT

- COMINT, one of the primary SIGINT disciplines, includes information derived from intercepted communications transmissions.
  - COMINT targets voice and teleprinter traffic, video, Morse code traffic, or even facsimile messages. Assuming access is possible, COMINT can be collected from the air waves, cable, fiber optics, or any other transmission medium.
- 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.
- Foreign instrumentation signals intelligence (FISINT), consists of intercepts of telemetry from an opponent's weapons systems as they are being tested.
  - Telemetry units provide designers with information on a prototype's guidance system operation, fuel usage, staging, and other parameters vital for understanding operational characteristics. These data enable the designer to evaluate the performance of the prototype. However, if intercepted, they also provide an adversary with the ability to estimate the capability of the prototype.

Signals intelligence collection can be performed from a variety of platforms

- Examples include overt ground collection sites, such as the Russian facility at Lourdes, Cuba; ships and aircraft; and covert locations inside the United States. SIGINT facilities can monitor transmissions from communications satellites, as well as terrestrial facilities.
- This is particularly important because many international transmissions originating in the United States depend on communications satellites for passage overseas.
- Communications satellites supporting the transmission of U.S. Government, private sector, and public communications include the International Maritime Satellite system INMARSAT), the International Telecommunications Satellite system (INTELSAT),and the European Satellite system (EUROSAT).
- International communications satellites are routinely monitored by foreign intelligence services, including the Russian and Chinese intelligence services.
- Most collection capabilities targeting the United States are either ground or sea based, and target line-of-site or satellite communication systems.
- Space-based collection systems can also collect COMINT, FISINT, and ELINT.

SIGINT Summary

Electronic intelligence (ELINT) and communications intelligence (COMINT) are the two main sub-fields of signals intelligence (SIGINT).

- **Signals Intelligence (SIGINT)** refers to electronic transmissions that can be collected by ships, planes, ground sites, or satellites.
- ELINT and COMINT are the two main sub-fields of signals intelligence (SIGINT). ELINT is intelligence gathered using electronic sensors.
- COMINT is a type of SIGINT and refers to the interception of communications between two parties.
- In ELINT, intelligence gathered is generally those other than personal communications. The purpose is often to ascertain the capabilities of a target, such as the location of radar. The sensors might be used to gather that data may be active or passive. A given signal is analyzed and compared to recorded data for known signal types.
- If the signal type is recognized, that information can be recorded; it can be classified as new if no match is returned. Data gathered by ELINT is generally classified.

Types of Intelligence

- The Intelligence Cycle (IC) is a process of collecting information and developing it into intelligence for use by IC customers. The steps in the process are direction, collection, processing, exploitation, and dissemination.

- IC products can either be based on a single type of collection or “all-source,” that is, based upon all available types of collection.

- IC products also can be produced by one IC element or coordinated with other IC elements, and delivered to IC customers in various formats, including papers, digital media, briefings, maps, graphics, videos, and other distribution methods.

Signals Intelligence (SIGINT)

- **Signals Intelligence (SIGINT)** can be defined as a category of intelligence comprising either individually or in combination all communications intelligence (COMINT), electronic intelligence (ELINT), and Instrumentation Signals Intelligence (FISINT), however transmitted; or more simply as intelligence derived from communications, electronic, and foreign instrumentation signals.

Other SIGINT Categories

- Signals intelligence (SIGINT) consists of several categories. Communications intelligence (COMINT) is directed at the analysis of the source and content of message traffic.

- While most military communications are protected by encryption techniques, computer processing can be used to decrypt some traffic, and additional intelligence can be derived from analysis of patterns of transmissions over time.

- Electronic intelligence (ELINT) is devoted analysis of non-communications electronic transmissions. This would include telemetry from missile tests (TELINT), or radar transmitters (RADINT).

SIGINT = ELINT+COMINT+FISINT

COMINT	•Interception of communications between people or machines
ELINT	•Detection and analysis of non-communications electronic transmissions •Electronic Warfare: radiation from electronic systems, jamming radiation, weapon systems and missiles
FISINT (Foreign Instrumentation Signature INTelligence)	•FISINT is also considered as a subset of MASINT (measurement and signature intelligence).
MASINT	•Scientific and technical intelligence obtained by quantitative and qualitative analysis of data •Data= metric dependence, modulation, plasma or hydromagnetic •MASINT can provide specific weapon system identifications, chemical compositions and material content and a potential adversary's ability to employ these weapons.

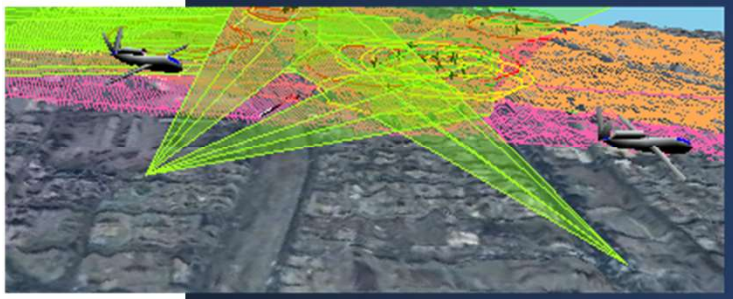
MASINT

- **Measurement and Signatures Intelligence (MASINT)** is a relatively little-known collection discipline that concerns weapons capabilities and industrial activities.

- MASINT includes the advanced processing and use of data gathered from overhead and airborne IMINT and SIGINT collection systems.

- Telemetry Intelligence (TELINT) is sometimes used to indicate data relayed by weapons during tests, while electronic intelligence (ELINT) can indicate electronic emissions picked up from modern weapons and tracking systems.

- Both TELINT and ELINT can be types of SIGINT and contribute to MASINT.



Signals Intelligence (SIGINT)

Electronic intelligence (ELINT) and communications intelligence (COMINT) are the two main sub-fields of signals intelligence (SIGINT).

- **Signals Intelligence (SIGINT)** refers to electronic transmissions that can be collected by ships, planes, ground sites, or satellites.
- ELINT and COMINT are the two main sub-fields of signals intelligence (SIGINT). ELINT is intelligence gathered using electronic sensors.
- COMINT is a type of SIGINT and refers to the interception of communications between two parties.
- In ELINT, intelligence gathered is generally those other than personal communications. The purpose is often to ascertain the capabilities of a target, such as the location of radar. The sensors might be used to gather that data may be active or passive. A given signal is analyzed and compared to recorded data for known signal types.
- If the signal type is recognized, that information can be recorded; it can be classified as new if no match is returned. Data gathered by ELINT is generally classified.

Six Basic Intelligence Sources

There are six basic intelligence sources, or collection disciplines:

SIGINT—Signals Intelligence

IMINT—Imagery Intelligence

MASINT—Measurement and Signature

HUMINT—Human intelligence

OSINT—Open-Source Intelligence

GEOINT—Geospatial Intelligence

Signals Intelligence (SIGINT)

- Signals intelligence (SIGINT) consists of several categories. Communications intelligence (COMINT) is directed at the analysis of the source and content of message traffic.

- While most military communications are protected by encryption techniques, computer processing can be used to decrypt some traffic, and additional intelligence can be derived from analysis of patterns of transmissions over time.

- Electronic intelligence (ELINT) is devoted analysis of non-communications electronic transmissions. This would include telemetry from missile tests (TELINT), or radar transmitters (RADINT).

Signals Intelligence (SIGINT)

SIGINT = COMINT+ELINT+FISINT

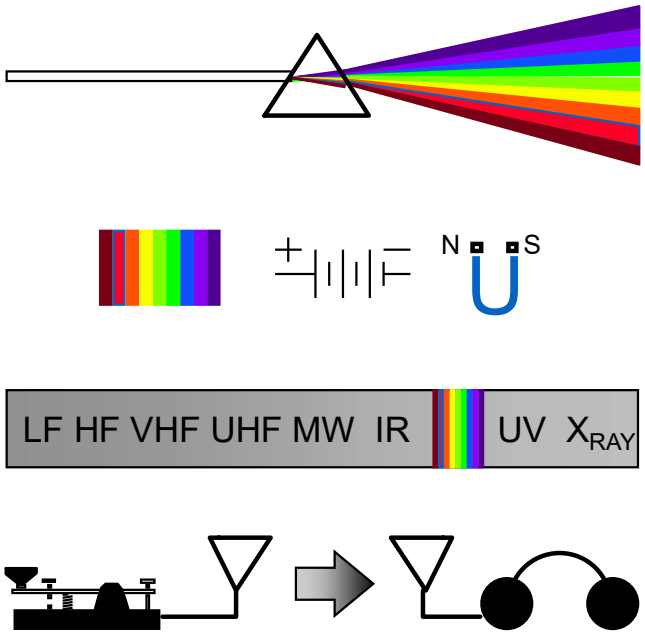
Communications Intelligence (COMINT) + Electronic Intelligence (ELINT) + Foreign Instrumentation Signals Intelligence (FISINT)

Note

Signals intelligence (SIGINT) is “a category of intelligence comprising either individually or in combination all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted”.

Simply, SIGINT is intelligence gained by exploiting an adversary’s use of the electromagnetic spectrum with the aim of gaining undetected firsthand intelligence on the adversary’s intentions, dispositions, capabilities, and limitations.

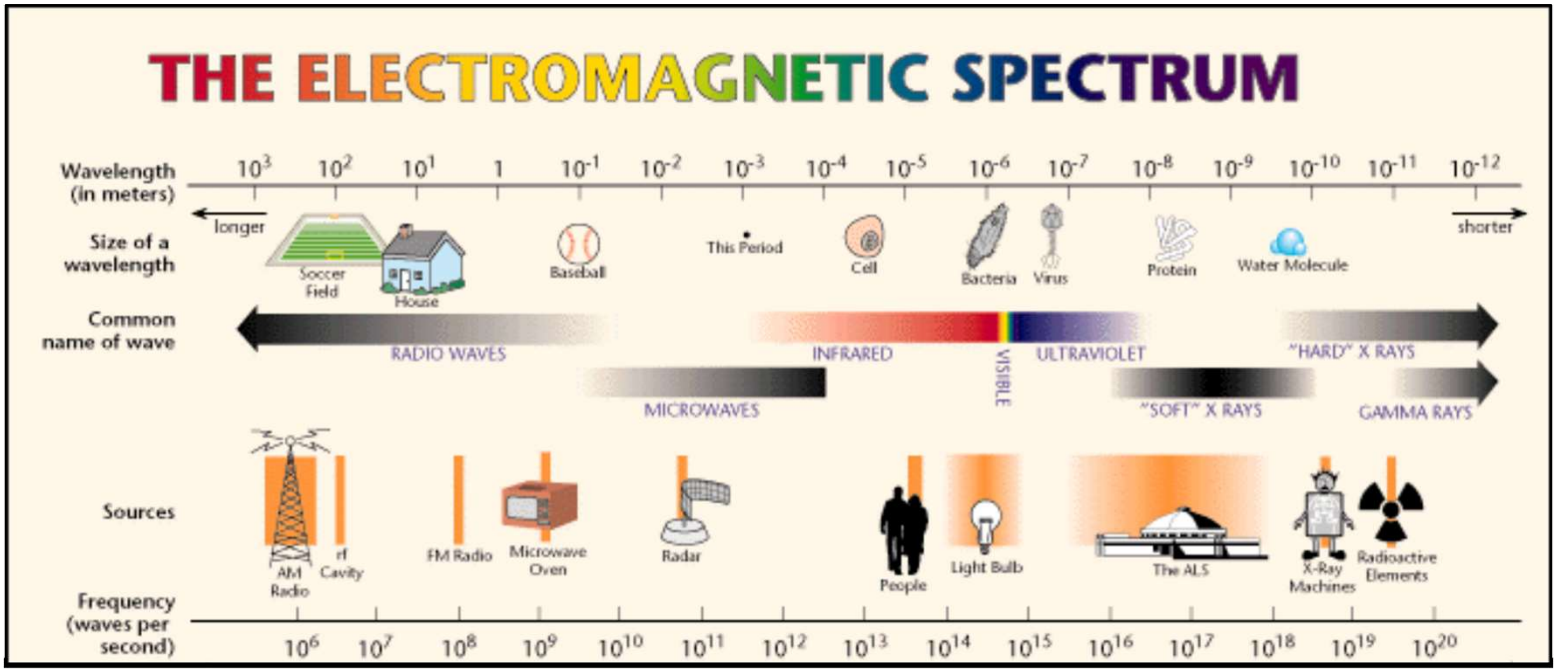
How Did We Get Here?



Days before radio…..

- **1680** Newton first suggested concept of spectrum, but for visible light only
- **1831** Faraday demonstrated that light, electricity, and magnetism are related
- **1864** Maxwell's Equations: spectrum includes more than light
- **1888** German physicist Heinrich Hertz produced and detected electromagnetic waves in his laboratory. His goal was to verify some of the predictions about these waves that had been made by Scottish physicist James Clerk Maxwell.
- **1890's** First successful demos of radio transmission

Electromagnetic Waves

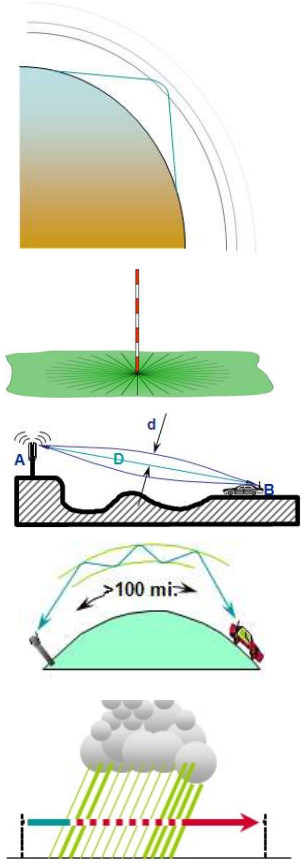


Courtesy Berkeley National Laboratory

Radar Frequencies

Radio Frequencies and How they Propagate

Band Name		Freq.	Length	Example Uses	How Signal Propagates
ELF	Extremely Low Frequency	3 – 300 Hz.	100,000 – 1,000 KM.	Inductive coupling to trace wiring in walls, etc.; AC mains power to users	No practical propagation outside the conducting wires
VLF	Very Low Frequency	3 – 30 KHz.	100 – 10 KM.	100+ mile long buried antennas transmit codes to submerged submarines	Surface waves and Guided/trapped between the earth and the ionosphere
LF	Low Frequency	30 – 300 KHz.	10 - 1 KM.	WWVB clock time signals, rudimentary navigational beacons, defunct LORAN	Surface (Ground)waves and Guided between earth and the ionosphere D-Layer
MF	Medium Frequency	300 – 3,000 KHz.	1,000 – 100 Meters	Commercial AM broadcasting, maritime offshore radio	Surface (Ground)waves and reflection off of ionosphere E and F-Layers at night
HF	High Frequency	3 – 30 MHz.	100 – 10 Meters	Short wave broadcasting, HF military and aeronautical links, amateur radio, CB radio	Very Localized Surface (Ground)waves and refraction in ionosphere E, F1, and F2 Layers
VHF	Very High Frequency	30 – 300 MHz.	10 – 1 Meters	Over-air broadcast television, FM radio, aeronautical voice and nav aids, two way radio	Direct wave, rare E/F1/F2 layer refraction, occasional tropospheric weather ducting
UHF	Ultra High Frequency	300 – 3000 MHz.	1 – 0.1 Meters	UHF TV, cellular/broadband wireless, MW ovens, GPS, nav aids, WX/speed radar, WiFi	Direct wave, rare tropospheric weather ducting
SHF	Super High Frequency	3 – 30 GHz.	10 – 1 CM.	Point-to-Point and satellite microwave links, proximity detectors, radars	Direct Wave, very sensitive to obstructing objects
EHF	Extremely High Frequency	30 – 300 GHz.	10 – 1 MM.	Very local microwave links/radars/sensors, MASER weapons	Direct Wave; major air and obstacle absorption



Properties of Waves

Relationship Between Frequency and Wavelength

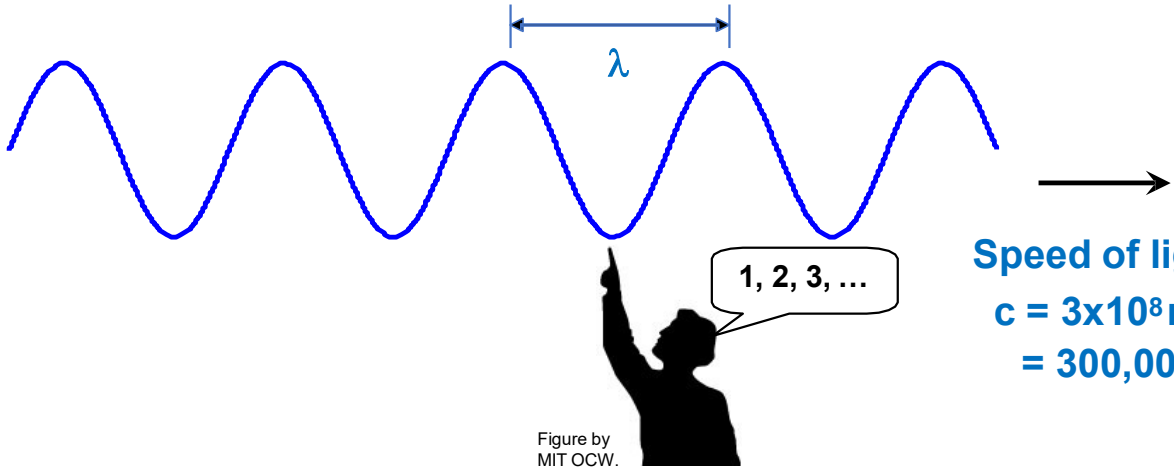


Figure by MIT OCW.

Speed of light, c

$c = 3 \times 10^8$ m/sec

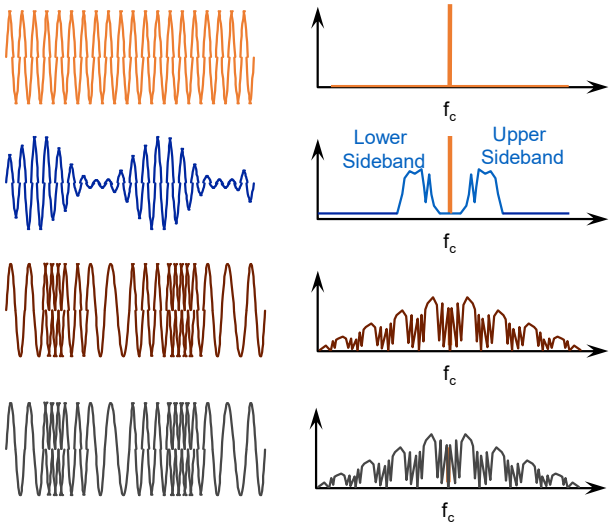
= 300,000,000 m/sec

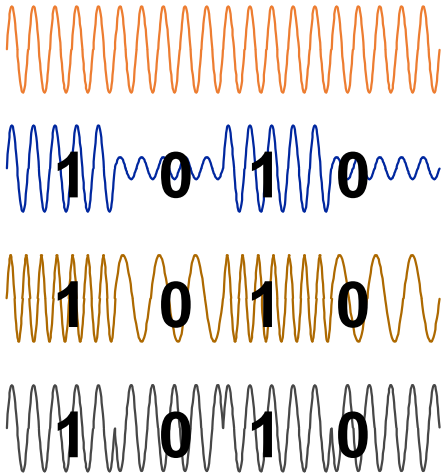
$$\text{Frequency (1/s)} = \frac{\text{Speed of light (m/s)}}{\text{Wavelength } \lambda \text{ (m)}}$$

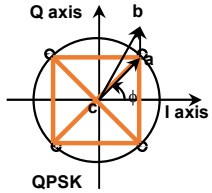
Examples:

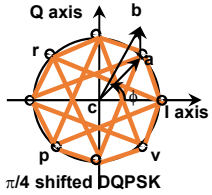
Frequency	Wavelength
100 MHz	3 m
1 GHz	30 cm
3 GHz	10 cm
10 GHz	3 cm

Basics of Communications Signals

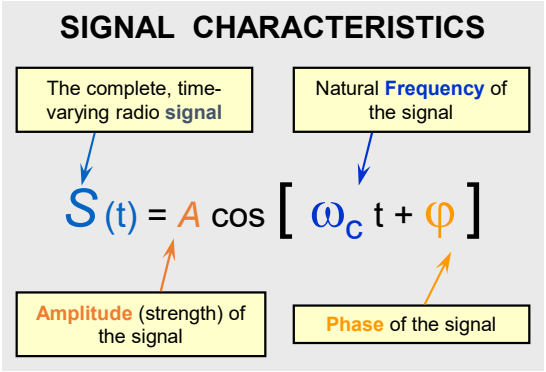




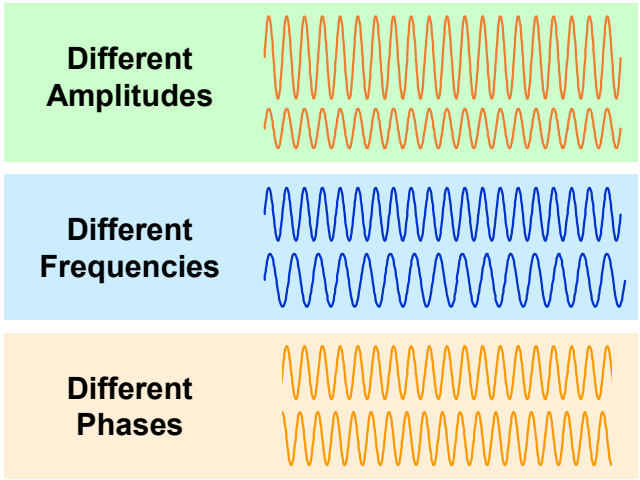




Characteristics of a Communication Signal

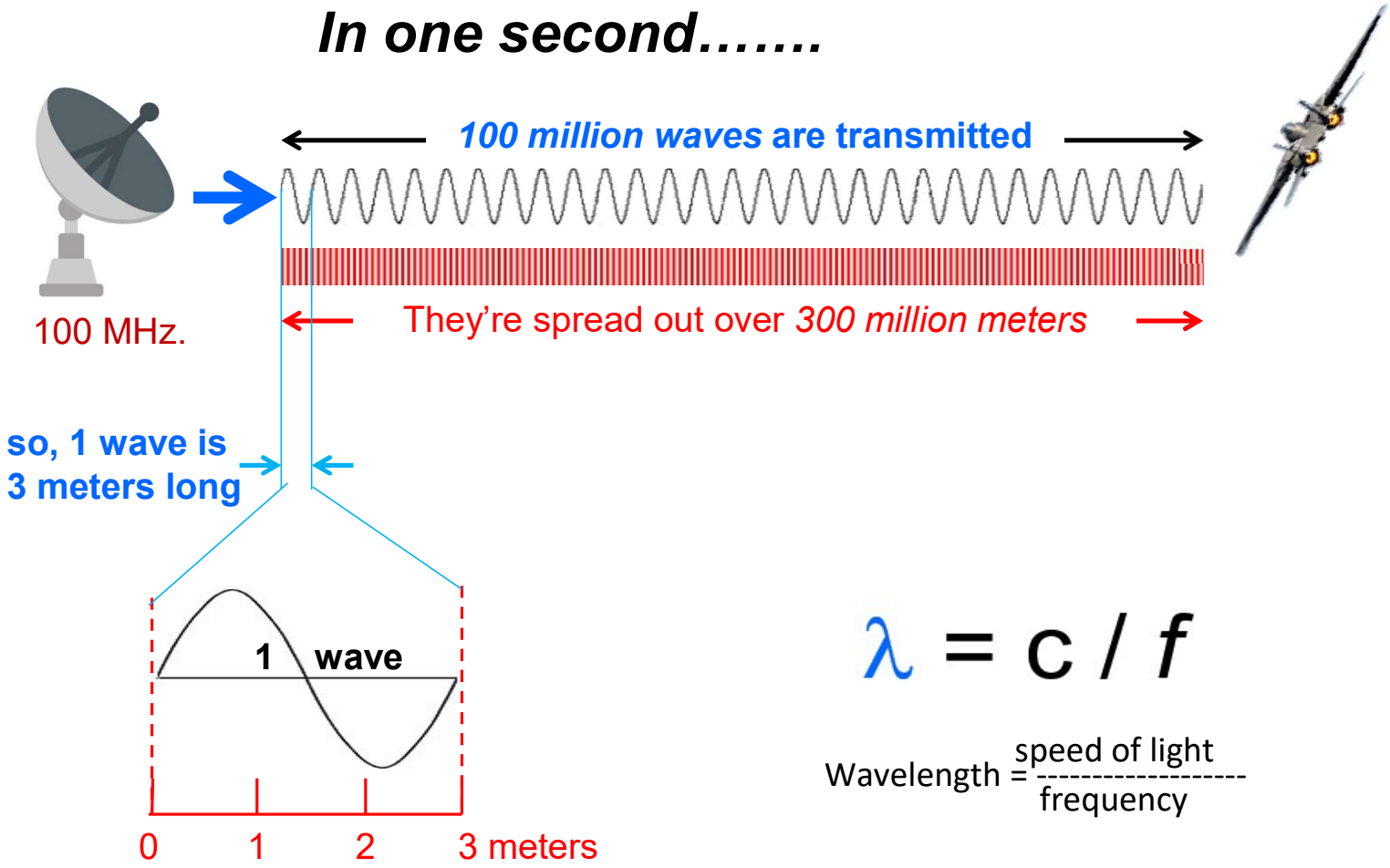


Compare these Signals:



- The purpose of telecommunications is to send information from one place to another
- Our civilization exploits the transmissible nature of radio signals, using them in a sense as our "carrier pigeons"
- To convey information, some characteristic of the radio signal must be altered (I.e., 'modulated') to represent the information
- The sender and receiver must have a consistent understanding of what the variations mean to each other
- RF signal characteristics which can be varied for information transmission:
  - Amplitude
  - Frequency
  - Phase

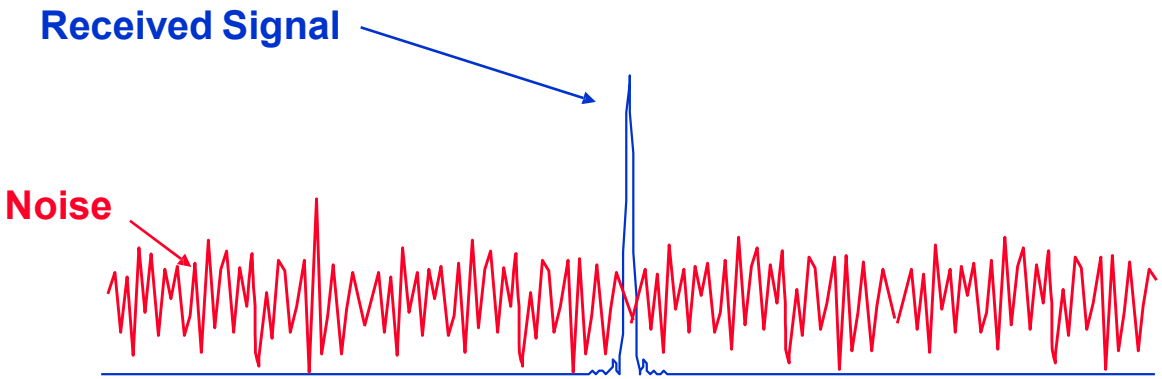
Frequency vs. Wavelength Example



$$\lambda = c / f$$

$$\text{Wavelength} = \frac{\text{speed of light}}{\text{frequency}}$$

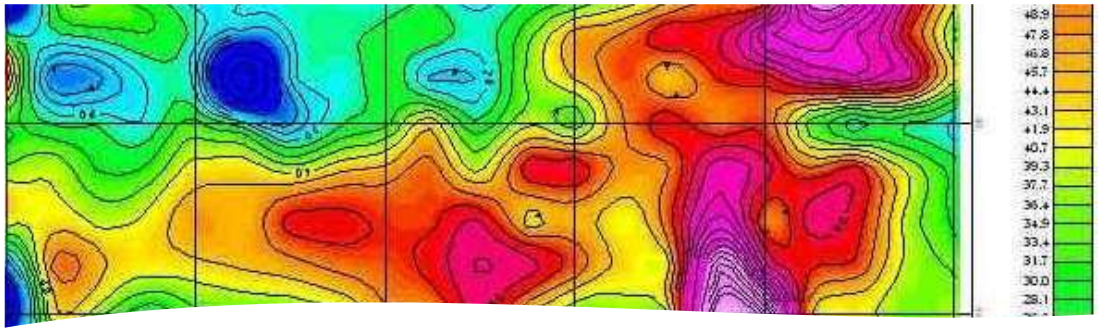
Signal-to-Noise Ratio



$$\text{SNR} = \frac{\text{Received Signal Energy}}{\text{Noise Energy}}$$

Example of Intelligence Cycle

- Collect
  - Sensors
- Exploit
  - Analysis/Process
- Disseminate
  - Communication



Geophysical Intelligence

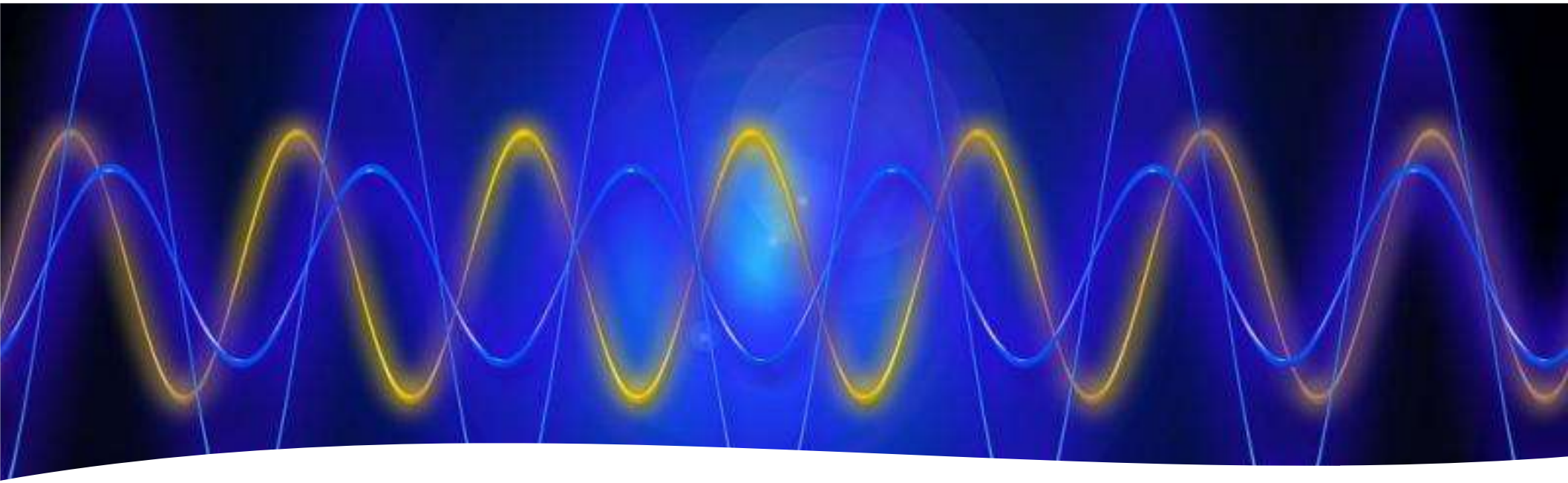
- Geophysical intelligence is a MASINT branch created to find and analyze underground resources. Its purpose is to detect moving and non-moving objects. That's why MASINT is very helpful in geophysics.

Signal Interception

COMMUNICATIONS INTELLIGENCE (COMINT)

ELECTRONIC INTELLIGENCE (ELLNT)

FOREIGN SIGNALS INTELLIGENCE (FISINT)



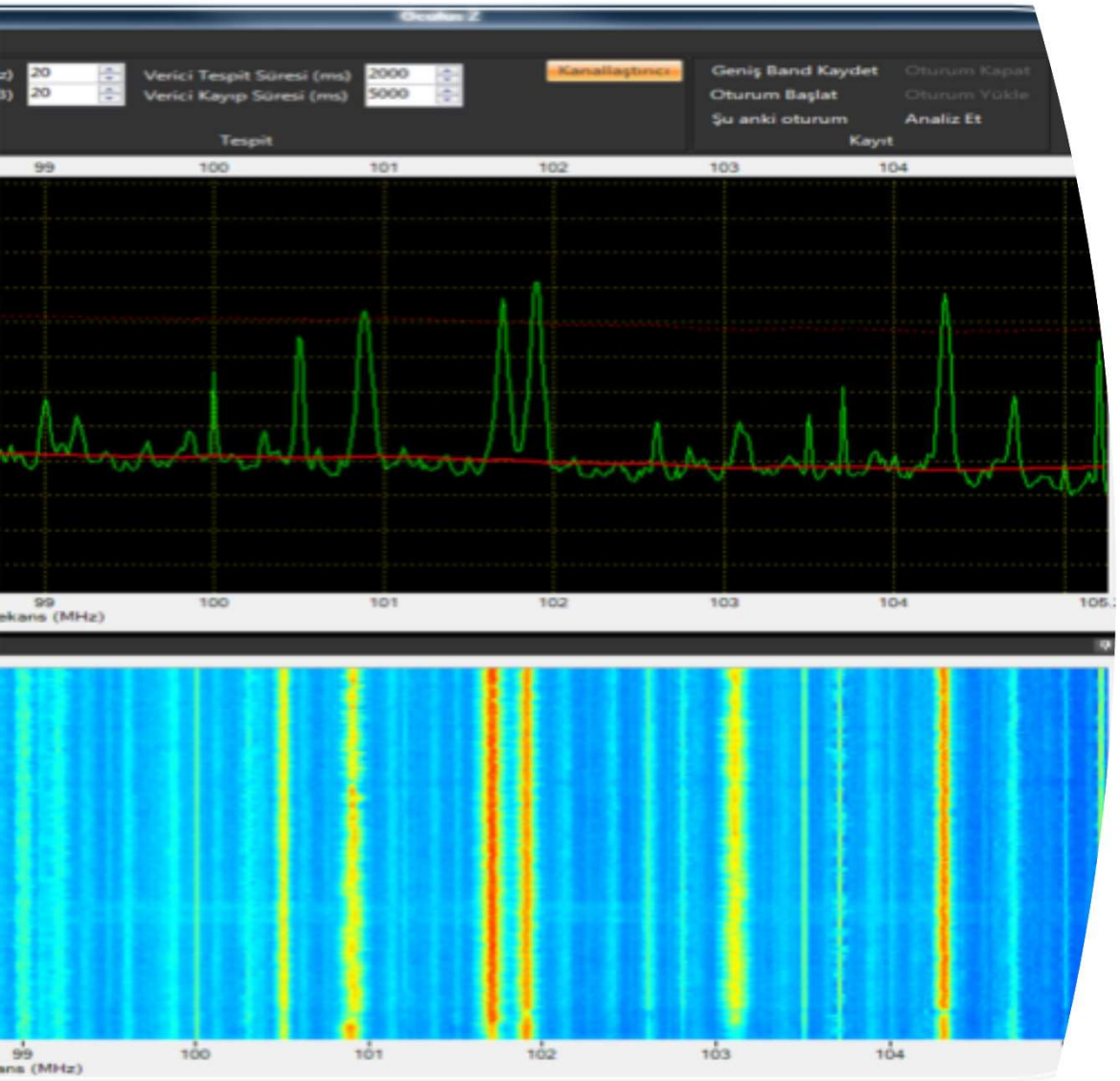
Signals Intelligence Operations

- Most facets of military operations involve the use of some device or system that radiates or receives electromagnetic energy via air waves, metallic cable, or fiber optics.
- Radios, radars, sensors, smart munitions, telephone systems, and computer networks use electromagnetic radiation.
- Both complex and unsophisticated military organizations depend on these systems and their inherent use of the electromagnetic spectrum.

- Signals intelligence operations are the principal way to exploit an adversary's use of the electromagnetic spectrum.

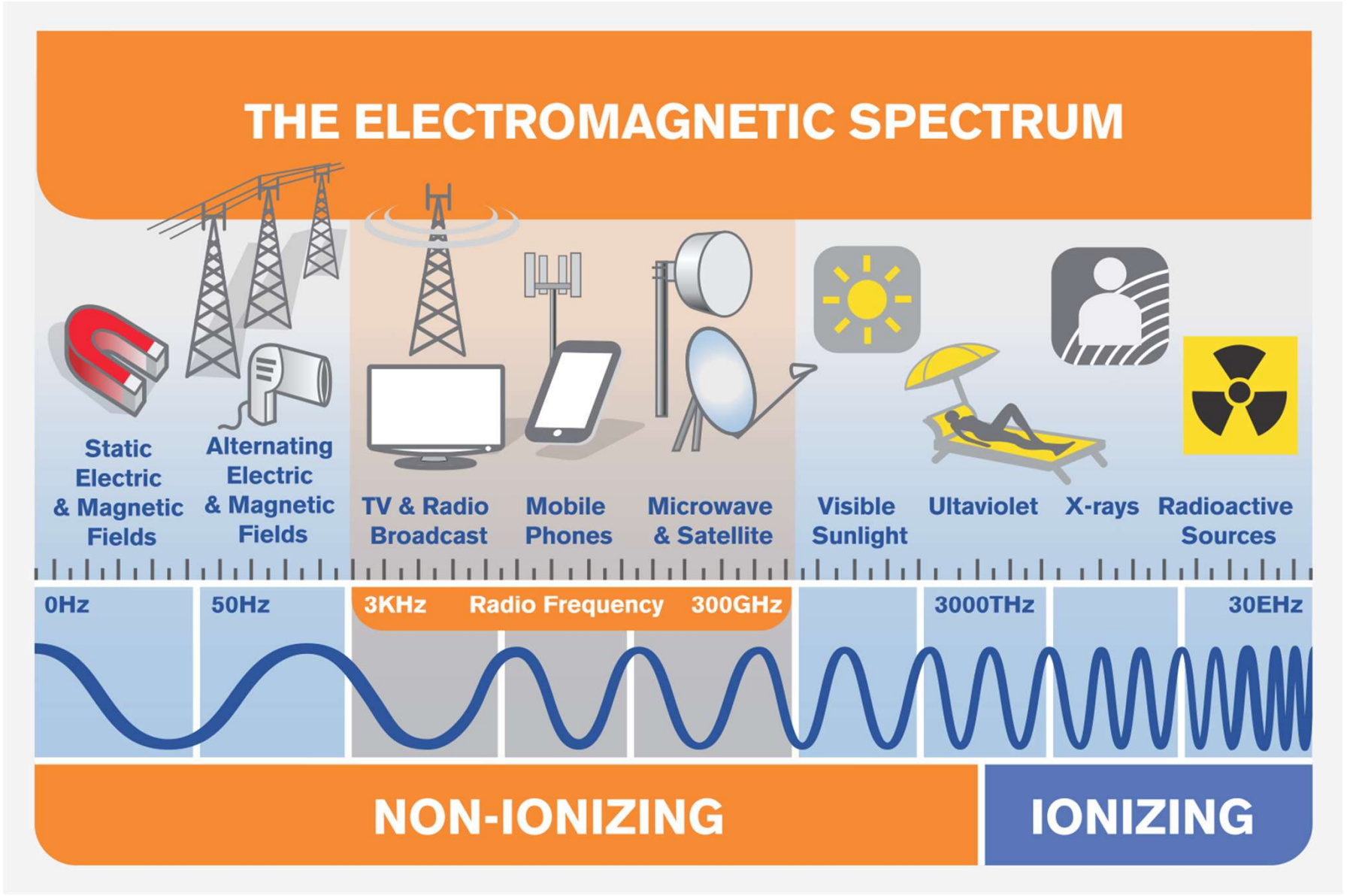
Communication Signal Scenarios

- Wide Spectral Coverage (1.5 MHz - 60 GHz)
- Complex Waveforms (Burst, FH, DS)
- Non-Standard Data Formats
- High Signal Density
- Low SNR Conditions
- Both NB and WB Signals (FDM, TDM)
- CDMA and OFDM/OFDMA Types
- Encrypted Signals
- Short Dwell Times



Signals Intelligence (SIGINT) Sources

- Signals intelligence is derived from signal intercepts comprising however transmitted either individually or in combination:
  - All communications intelligence (COMINT), electronic intelligence (ELINT) and foreign instrumentation signals intelligence (FISINT).

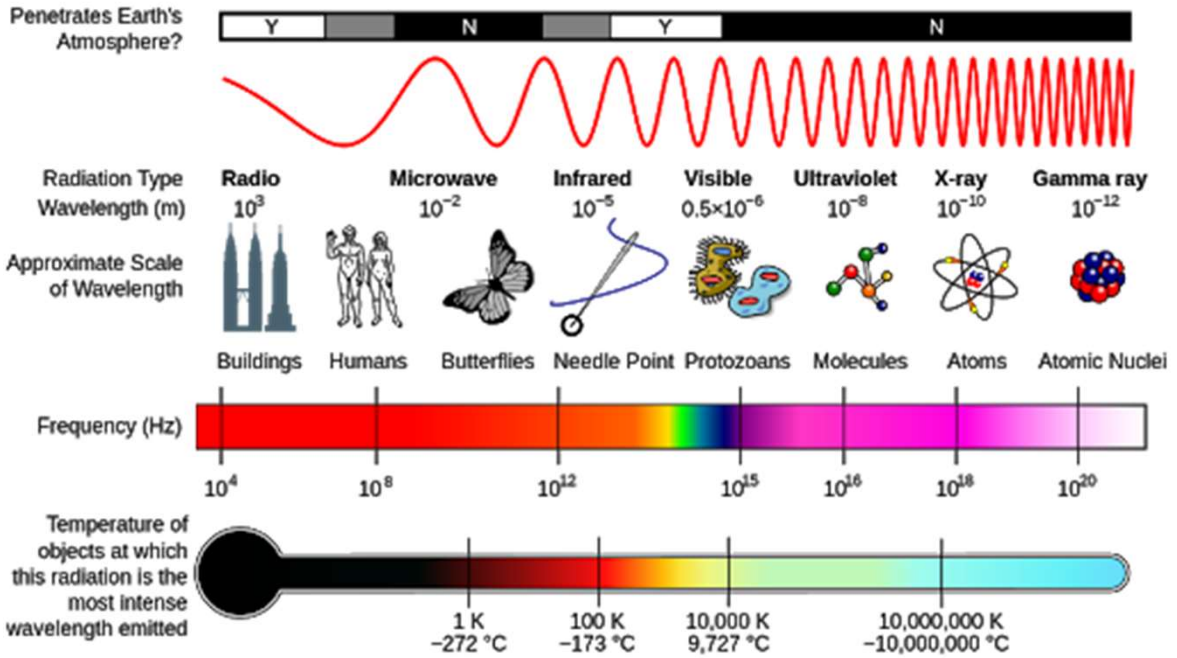

THE ELECTROMAGNETIC SPECTRUM
Static Electric & Magnetic Fields
Alternating Electric & Magnetic Fields
TV & Radio Broadcast
Mobile Phones
Microwave & Satellite
Visible Sunlight
Ultaviolet
X-rays
Radioactive Sources
0Hz
50Hz
3KHz
Radio Frequency
300GHz
3000THz
30EHz
NON-IONIZING
IONIZING

Information Derived from Electronic Signals

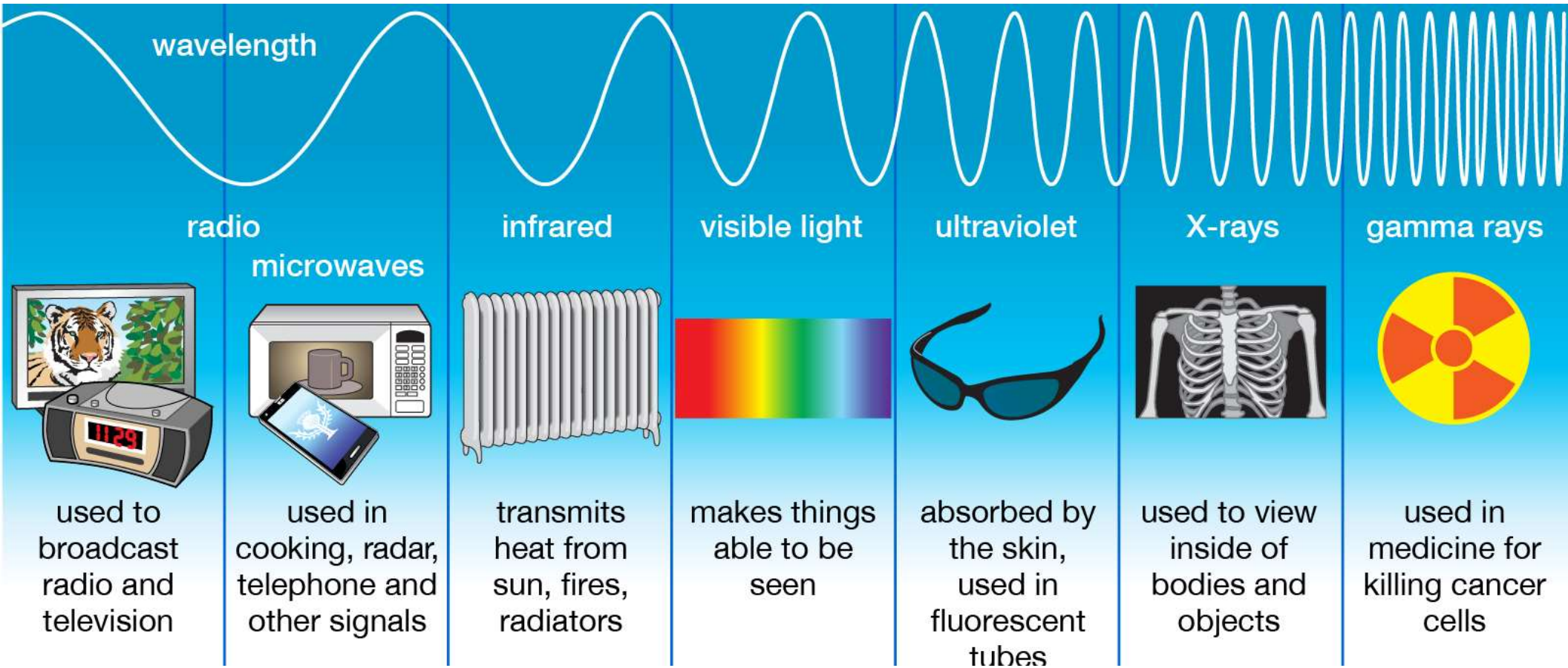
- Electromagnetic emissions

- Signal activity throughout the radio frequency spectrum
  - Radio
  - Microwave
  - Infrared
  - Laser
  - UV
  - etc.

- COMINT
  - Speech
  - Image
  - Video
  - Text



Types of Electromagnetic Radiation



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

Role of Signals Intelligence Analysts

- Utilizing sophisticated equipment, Signals Intelligence Analysts extract, analyze and identify activity and communication that come from electromagnetic emissions.

- These analysts relay their findings by producing combat, strategic and tactical intelligence reports and notify unusual activity or critical situations so we can respond with the necessary speed, force and precision.

Signals Intelligence (SIGINT) is “a category of Intelligence”

Communications intelligence (COMINT)

Electronics intelligence (ELINT)

Foreign Instrumentation Signals Intelligence Foreign instrumentation signals intelligence (FISINT)

SIGINT Planforms and Applications

- Various Applications
- Airborne
- Ground
- Naval
- Space
- Cyber

Communications Intelligence

- Communications intelligence (COMINT) is the technical and intelligence information derived from foreign communications by anyone of the than the intended recipient.

COMINT

The addresses, if the signal is not a general broadcast and if addresses are retrievable from the message.

These stations may also be COMINT (e.g., a confirmation of the message or a response message), ELINT (e.g., a navigation beacon being activated) or both.

Rather than, or in addition to, an address or other identifier, there may be information on the location and signal characteristics of the responder.

COMINT

The addresses, if the signal is not a general broadcast and if addresses are retrievable from the message.

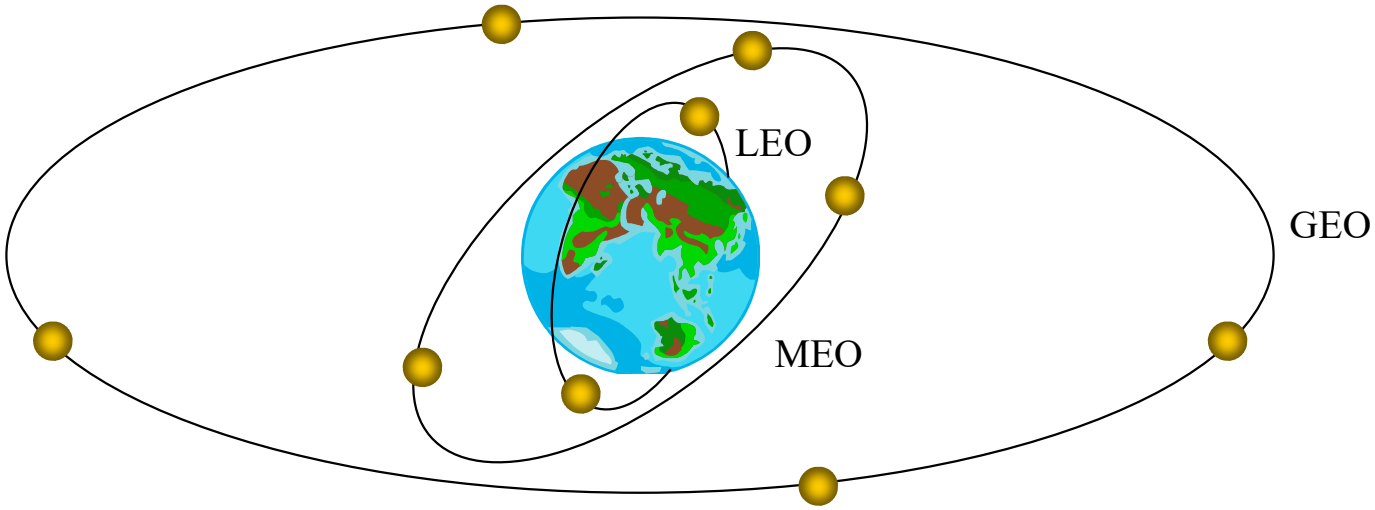
These stations may also be COMINT (e.g., a confirmation of the message or a response message), ELINT (e.g., a navigation beacon being activated) or both.

Rather than, or in addition to, an address or other identifier, there may be information on the location and signal characteristics of the responder.

Communications Intelligence (COMINT)

- Communications intelligence (COMINT) is information gathered from the communications of individuals, including telephone conversations, text messages, data, text and various types of online interactions.
  - Radio monitoring and radio location in the 10 kHz to 40 GHz frequency range: land-based, naval and airborne applications.
  - VHF/UHF
  - Satellite communications

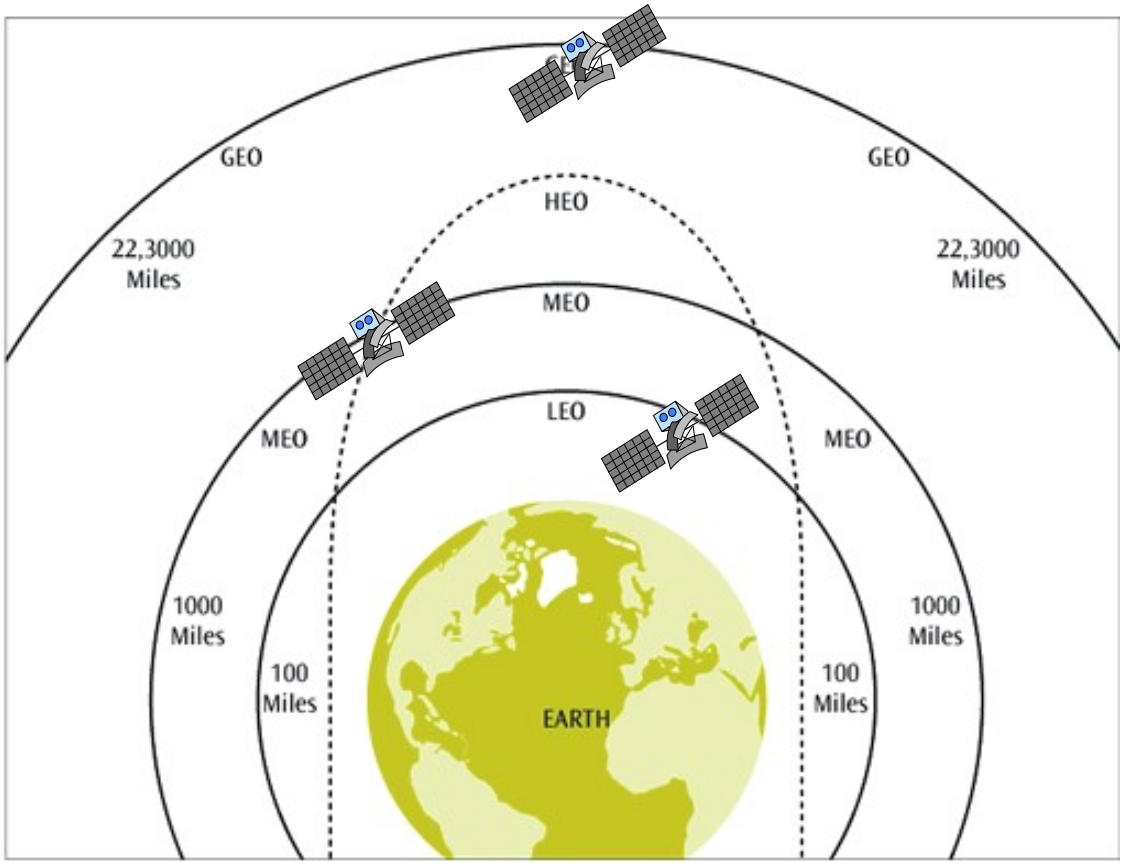
Satellite Orbits



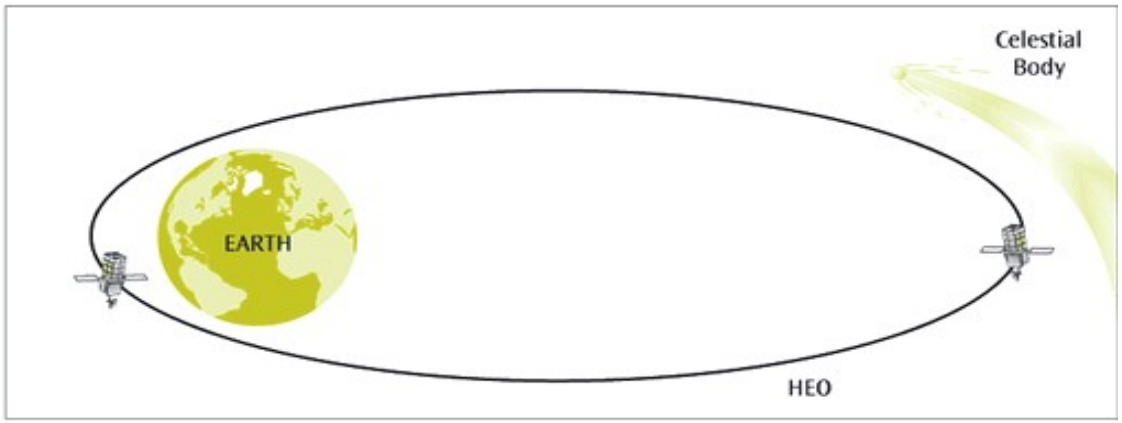
LEO: Low Earth Obit
MEO: Medium Earth Orbit
GEO: Geostationary Earth Orbit

LEO: 500 - 900 km
MEO: 5,000 - 12,000 km
GEO: 36,000 km

Satellite orbits: LEO, MEO, GEO and HEO



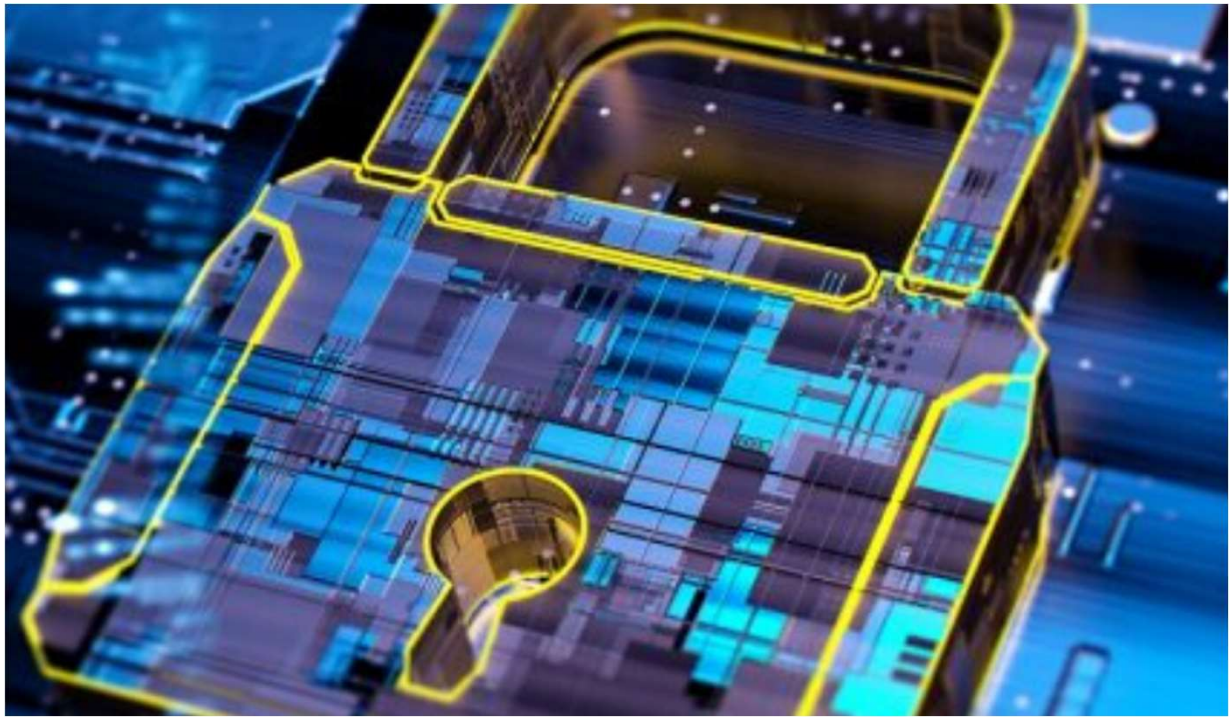
HEO Polarization Highly Elliptical Orbit



Electronics Intelligence

- Electronics intelligence (ELINT) is the technical and intelligence information derived from foreign noncommunication electromagnetic radiation emanating from anywhere other than nuclear detonations or radioactive sources.

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



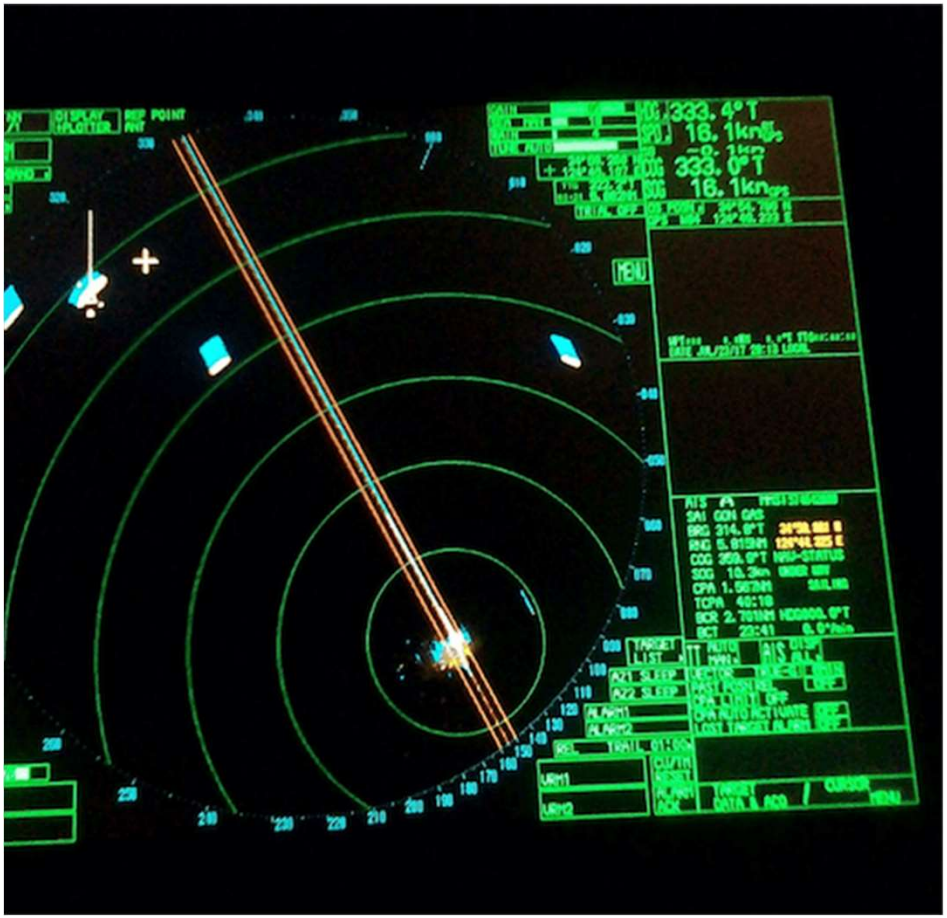
- ELINT includes the interception and analysis of noncommunications transmissions, such as radar.
- ELlNT is used to identify the location of an emitter, determine its characteristics, and infer the characteristics of supported systems.

ELINT

Electronic Intelligence (ELINT)

- Electronics intelligence (also called ELINT) is technical and intelligence information obtained from electromagnetic emissions that are not radiated by communications equipment or by nuclear detonations and radioactive sources.

- By analyzing the electronic emissions from a given radar, weapon or electronic system, an intelligence analyst can very often determine the purpose of the device.

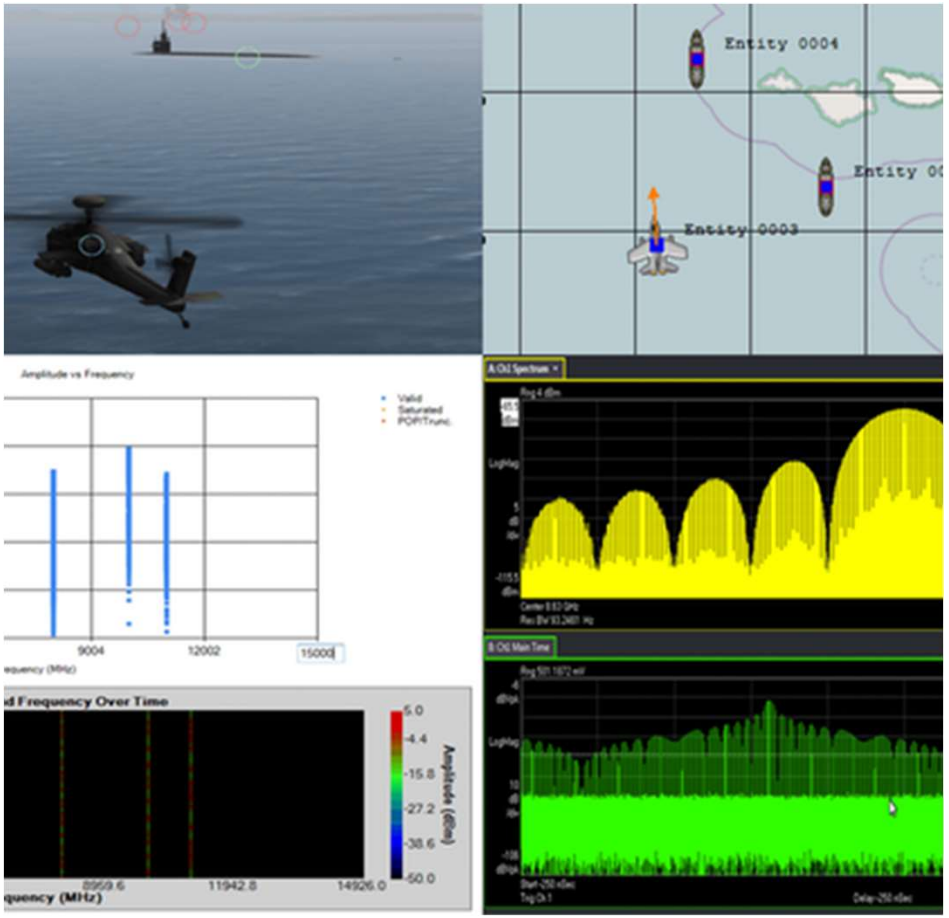


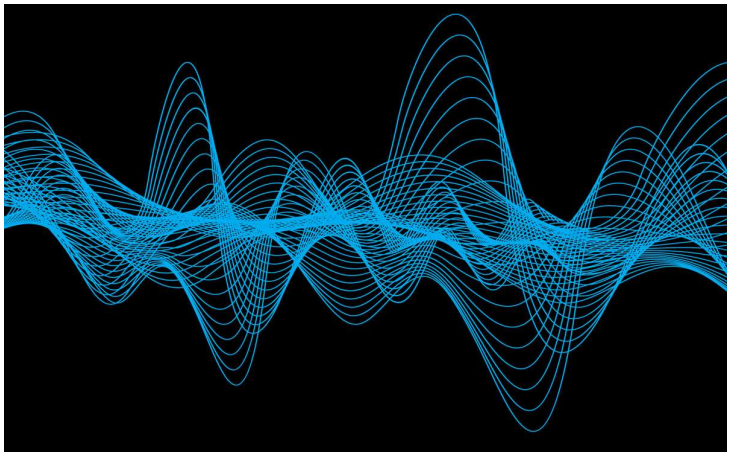
The Basic Concepts of ELINT

- Although ELINT is technically a subset of SIGINT or Signals Intelligence, ELINT specifically deals with radar signals, whereas SIGINT is often associated only with Communication or data link signals.

- Modern Electronic Warfare (EW) as is commonly defined is made up of 3 key components: Electronic Attack (EA), Electronic Support (ES), and Electronic Protection (EP).

- However, Electronic Warfare heavily relies on Electronic Intelligence (ELINT) and the data it provides including radar operating parameters, waveform details, geo-location, and other pertinent information.





Applications and Solution

Airborne

- Fighter Jets
- Special Mission Aircrafts
- Transport Aircrafts
- Unmanned Aerial Vehicles (UAVs)

Ground

- Vehicle-Mounted
- Soldiers
- Base Station

Naval

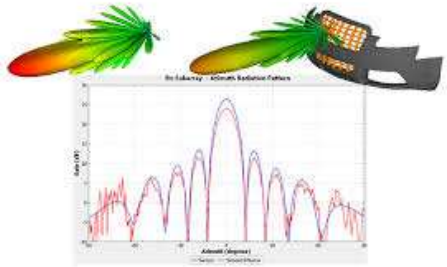
- Ships
- Submarines
- Unmanned Marine Vehicles (UMVs)

Space

Cyber

ELINT

- Search
- Intercept
- Locate
- Record
- Analysis of radiated EM energy

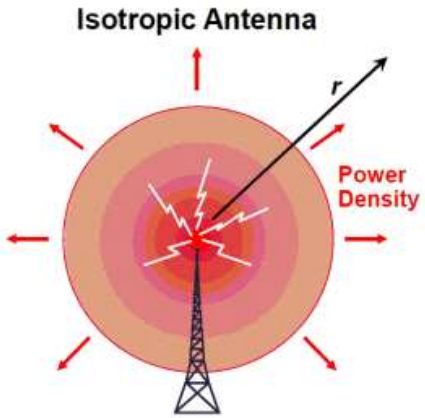


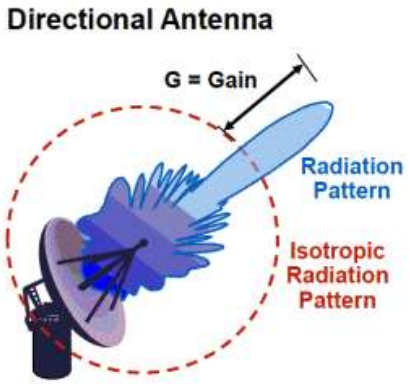
ELINT Receiver

- ELINT Receiver measure:
  - Angle of Arrival (AOS)
  - Pulse Width
  - Pulse Reception Frequency
  - Frequency
  - Time of Arrival
  - Scan Rate
  - Location of fixing emitter

Antennas and Radiation

- Antenna is an electrical device which converts electric power into radio waves, and vice versa, antenna are used not only on radar but also on jammers, **Radar warning receiver** (**RWR**) and communication system .
- The function of the antenna during transmission is to concentrate the radar energy from the transmitter into a shaped beam that points in the desired direction.
- During the reception, or listening time, the function of the antenna is to collect the returning radar energy, contained in the echo signals, and deliver these signals to the receiver. Antennas are often distinguished by their beam shape and efficiency.





Yagi-Uda Antenna

Note

Signals intelligence (SIGINT) is “a category of intelligence comprising either individually or in combination all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted”.

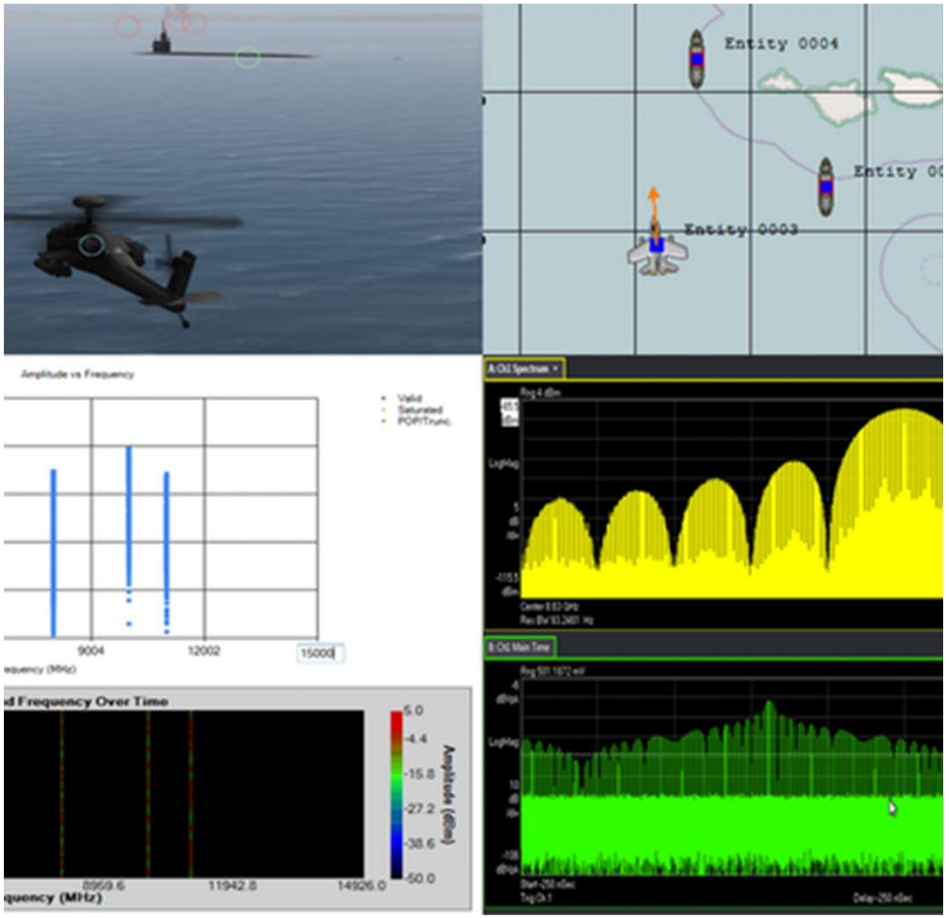
Simply, SIGINT is intelligence gained by exploiting an adversary’s use of the electromagnetic spectrum with the aim of gaining undetected firsthand intelligence on the adversary’s intentions, dispositions, capabilities, and limitations.

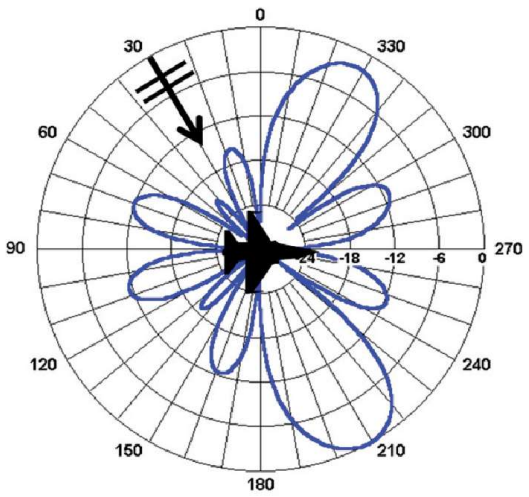
The Basic Concepts of ELINT

- Although ELINT is technically a subset of SIGINT or Signals Intelligence, ELINT specifically deals with radar signals, whereas SIGINT is often associated only with Communication or data link signals.

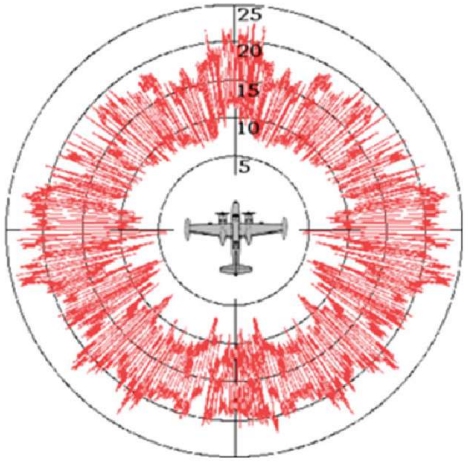
- Modern Electronic Warfare (EW) as is commonly defined is made up of 3 key components: Electronic Attack (EA), Electronic Support (ES), and Electronic Protection (EP).

- However, Electronic Warfare heavily relies on Electronic Intelligence (ELINT) and the data it provides including radar operating parameters, waveform details, geo-location, and other pertinent information.





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.

A main purpose of Technical ELINT (TechELINT)

- A main purpose of Technical ELINT (TechELINT) is to obtain signal parameters which can define the capabilities and the role that the emitter plays in the larger system, such as a ground radar locating aircraft, and thus lead to the design of radar detection, countermeasure, or counterweapons equipment.

- The overall process, including operation of the countermeasures, is part of electronic warfare.

Operational ELINT (OpELINT)

- Operational ELINT (OpELINT) concentrates on locating specific ELINT targets and determining the operational patterns of the systems.
- These results are commonly called Electronic Order of Battle (EOB).
- OpELINT also provides threat assessments, often referred to as “tactical ELINT.” OpELINT intelligence products support military operational planners and tactical military commanders on the battlefield.
- A former third major branch of ELINT is the collection, processing, and reporting of foreign telemetry signals intelligence (TELINT).

Foreign Instrumentation Signals Intelligence

- Foreign instrumentation signals intelligence (FISINT) is the technical and intelligence information derived from the intercept of foreign instrumentation signals by anyone other than the intended recipients. (FISINT is primarily strategic in nature and will not be addressed further in this manual.)

India's Eyes in the Space: The spy satellites network

Concept of Employment

- SIGINT can be employed in tactical situation when the enemy uses electromagnetic spectrum communications and/or systems.
- Optimal employment is against enemy forces that depend on tactical communications and noncommunications for command and control of their operations.
- SIGINT operations are more difficult against enemy forces that have established more permanent emplacements using land lines or other cabled communications systems.

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.

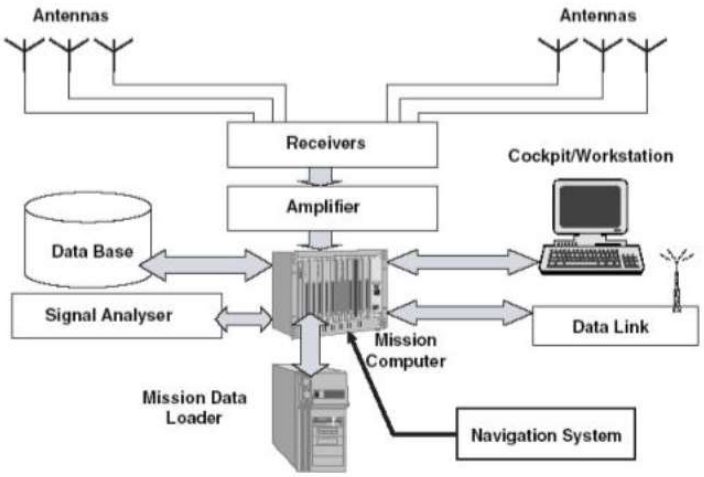
- These military forces also use the electromagnetic spectrum to collect, process, and report intelligence and to support other administrative and logistics operations.

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



SIGINT Collection

Signal intelligence (SIGINT) is information gathering by interception of signals, which includes either communication signals or electronic signals of a given target.

SIGINT systems form one of the core systems in military defense and fall under the category intelligence, surveillance, and reconnaissance (ISR).

SIGINT systems provide intelligence on: Composition, Intentions, Threat capabilities, and Disposition

ELINT using Software Defined Radio (SDR)

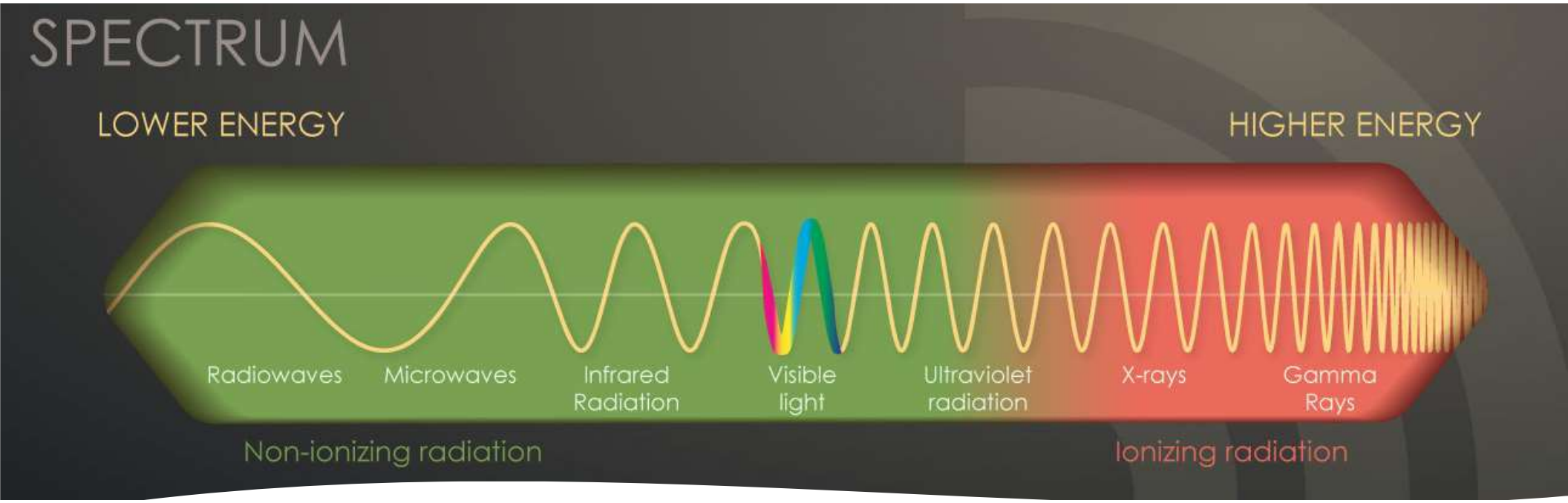
- DSP/FPGA for electronic intelligence
-
- Developing electronic intelligence systems using signal processing hardware: FPGA, DSP and I/O modules
- Mix FPGA with DSP processors, and to integrate that processing power with very fast communications ADCs, capable of sampling IF signals directly
- Most modern 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.

FISINT

- FISINT consists of intercepts of telemetry from an opponent's weapons systems as they are being tested.

- Telemetry units provide designers with information on a prototype's guidance system operation, fuel usage, staging, and other parameters vital for understanding operational characteristics.

- These data enable the designer to evaluate the performance of the prototype. However, if intercepted, they also provide an adversary with the ability to estimate the capability of the prototype.



Radiation

- This source of intelligence does not include energy emanating from nuclear detonations or radioactive sources.
- Rather, it concerns unintentional emissions of energy from electronic systems (while ELINT is based on intentional radiations from the same systems).
- Inadequate shielding of electronic systems, or the following of incorrect procedures, may result in inadvertent energy emissions, which, when analyzed, may reveal a great deal about a system's purpose or capabilities.

Foreign Instrumentation Signals Intelligence (FISINT)

FISINT (Foreign Instrumentation Signature INTelligence) is intelligence from the interception of foreign electromagnetic emissions associated with the testing and operational deployment of foreign aerospace, surface, and subsurface systems.

Since it deals with signals that have communicational content, it is a subset of Communications Intelligence (COMINT).

Unlike general COMINT signals, the content of FISINT signals is not in regular human language, but rather in machine to machine (instrumentation) language or in a combination of regular human language and instrumentation language.

FISINT is also considered as a subset of MASINT (measurement and signature intelligence).

Example of Foreign Instrumentation Signals Intelligence (FISINT)

- Typical examples FISINT communication are:
  - Telemetry data (TELINT). Missiles, satellites and other remotely monitored devices often transmit streams of data concerning their location, speed, engine status and other metrics.
  - Video data links. These may be from UAVs or from satellites used for reconnaissance.
  - Remote access and control transmissions, such as from remote keyless systems and wireless traffic light control systems.
  - Command signals used in teleoperation, such as the control of aerial vehicles, missiles and remotely-controlled robots.

ELINT vs. COMINT

- ELectronic INTelligence (ELINT)
  - ELectronic INTelligence primarily dedicated to the interception and analysis of radar emissions from surveillance, fire-control or missile guidance radars, and is often allied to an ECM system to provide protection from these.

- COMmunications INTelligence (COMINT)
  - COMmunications INTelligence, as its name implies, is intended for the interception of communications, whether by voice or datalink.

Foreign Instrumentation Signals Intelligence (FISINT)

- FISINT (Foreign Instrumentation Signature INTelligence) is intelligence from the interception of foreign electromagnetic emissions associated with the testing and operational deployment of foreign aerospace, surface, and subsurface systems.

- Since it deals with signals that have communicational content, it is a subset of Communications Intelligence (COMINT).

- Unlike general COMINT signals, the content of FISINT signals is not in regular human language, but rather in machine to machine (instrumentation) language or in a combination of regular human language and instrumentation language.

- FISINT is also considered as a subset of MASINT (measurement and signature intelligence).

Example of Foreign Instrumentation Signals Intelligence (FISINT)

- Typical examples FISINT communication are:
  - Telemetry data (TELINT). Missiles, satellites and other remotely monitored devices often transmit streams of data concerning their location, speed, engine status and other metrics.
  - Video data links. These may be from UAVs or from satellites used for reconnaissance.
  - Remote access and control transmissions, such as from remote keyless systems and wireless traffic light control systems.
  - Command signals used in teleoperation, such as the control of aerial vehicles, missiles and remotely-controlled robots.

ELectronic INTelligence (ELINT)

- For platform protection ELINT is vital, in that it provides not only direction-finding but also analysis of the incoming signals to provide immediate warning of threat radars, including surveillance, fire control, targeting and missile guidance systems.

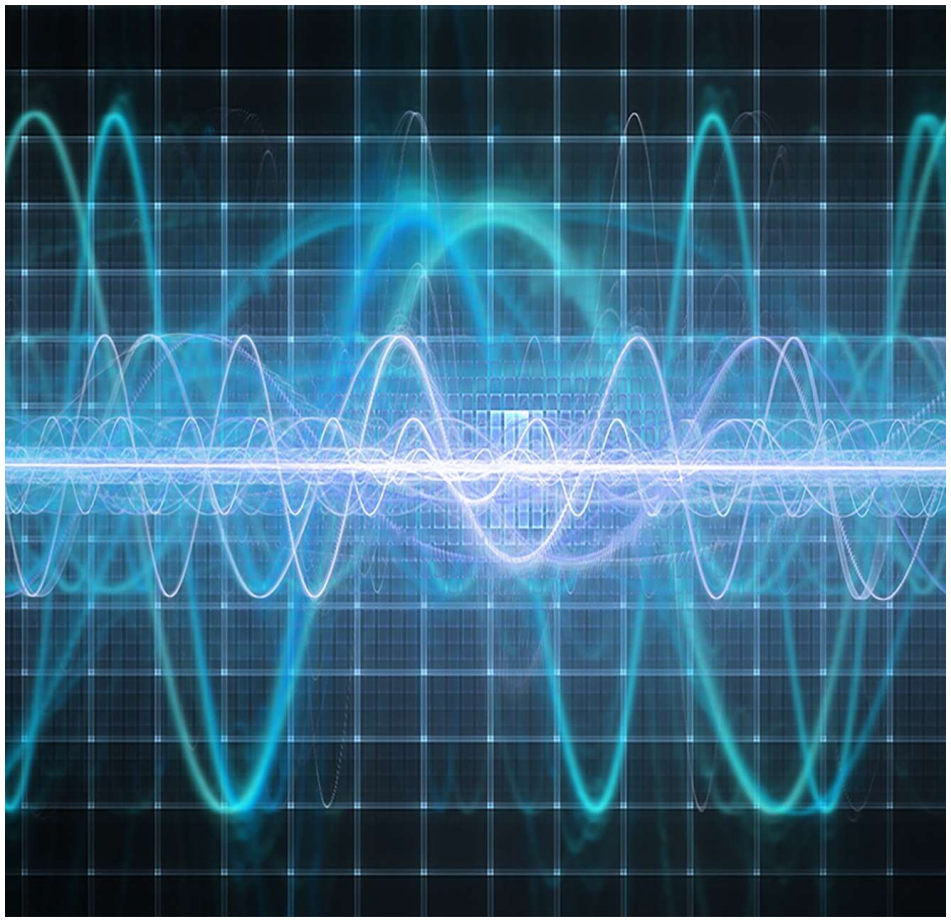
- Signals from radar systems are intercepted by a warning receiver and are analyzed by an associated processor to give a wide range of parameters, including direction, type of radar, frequency, frequency agility, Pulse Repetition Frequency (PRF), and PRF type.

- These parameters are usually sufficient to characterize the type of emitter, and complete identification is then carried out by comparing the analyzed signal with parameters of hostile and friendly emitter characteristics stored in a library within the computer memory.

- Analysis of the signals and warning of a threat is virtually instantaneous and enables countermeasures of jamming and/or decoys to be initiated.

Electromagnetic Threat Environment

- For aircraft, ships and armored fighting vehicles effective warning systems are essential for survival in the electromagnetic threat environment of the modern battlefield.
- The warning receivers mentioned in the previous paragraph are being continuously updated to cope with the latest threats.
- These receivers are normally either crystal video or superheterodyne-based equipment, both of which have their own advantages.
- Crystal video receivers, either narrowband or wideband, can operate over a frequency range from 0.5 to 40 GHz, covering all radar transmissions except those in the 94/95 GHz millimetric waveband.
- They are effective against pulsed, frequency-agile, PRI-agile, spread spectrum and continuous-wave transmitters.
- Superheterodyne receivers are more expensive but provide a coverage from 0.01 to 40 GHz with a high level of sensitivity, plus long pick-up ranges and sidelobe penetration.



COMmunications INTelligence (COMINT)

- COMINT provides both interception, direction-finding and analysis of hostile transmissions, primarily to assess the movements and intentions of the opposing forces.
- Analysis of the signals provides much valuable information of the intentions for command-and-control purposes, and the most recent systems provide the operator with the ability to detect and analyze unusual and complex signals as well as the normal interception and DF facilities.
- The receiving equipment is frequently allied to a computer-based processing and display system so that automatic position fixing in the land-based role can be carried out using remote-controlled DF stations.
- Spectra and/or time waveforms are normally provided, together with alphanumeric readouts which include type of transmission, frequency, modulation and other signal parameters.
- These parameters are used to determine the types of communication and radar systems in use, whether they are mobile or static, the direction of any movement, and so on.
- Multisignal detection and analysis is provided in nearly all equipment, and a map display overprinted with the intercepted information can be incorporated to give the battlefield commander an overall picture of both the tactical and the electromagnetic situation.

Principles behind Intelligence, Surveillance and Reconnaissance (ISR)

- Intelligence, Surveillance and Reconnaissance (ISR) provides the foundation for all military operations, and its principles have been used in warfare for centuries. The individual elements of ISR are:
  - Intelligence: the final product derived from surveillance and reconnaissance, fused with other information;
  - Surveillance: the persistent monitoring of a target; and
  - Reconnaissance: information-gathering conducted to answer a specific military question.

ISR Actors

- To enable information-gathering to take place, and to ensure that information is analyzed, and intelligence is produced for decision-makers, there are several primary actors involved, including:
  - Surveillance and reconnaissance collection assets
    Their role is to collect information. Examples include Alliance Ground Surveillance (AGS), AWACS aircraft which use radar, observation satellites, electronic assets and special ground reconnaissance troops.
  - Intelligence analysts
    Their role is to exploit and analyze information from multiple sources. Examples include national military and civilian analysts working at the strategic level in intelligence organizations, imagery analysts at all levels, and encryption experts.
  - Decision-makers
    Their role is to use intelligence to inform their decision-making. Examples include political leaders and military commanders.

Defining Intelligence

- Intelligence is the product resulting from the collection, collation, evaluation, analysis, integration, and interpretation of collected information.
    - It is a specialized information product that provides information.
    - One of the most important functions of intelligence is the reduction of the ambiguity inherent in the observation of external activities.

Intelligence

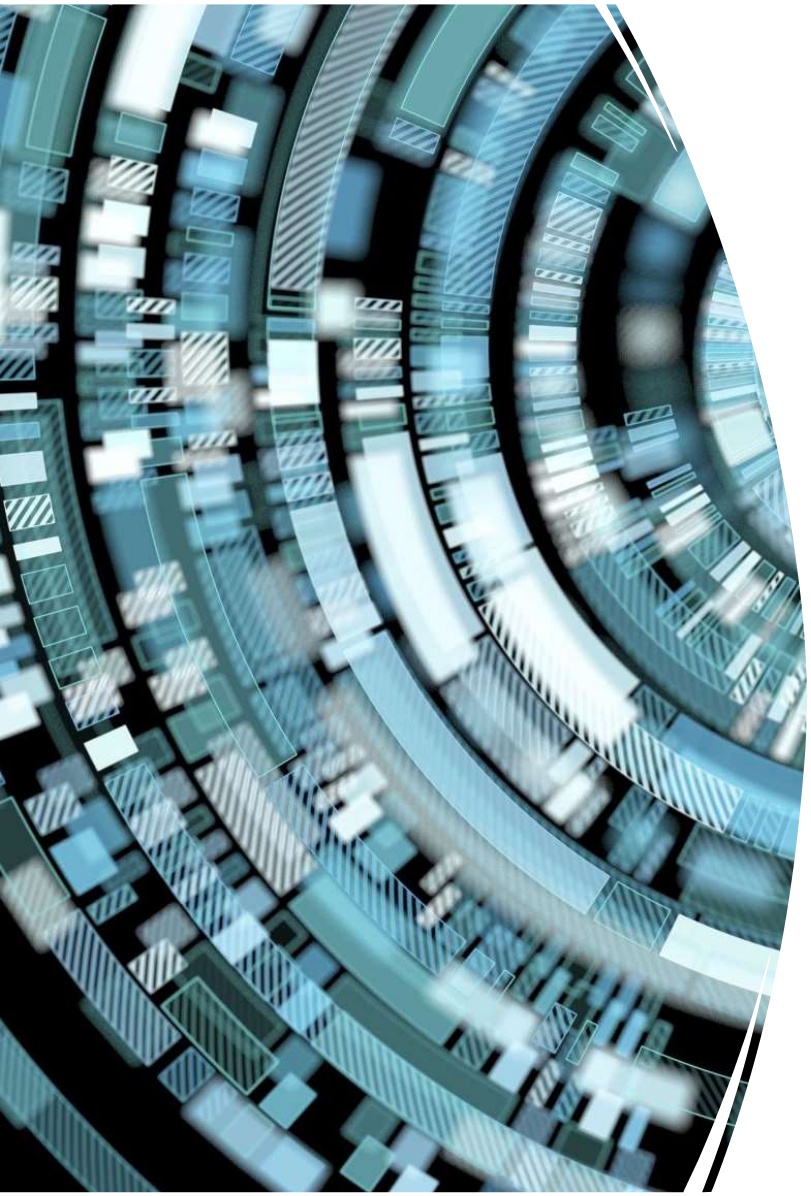
- “Intelligence is the product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas; it is the information and knowledge about a topic obtained through observation, investigation, analysis, or understanding.”

- (JP 1-02: Department of Defense Dictionary of Military and Associated Terms)

Surveillance

- “Surveillance is the systematic observation of aerospace [sic], surface or subsurface areas, places, persons, or things, by visual, aural, electronic, photographic, or other means.” (JP 1-02)

- DoD emphasizes that surveillance operations are sustained operations designed to gather information by a collector, or series of collectors, having timely response and persistent observation capabilities, a long dwell time and clear continuous collection capability.



Reconnaissance

- Reconnaissance is a mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or potential enemy, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area.” (JP 1-02)
-
    - The DoD perspective emphasizes that reconnaissance operations are transitory in nature and generally designed to collect information for a specified time by a collector that does not dwell over the target or in the area.

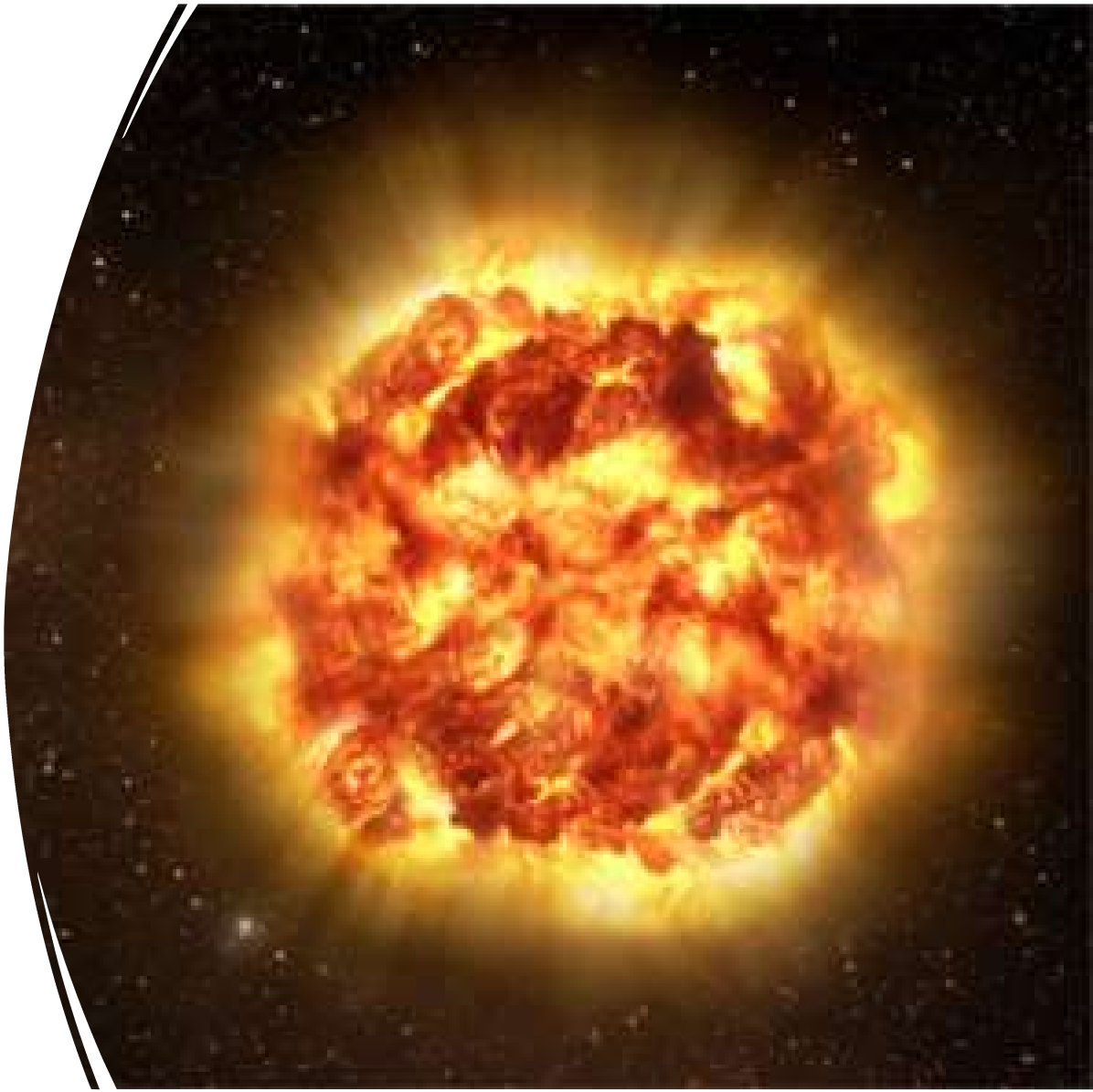
From Information to Intelligence

- The information derived from surveillance and reconnaissance, converted into intelligence by exploitation and analysis, is used to formulate strategy, policy, and military plans; to develop and conduct campaigns; guide acquisition of future capabilities; and to protect, prevent, and prevail against threats and aggression aimed at the US and its interests.

    - **Surveillance and reconnaissance assets are not inherently strategic, operational, or tactical in nature; they can be used to gather information to meet requirements at all levels of warfare. ISR operations** are conducted across the range of military operations from peace, to war, to conflict resolution.

Fusion

- Fusion refers to bringing together all types of intelligence to create one consolidated picture of the threat.
    - Various sources of intelligence form the basic structure of the intelligence community.



ISR Missions

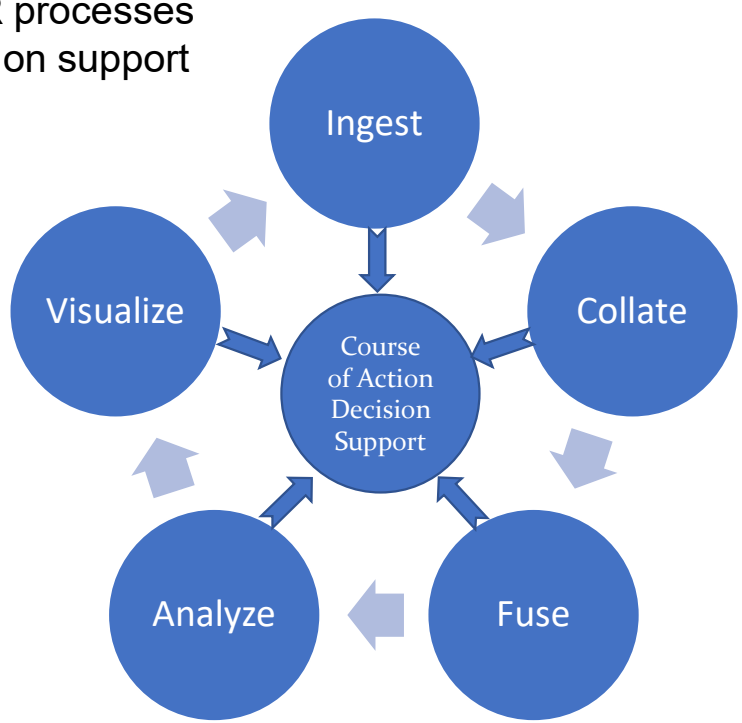
ISR Intelligence Architectures

Component of command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) applications

Image intelligence (IMINT), signals intelligence (SIGINT), and measurement and signatures intelligence (MASINT) collection systems

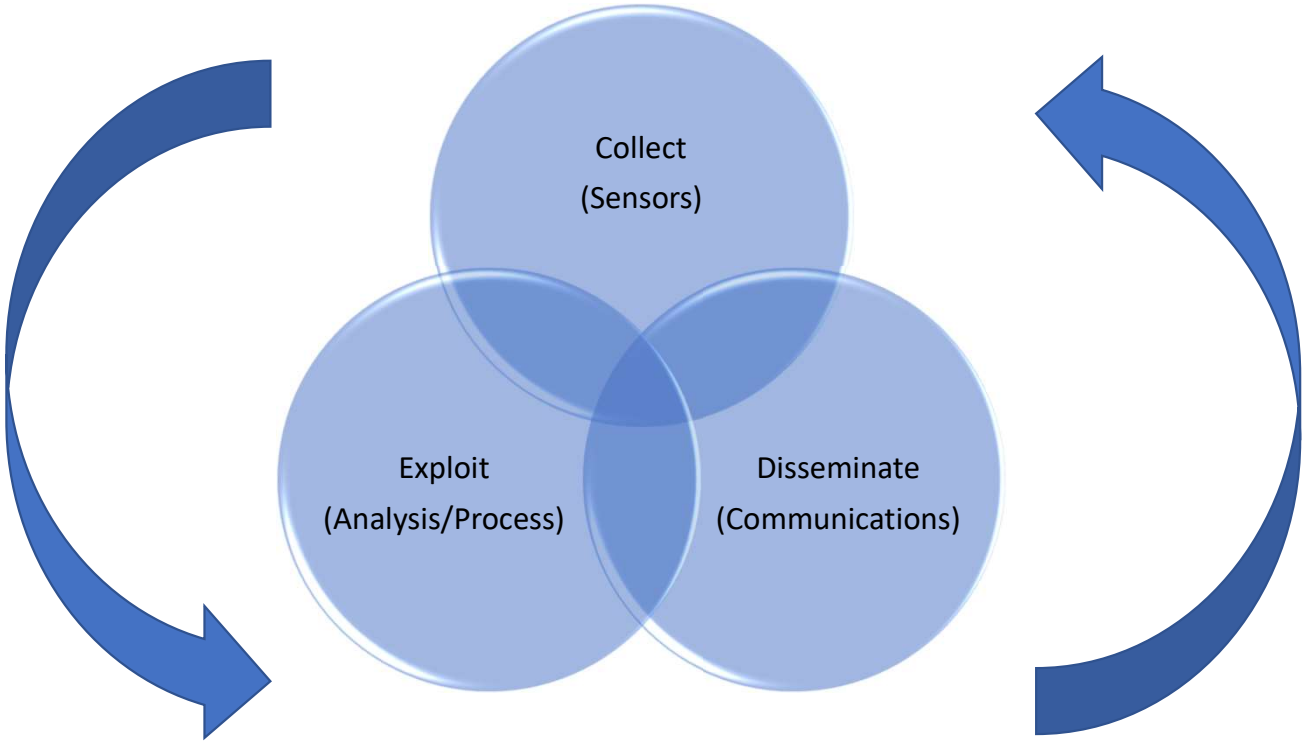
Overview of of C4ISR

Ultimately, all C4ISR processes must feed the decision support of the warfighter!



In short, C4ISR represents ***TOTAL SPECTRUM DOMINANCE***

The Primary Mission of C4ISR



Command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR)

C5ISR

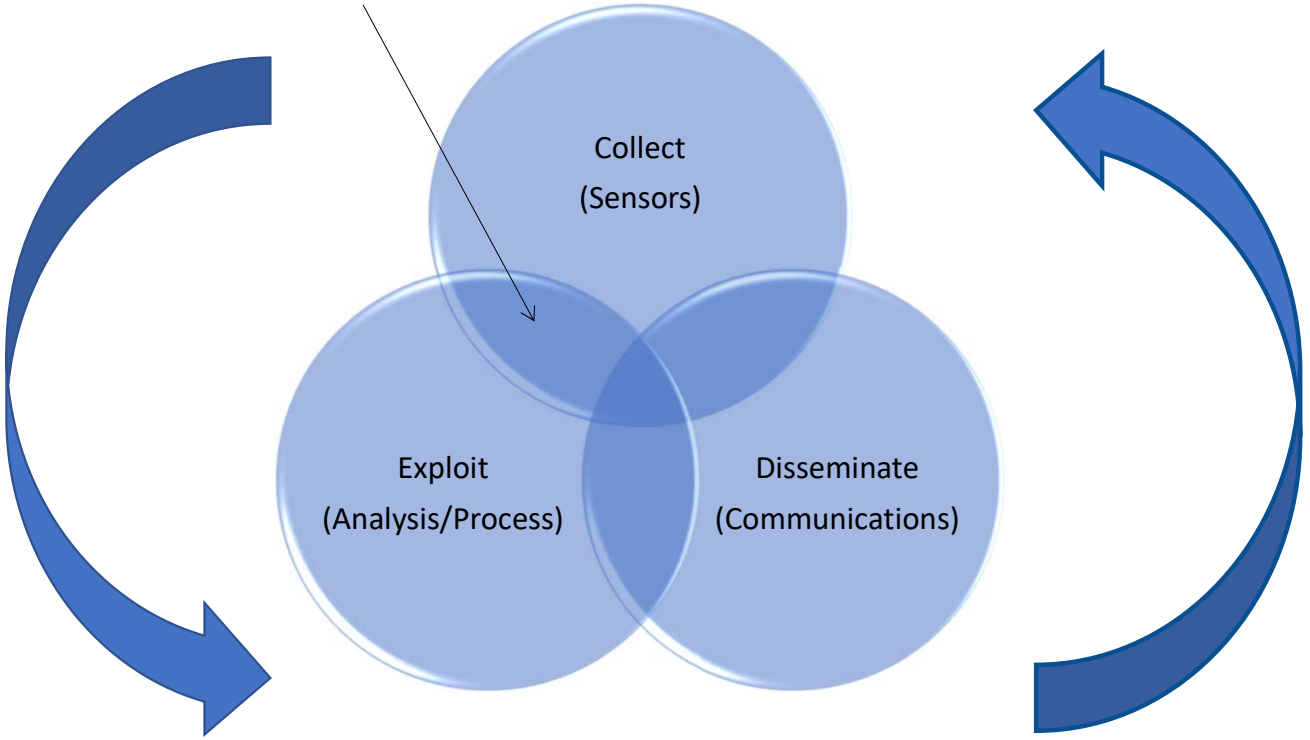
- Command, control, computers, communications, cyber-defense (C5), intelligence, surveillance, and reconnaissance (ISR)

C6ISR

- Command, control, communications, computers, cyber-defense, combat systems (C6), intelligence, surveillance, and reconnaissance (ISR)

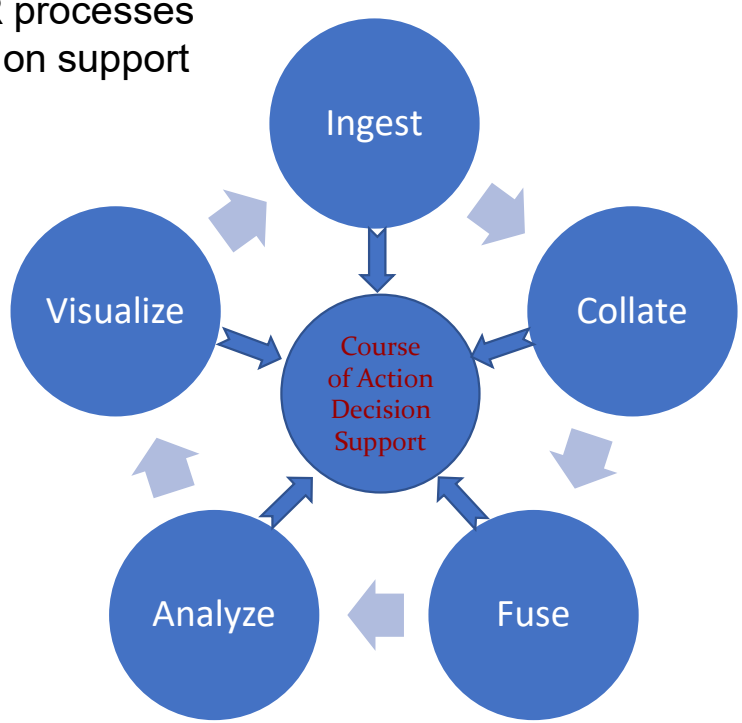
The Primary Mission of C4ISR

Regions of Sensor Fusion and Interoperability



Overview of of C4ISR

Ultimately, all C4ISR processes must feed the decision support of the warfighter!



In short, C4ISR represents ***TOTAL SPECTRUM DOMINANCE***

Component of command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) applications

C4ISR covers a broad range of technologies, capabilities, and mission profiles.

ISR Intelligence Architectures

- A broad range of technologies, including sensors, AI/ML, sensor fusion, aircraft, satellites, communication systems, navigation solutions, radars, Secondary Surveillance Phased Array Radar (SSPAR) and data exploitation.

- By leveraging a combination of these technologies, we can develop a complex system-of-systems architecture that can provide a needed mission capability.

- Automatic Dependent Surveillance Broadcast (ADS-B) to provide next-generation surveillance derived through down- and cross-link of global positioning satellite (GPS) navigation data.

Electronic Warfare (EW)

- Electronic warfare (EW) is the military action to exploit the electromagnetic (EM) spectrum, which encompasses the interception and identification of EM emissions, the employment of EM energy, including directed energy, to reduce or prevent hostile use of the EM spectrum and actions to ensure its effective use by friendly forces.
- The three components of EW are:
  - a. electronic warfare support measures (ESM);
  - b. electronic countermeasures (ECM); and
  - c. electronic protective measures (EPM).

Electronic Warfare Support Measures

- **Electronic** warfare support measures (ESM) are defined as that division of EW involving actions taken to search for, intercept and identify EM emissions and locate their sources for the purpose of immediate threat recognition.
  - It provides a source of information required for immediate decisions involving ECM, EPM and other tactical **It also provides information that contributes to the overall** signal intelligence (SIGINT) effort.

Electronic warfare

- Electronic warfare support measures systems collect data and produce information or intelligence which can be used to:
  - a. contribute as a “single source” of information to produce Red SA within the ISTAR system;
  - b. provide targeting information for ECM operations;
  - c. initiate self-protection measures;
  - d. support EPM efforts;
  - e. create or modify EW/SIGINT data bases; and.
  - f. provide warning to the supported commander.

Electronic Countermeasures (ECM)

- **Electronic countermeasures** (ECM) are defined as that division of EW involving actions taken to prevent or reduce an adversary's effective use of the EM spectrum through the use of EM energy. There are three subdivisions of ECM**:**
  - a. **Electronic Jamming. The deliberate radiation,** re-radiation or reflection of EM energy with the object of impairing the effectiveness of electronic devices, equipment or systems being used by an adversary.
  - b. **Electronic Deception. The deliberate radiation,** re-radiation, alteration, absorption or reflection of EM energy in a manner intended to confuse, distract or seduce an adversary or his electronic systems.
  - c. **Electronic Neutralization. The deliberate use of** EM energy to either temporarily or permanently damage an adversary’s devices that rely exclusively on the EM spectrum.

Electronic Protective Measures (EPM)

- **Electronic protective** measures (EPM) are defined as that division of EW involving actions taken to ensure friendly effective use of the EM spectrum
- despite the adversary's use of EM energy. There are two subdivisions of EPM:
  - a. **Active EPM. Detectable measures, such as** altering transmitter parameters as necessary, to ensure friendly effective use of the EM spectrum.
  - b. **Passive EPM. Undetectable measures, such as** operating procedures and technical features of equipment, which are meant to ensure friendly effective use of the EM spectrum.

Electronic Warfare (EW)

- EW Assets. Electronic warfare (EW) assets will vary depending on the mission and operational environment but will include at least:
- a. an ESM suite capable of providing localized force protection and limited EW reporting; and
- b. connectivity to national and allied EW/SIGINT assets.

What is Intelligence?

- Intelligence is information gathered within or outside that involves threats to a nation, its people, property, or interests, development, proliferation, or use of weapons of mass destruction, and any other matter bearing on the national or homeland security.

- Intelligence can provide insights not available elsewhere that warn of potential threats and opportunities, assess probable outcomes of proposed policy options, provide leadership profiles on foreign officials, and inform official travelers of counterintelligence and security threats

Example of Intelligence Cycle

- Collect
  - Sensors
- Exploit
  - Analysis/Process
- Disseminate
  - Communication

Types of Intelligence

- The Intelligence Cycle (IC) is a process of collecting information and developing it into intelligence for use by IC customers. The steps in the process are direction, collection, processing, exploitation, and dissemination.

- IC products can either be based on a single type of collection or “all-source,” that is, based upon all available types of collection.

- IC products also can be produced by one IC element or coordinated with other IC elements, and delivered to IC customers in various formats, including papers, digital media, briefings, maps, graphics, videos, and other distribution methods.

MASINT—Measurement and Signature Intelligence

- MASINT—Measurement and Signature Intelligence is technically derived intelligence data other than imagery and SIGINT.
- The data results in intelligence that locates, identifies, or describes distinctive characteristics of targets.
- It employs a broad group of disciplines including nuclear, optical, radio frequency, acoustics, seismic, and materials sciences.
- Examples of this might be the distinctive radar signatures of specific aircraft systems or the chemical composition of air and water samples. The Directorate for MASINT and Technical Collection (DT), a component of the Defense Intelligence Agency, is the focus for all national and Department of Defense MASINT matters.

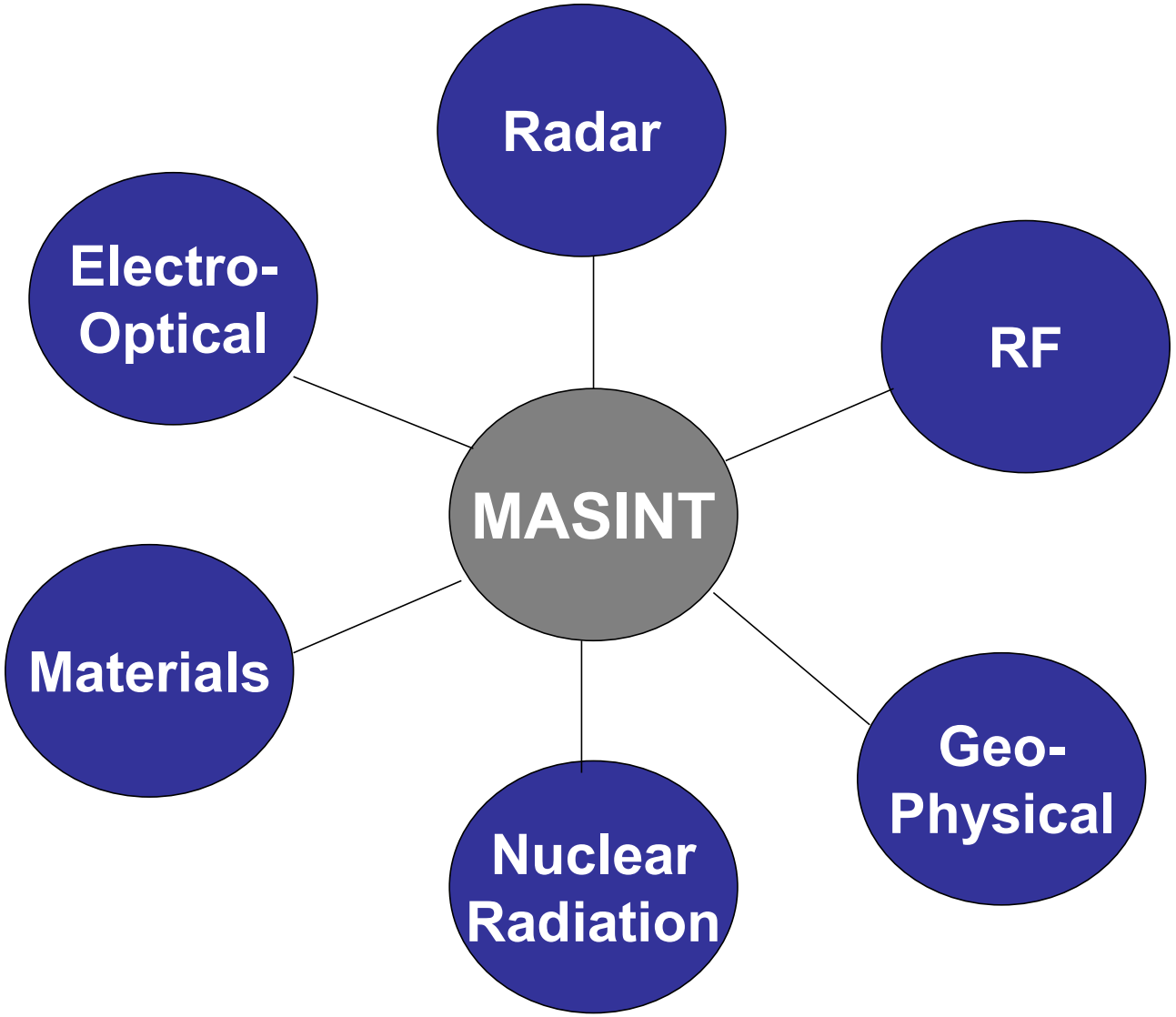
Measurement and Signatures Intelligence (MASINT)

Measurement and Signatures Intelligence (MASINT) is a relatively little-known collection discipline that concerns weapons capabilities and industrial activities.

MASINT includes the advanced processing and use of data gathered from overhead and airborne IMINT and SIGINT collection systems.

Telemetry Intelligence (TELINT) is sometimes used to indicate data relayed by weapons during tests, while electronic intelligence (ELINT) can indicate electronic emissions picked up from modern weapons and tracking systems.

Both TELINT and ELINT can be types of SIGINT and contribute to MASINT.


Radar
Electro-
Optical
RF
MASINT
Materials
Geo-
Physical
Nuclear
Radiation

MASINT

These sub-disciplines are carryovers from the consolidation of diverse activities into MASINT and are useful to technologists and phenomonologists who must match sensing technologies to observable phenomena associated with a particular target or activity.

MASINT is best described by its six sub-disciplines:

1. Radar,
2. RF,
3. Geophysical,
4. Nuclear Radiation,
5. Materials
6. Electro-Optical

MASINT Contribution

- MASINT can provide unique contributions to the IC in terms of specific weapon identification, chemical compositions, material content, etc.

- Such unique identifications will be a major factor in answering the future questions of `who, what, where, when and why.' In fact, some believe MASINT will be the most important `technical INT` of the future.“
  - According to the official definition, MASINT is "technically derived intelligence that detects, locates, tracks, identifies and describes the specific signatures of fixed and dynamic target sources." If this definition seems aggravatingly vague, it is because MASINT is indeed hard to characterize neatly.

  - It is a sprawling discipline, a passive discipline, overlapping but not conforming to accepted notions of SIGINT, IMINT and sometimes even HUMIN

MASINT Processing and Exploitation Techniques

- Measurement and Signal Intelligence (MASINT) provides technically derived intelligence to detect, locate, track, identify, and describe the specific characteristics of fixed and dynamic target objects and sources. Numerous scientific disciplines and advanced technologies are applied in dedicated MASINT systems.

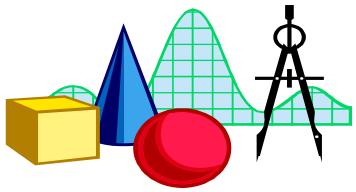
- There are also advanced MASINT processing and exploitation techniques, which broaden the usefulness of data collected by IMINT and SIGINT systems.

- MASINT collection systems include, but are not limited to, radar spectroradiomentric, electro-optical, acoustic, radio frequency, nuclear detection, and seismic sensors, as well as techniques for gathering chemical, biological, nuclear, and other material samples.

More Definitions

- **INTELLIGENCE GEOINT (Geospatial Intelligence):**
  definition provided by United States Intelligence Community
  - The exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth.

- **AGI (Advanced Geospatial Intelligence):**
  - AGI is an extension of GEOINT. AGI includes but not limited to infrared intelligence, multi-spectral intelligence, and radio frequency intelligence. Taking information from imagery data beyond the visual spectrum allows AGI to be used to *see through* some objects. For example, data can also be used to determine temperature and chemical makeup.



Other Sources

- Nuclear Radiation
- X-Ray
- Gamma Ray
- Neutron

Materials

Gases

Liquids

Particulates

Solids

Debris

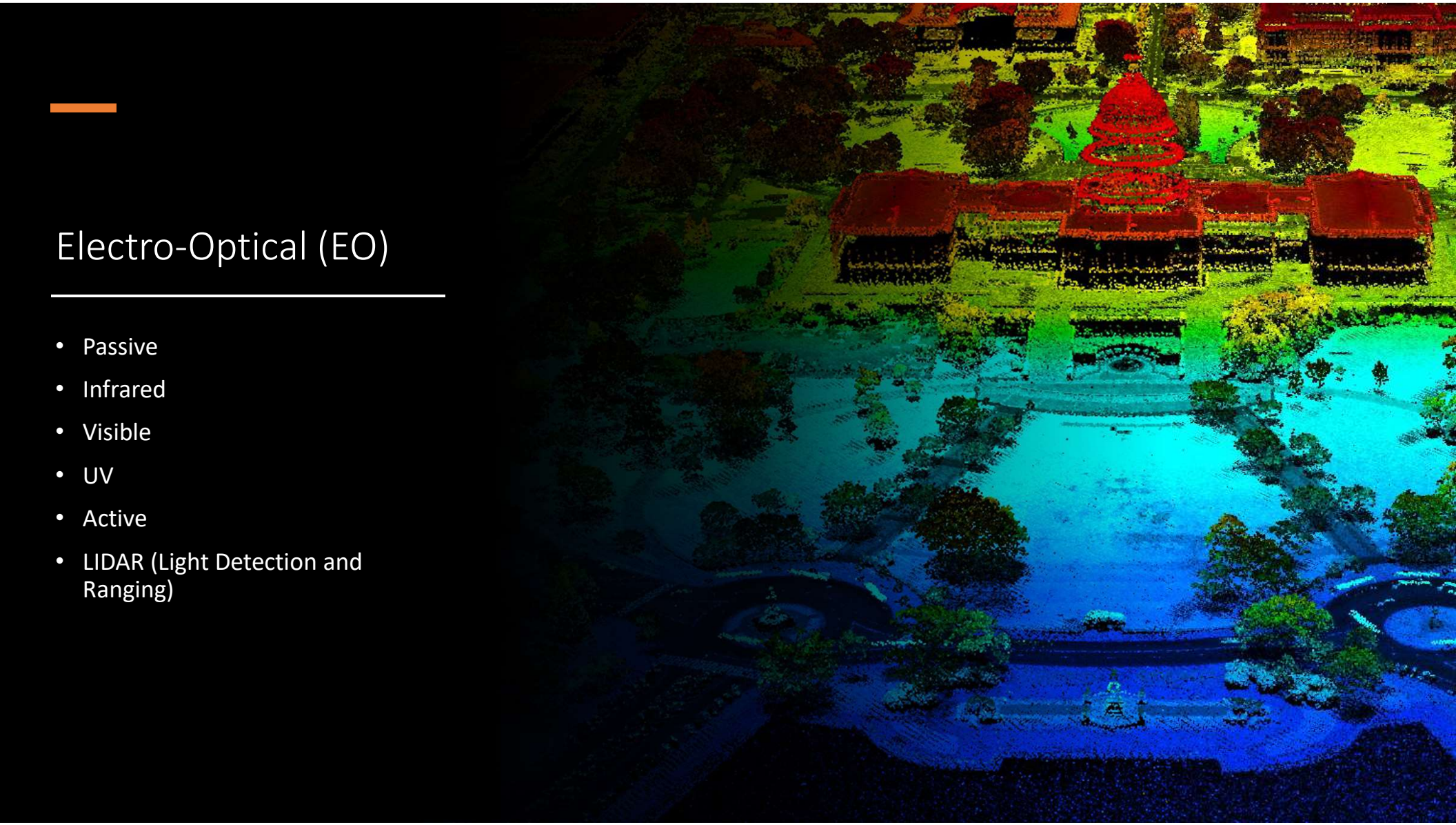
Effluents

Electro-optics (EO)

- **Electro-optics involves components, devices and systems which operate by modification of the optical properties of a material by an electric field. Thus it concerns the interaction between the electromagnetic (optical) and the electrical (electronic) states of materials.**
- **The electro-optic effect relates to a change in the optical properties of the medium which usually is a change in the birefringence and not simply the refractive index.**

Electro-Optical (EO)

- Passive
- Infrared
- Visible
- UV
- Active
- LIDAR (Light Detection and Ranging)



Imagery Intelligence (IMINT)

- **Imagery Intelligence (IMINT)** is sometimes also referred to as photo intelligence (PHOTINT).

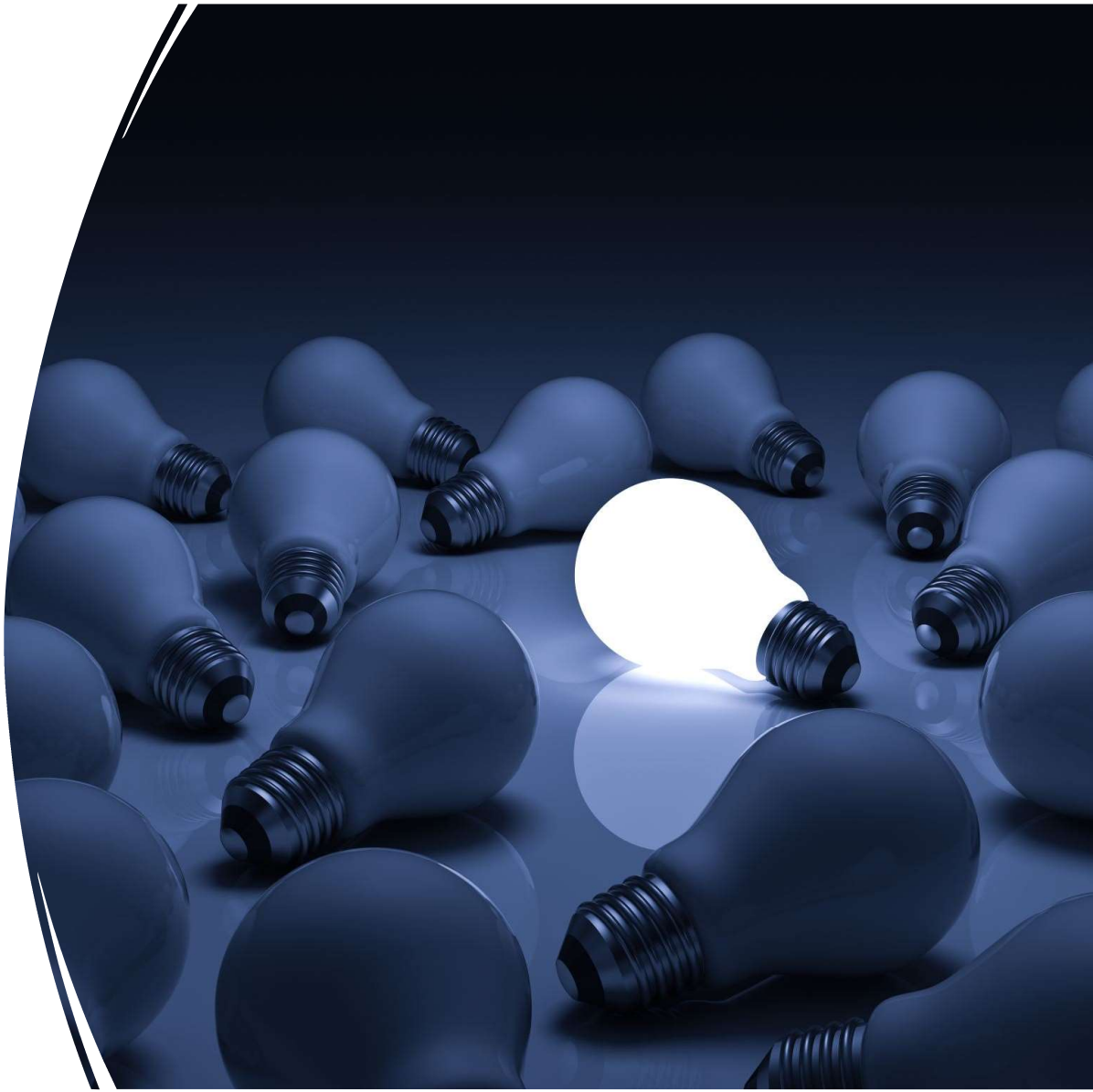
- One of the earliest forms of IMINT took place during the Civil War, when soldiers were sent up in balloons to gather intelligence about their surroundings.

- IMINT was practiced to a greater extent in World Wars I and II when both sides took photographs from airplanes.

Imagery Intelligence (IMINT)

- Imagery intelligence (IMINT) is intelligence derived from the analysis of any image acquired by photographic, radar, electro-optical (EO), infra-red, thermal and multi-spectral sensors.

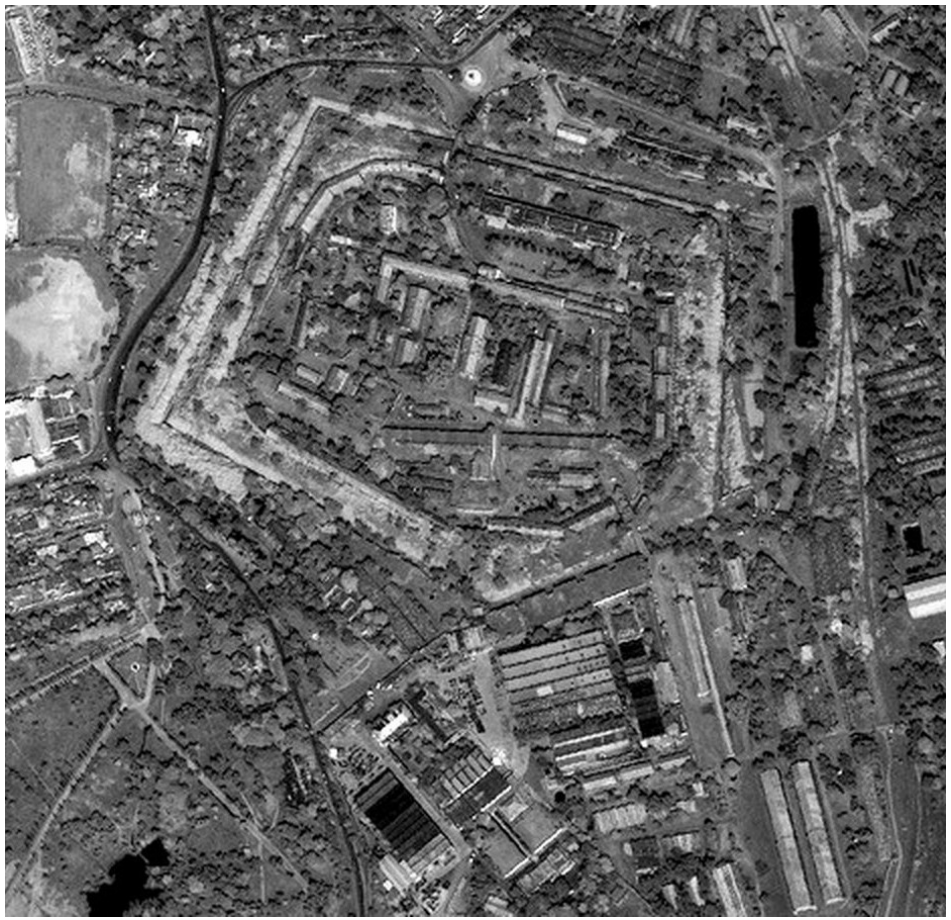
- It is an important element of the all-source intelligence capability at the strategic, operational and tactical levels.



Geospatial Intelligence (GEOINT)

- **Geospatial Intelligence (GEOINT)** is the analysis and visual representation of security related activities on the earth.

- It is produced through an integration of imagery, imagery intelligence, and geospatial information.



HUMINT

- Human intelligence is derived from human sources.
- To the public, HUMINT remains synonymous with espionage and clandestine activities; however, most of HUMINT collection is performed by overt collectors such as strategic debriefers and military attaches.
- It is the oldest method for collecting information, and until the technical revolution of the mid- to late 20th century, it was the primary source of intelligence.

Human Intelligence (HUMINT)

- **Human Intelligence (HUMINT)** is the collection of information from human sources.

- The collection may be done openly, as when agents interview witnesses or suspects, or it may be done through clandestine or covert means (espionage).

Open-Source Intelligence (OSINT)

- **Open-Source Intelligence (OSINT)** refers to a broad array of information and sources that are generally available, including information obtained from the media (newspapers, radio, television, etc.), professional and academic records (papers, conferences, professional associations, etc.), and public data (government reports, demographics, hearings, speeches, etc.).

OSINT

- Open-Source Intelligence is publicly available information appearing in print or electronic form including radio, television, newspapers, journals, the Internet, commercial databases, and videos, graphics, and drawings.

- While open-source collection responsibilities are broadly distributed through the IC, the major collectors are the DNI's Open Source Center (OSC) and the National Air and Space Intelligence Center (NASIC).

Central MASINT Office (CMO)

- The Defense Intelligence Agency's **Central MASINT Office** (CMO), is the principal user of MASINT data. Measurement and Signatures Intelligence has become increasingly important due to growing concern about the existence and spread of weapons of mass destruction.

- MASINT can be used, for example, to help identify chemical weapons or pinpoint the specific features of unknown weapons systems. The FBI's extensive forensic work is a type of MASINT.

- The FBI Laboratory's Chem-Bio Sciences Unit, for example, provides analysis to detect traces of chemical, biological, or nuclear materials to support the prevention, investigation, and prosecution of terrorist activities.

OSINT Accessibility

Unlike the other INTs, open-source intelligence is not the responsibility of any one agency, but instead is collected by the entire U.S. Intelligence Community.

One advantage of OSINT is its accessibility, although the sheer amount of available information can make it difficult to know what is of value.

Determining the data's source and its reliability can also be complicated. OSINT data therefore still requires review and analysis to be of use to policymakers.

Discussions

Review

Types of Intelligence

- The Intelligence Cycle (IC) is a process of collecting information and developing it into intelligence for use by IC customers. The steps in the process are direction, collection, processing, exploitation, and dissemination.

- IC products can either be based on a single type of collection or “all-source,” that is, based upon all available types of collection.

- IC products also can be produced by one IC element or coordinated with other IC elements, and delivered to IC customers in various formats, including papers, digital media, briefings, maps, graphics, videos, and other distribution methods.

Six Basic Intelligence Sources

There are six basic intelligence sources, or collection disciplines:

- SIGINT—Signals Intelligence
- IMINT—Imagery Intelligence
- MASINT—Measurement and Signature
- HUMINT—Human intelligence
- OSINT—Open-Source Intelligence
- GEOINT—Geospatial Intelligence

Note

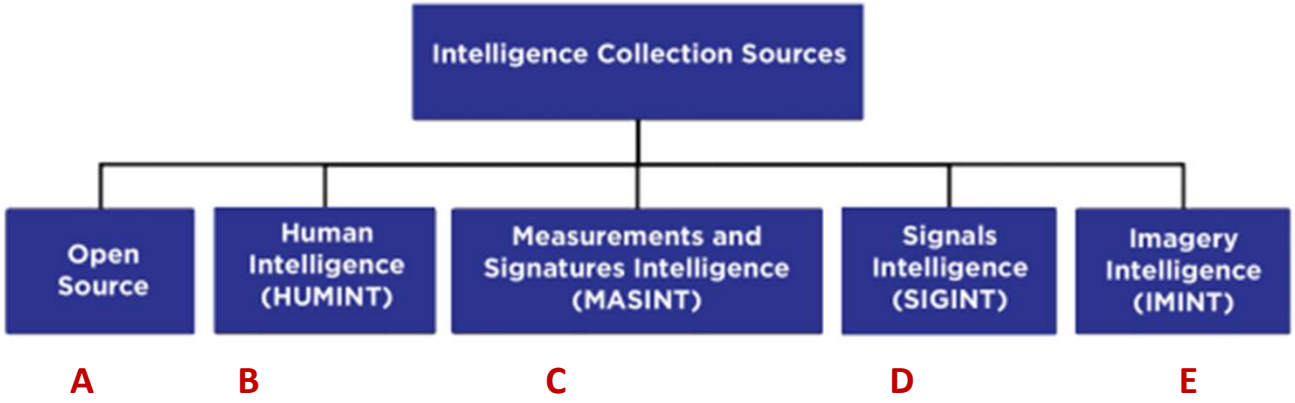
SIGNIT or Signal Intelligence is primarily used to intercept signals transmitted from communication systems, radars and other electronic devices.

Based on the type of signals received, this is further classified into: Communication Intelligence (COMINT), Electronic Intelligence (ELINT), and Foreign Instrumentation Signals Intelligence (FISINT).

Intelligence Collection Disciplines or the "INTs."

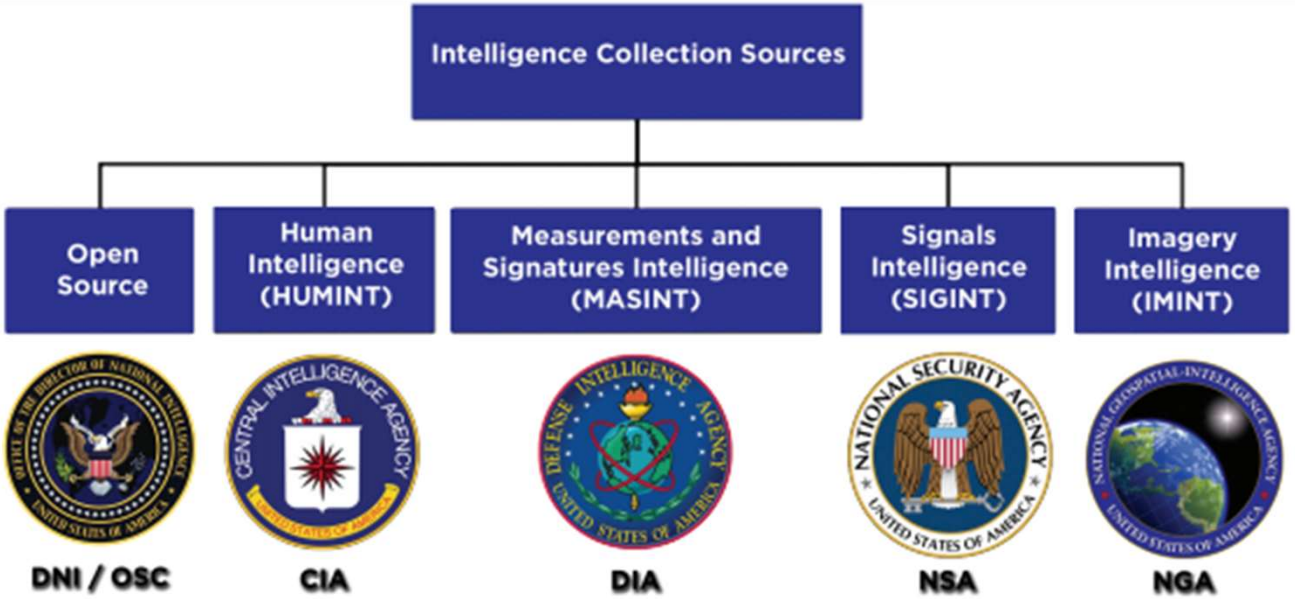
Signals Intelligence (SIGINT)	**Measurement and Signatures Intelligence (MASINT)**	**Imagery Intelligence (IMINT)**
Geospatial Intelligence (GEOINT)	**Human Intelligence (HUMINT)**	**Open-Source Intelligence (OSINT)**

Match Intelligence Collection Sources to Organizations



1. Central Intelligence Agency (CIA)
2. Federal Bureau of Investigation (FBI)
3. National Security Agency (NSA)
4. National Geospatial-Intelligence Agency (NGA)
5. Defense Intelligence Agency (DIA)
6. Director of National Intelligence – Open-Source Center (DIA/OSC)

Intelligence Collection Sources (USA)



Source: https://www.fbi.gov/about/leadership-and-structure/intelligence-branch

Note

SIGNIT or Signal Intelligence is primarily used to intercept signals transmitted from communication systems, radars and other electronic devices.

Based on the type of signals received, this is further classified into: Communication Intelligence (COMINT), Electronic Intelligence (ELINT), and Foreign Instrumentation Signals Intelligence (FISINT).

SIGINT Types and Technologies

- ELINT
- COMINT
- FISINT

Airborne

Ground

Naval

Space

Cyber

SIGINT = ELINT+COMINT+FISINT

COMINT

- Interception of communications between people or machines

ELINT

- Detection and analysis of non-communications electronic transmissions
- Electronic Warfare: radiation from electronic systems, jamming radiation, weapon systems and missiles

FISINT (Foreign Instrumentation Signature INTelligence)

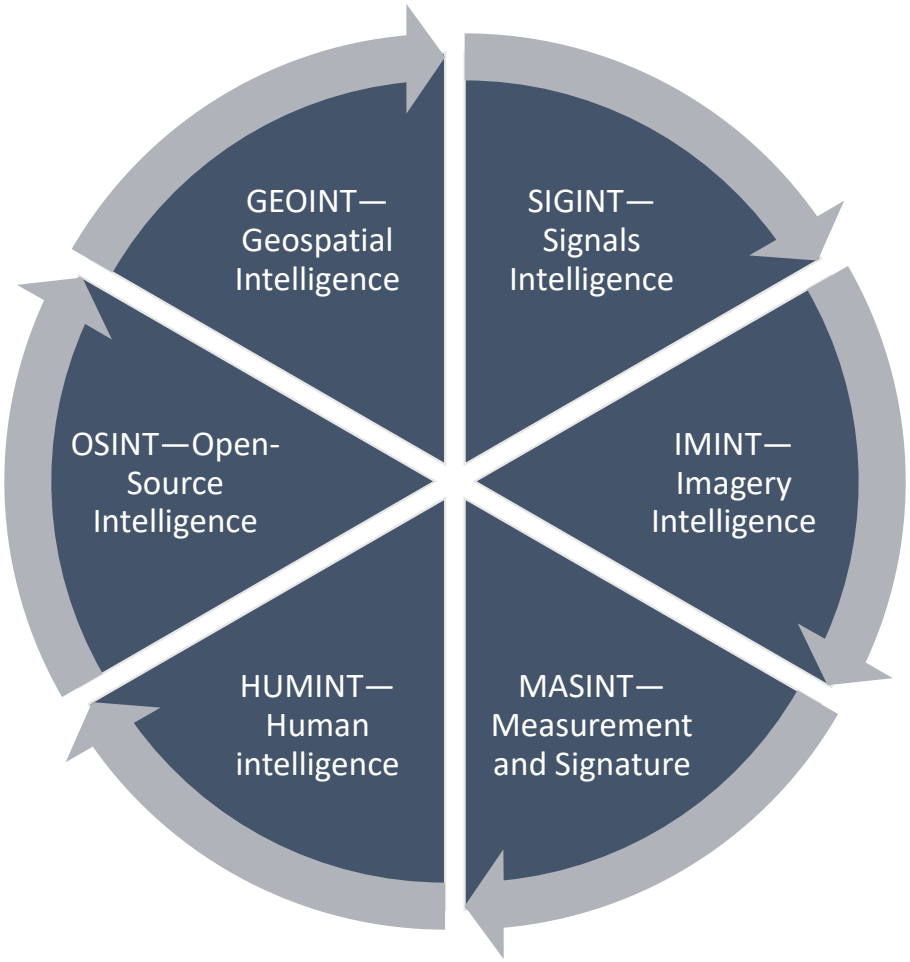
- FISINT is also considered as a subset of MASINT (measurement and signature intelligence).

MASINT

- Scientific and technical intelligence obtained by quantitative and qualitative analysis of data
- Data= metric dependence, modulation, plasma or hydromagnetic
- MASINT can provide specific weapon system identifications, chemical compositions and material content and a potential adversary's ability to employ these weapons.

Six Basic Intelligence Sources

There are six basic intelligence sources, or collection disciplines:

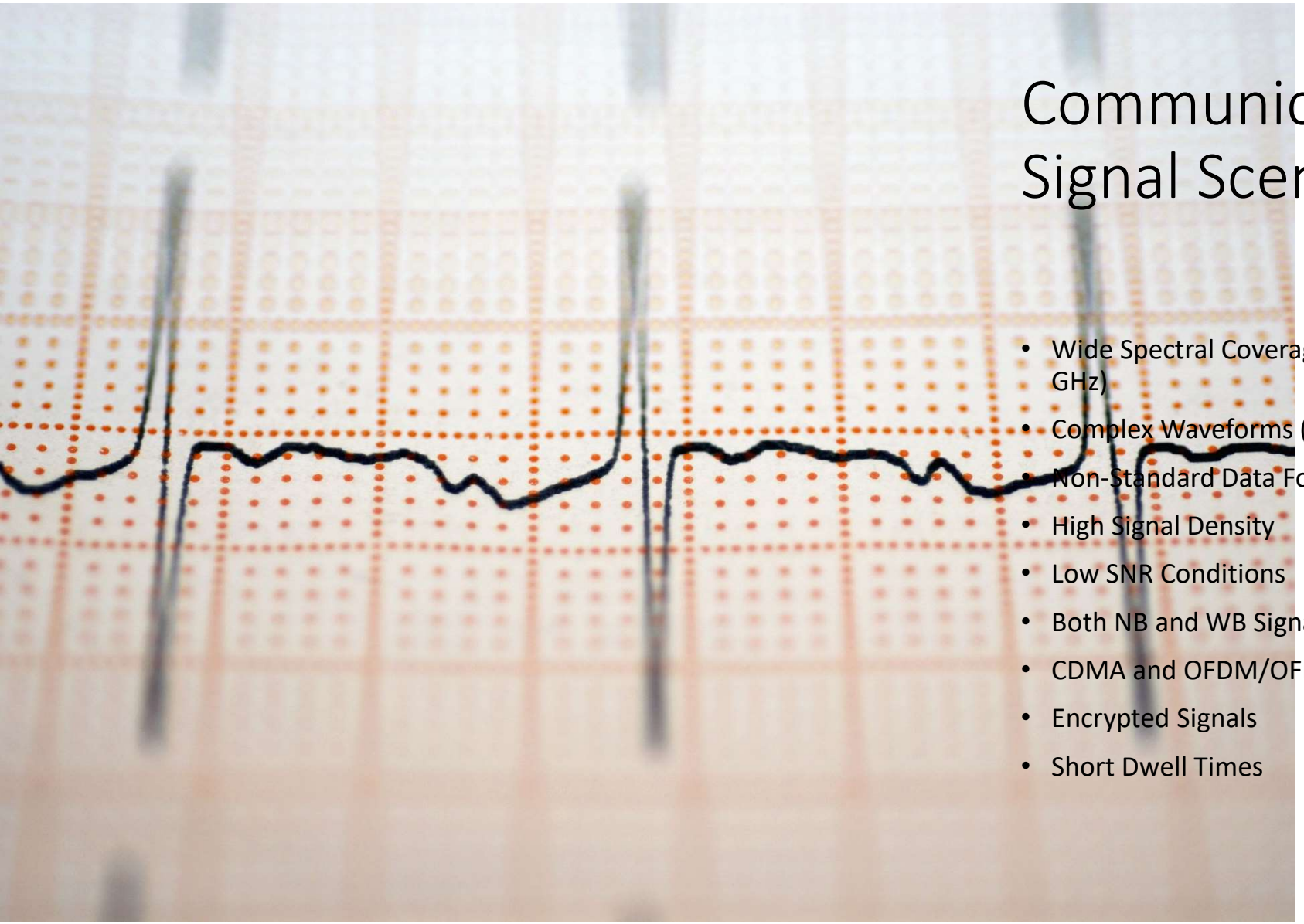


Communications Intelligence

- Communications intelligence (COMINT) is the technical and intelligence information derived from foreign communications by anyone of the than the intended recipient.

COMINT

- Search, DF and Intercept
- Location fixing of emitters
- Signal analysis and classifications
- Monitoring
- Recording
- Evaluation
- Tactical report generation



Communication Signal Scenarios

- Wide Spectral Coverage (1.5 MHz - 60 GHz)
- Complex Waveforms (Burst, FH, DS)
- Non-Standard Data Formats
- High Signal Density
- Low SNR Conditions
- Both NB and WB Signals (FDM, TDM)
- CDMA and OFDM/OFDMA Types
- Encrypted Signals
- Short Dwell Times

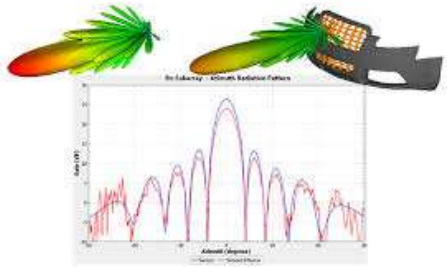
Electronics Intelligence

- Electronics intelligence (ELINT) is the technical and intelligence information derived from foreign noncommunication electromagnetic radiation emanating from anywhere other than nuclear detonations or radioactive sources.

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

ELINT

- Search
- Intercept
- Locate
- Record
- Analysis of radiated EM energy



ELINT Analysis

- The location of early warning, surveillance, and fire control radars can provide a general trace of the adversary's forward battle positions and locations of key C2 and fire control nodes and weapons systems.

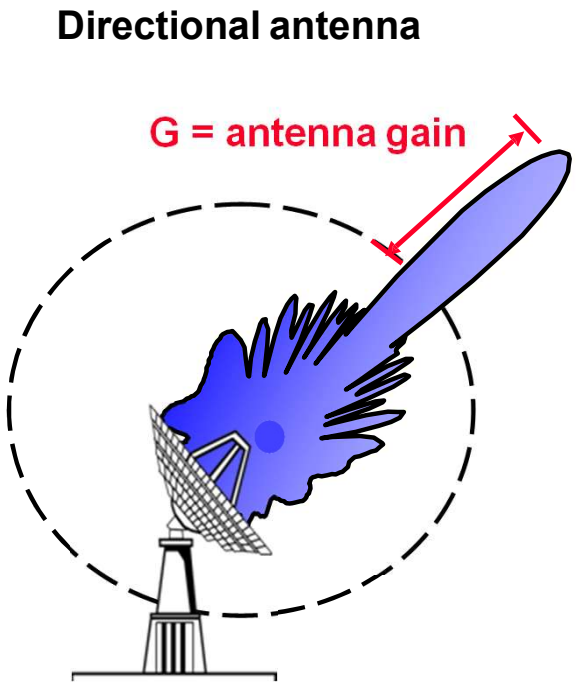
- Medium-range and counter weapons radar identification provides order of battle information since these systems are organic to specific adversary units.

- Identification and location of air defense radars provide information on the disposition of the adversary's air defense systems and their threat to strike, close air support, and assault support aircraft.

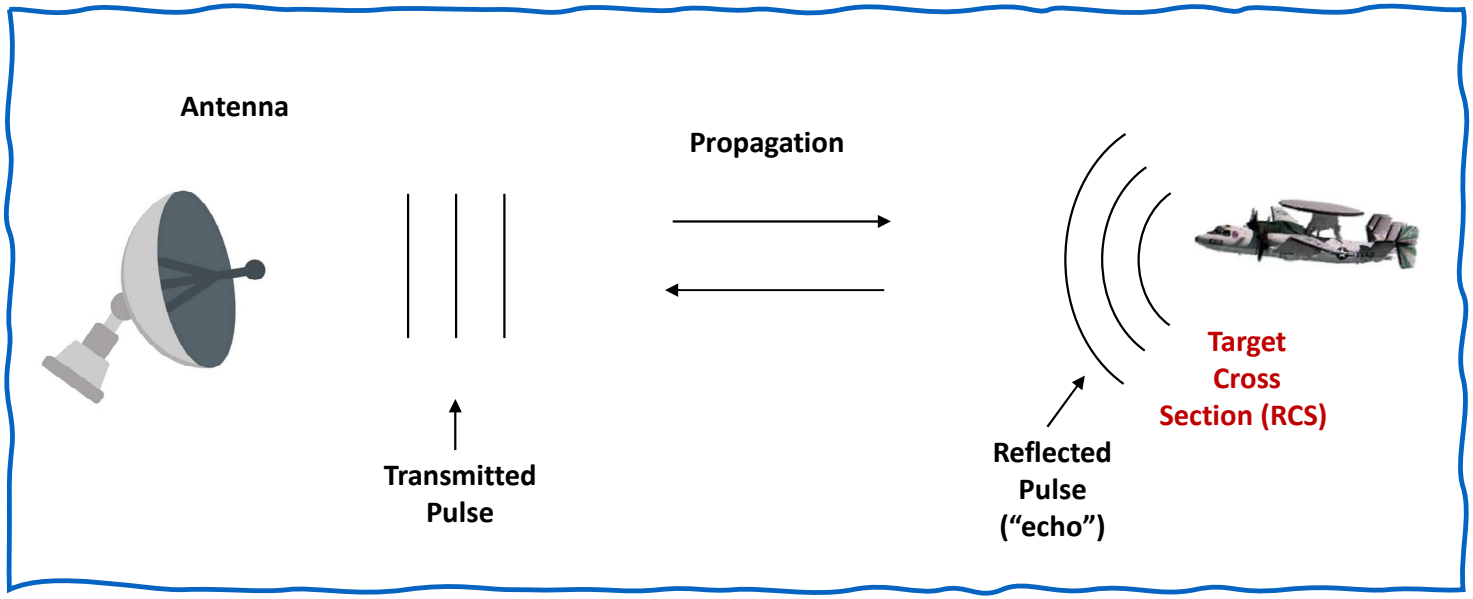
- Following the reporting of any I&W (indications and warning) information to tactical decisionmakers, technical data and detailed ELINT information is forwarded to

Radar Types

- Phased-Array Radar
- Passive vs. active radar
- Bistatic radar
- Continuous-wave radar
- Doppler radar
- Fm-cw radar
- Monopulse radar
- Planar array radar
- Pulse-doppler



RADAR
RAdio Detection And Ranging



Radar observables:

- Target range
- Target angles (azimuth & elevation)
- Target size (radar cross section)
- Target speed (Doppler)
- Target features (imaging)

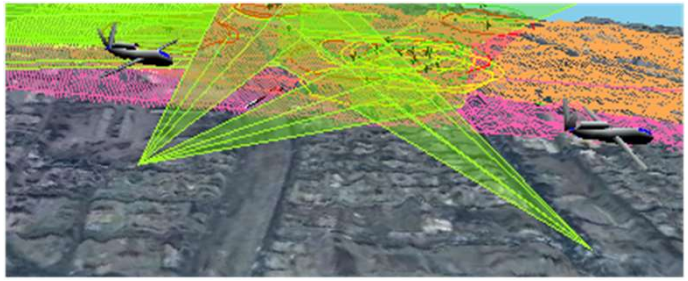
MASINT

- **Measurement and Signatures Intelligence (MASINT)** is a relatively little-known collection discipline that concerns weapons capabilities and industrial activities.

- MASINT includes the advanced processing and use of data gathered from overhead and airborne IMINT and SIGINT collection systems.

- Telemetry Intelligence (TELINT) is sometimes used to indicate data relayed by weapons during tests, while electronic intelligence (ELINT) can indicate electronic emissions picked up from modern weapons and tracking systems.

- Both TELINT and ELINT can be types of SIGINT and contribute to MASINT.



MASINT Information

- MASINT uses sensors to identify the distinctive characteristic of fixed, changing or moving targets.
- This is important in detecting, identifying and tracking threats such as missiles, enemy submarines or aircraft.
- In the simplest terms, MASINT involves using specially designed sensors to collect and analyze information associated with either a source, emitter, sender or receiver that isn't collected through other means.
- MASINT provides identification, early warning and tracking capabilities derived from various sensors. This information is utilized to assess impact locations or provide early warning.

- Radar;
- Radio Frequencies;
- Geo-Physical;
- Nuclear Radiation; and,
- Electro-optical sensors.

Discussions

Appendix A: Technical Definitions

- Collection
- Targeting
- Intercept management
- Signal detection
- Traffic analysis
- Electronic order of battle
- Communications intelligence

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.

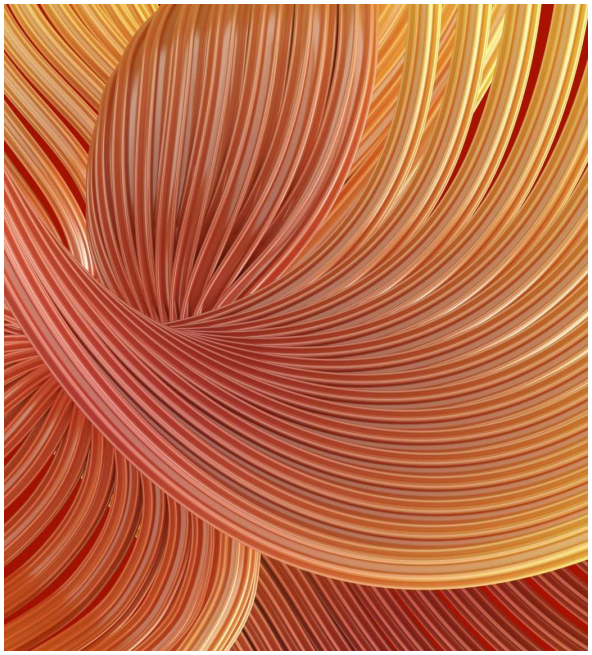
Simplified spectrum analyzer display of superheterodyned, amplitude modulated signals.

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).

If the frequency is not known, the operators may look for power on primary or sideband frequencies using a spectrum analyzer. Information from the spectrum analyzer is then used to tune receivers to signals of interest.

Hypothetical displays from four spectrum analyzers connected to directional antennas. The transmitter is at bearing 090 degrees.

Real-world transmitters and receivers usually are directional. In the figure to the left, assume that each display is connected to a spectrum analyzer connected to a directional antenna aimed in the indicated direction.

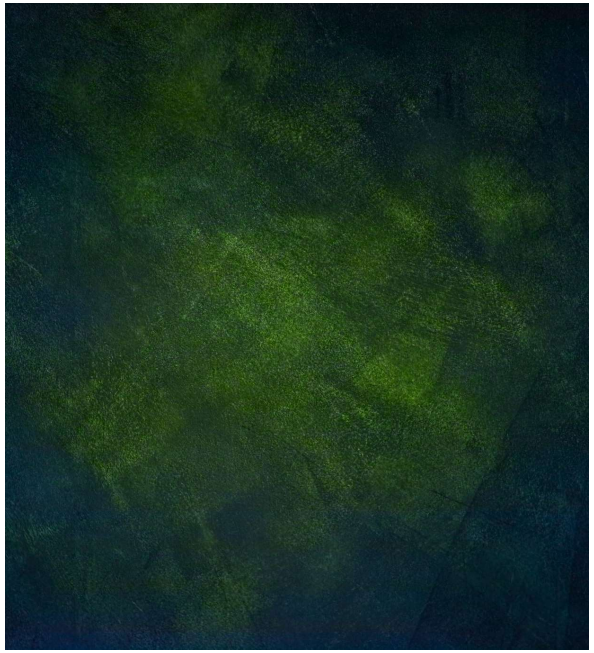


Electronic Order of Battle (EOB)

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.



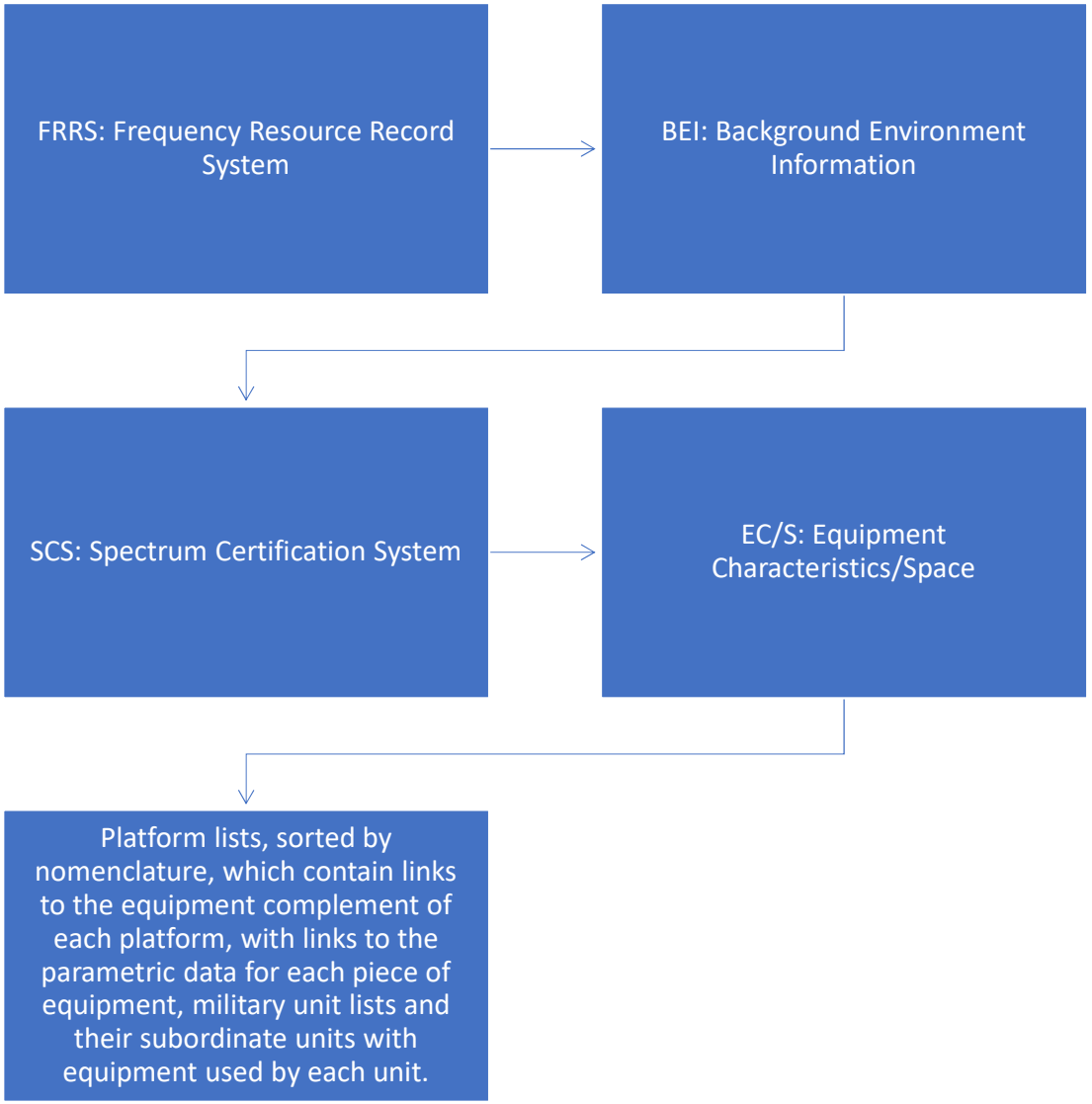
Generating the Electronic Order of Battle (EOB)

- 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

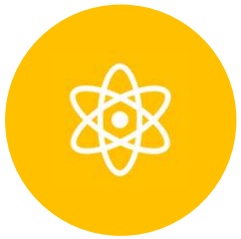
EOB and related data flow

- 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.

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

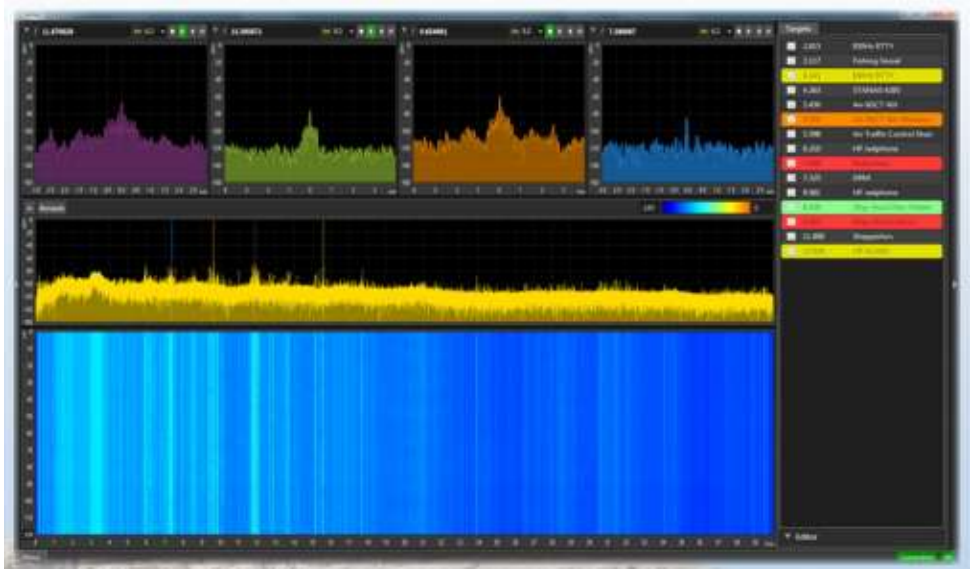
Name	Frequency
Direction Finding System	20 MHz – 6 GHz
HF Direction Finding System	1.5 MHz – 30 MHz
VHF Super Resolution Direction Finding Antenna	20 MHz – 300 MHz
VHF - UHF Super Resolution Direction Finding Antenna	20 MHz – 6 GHz

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.

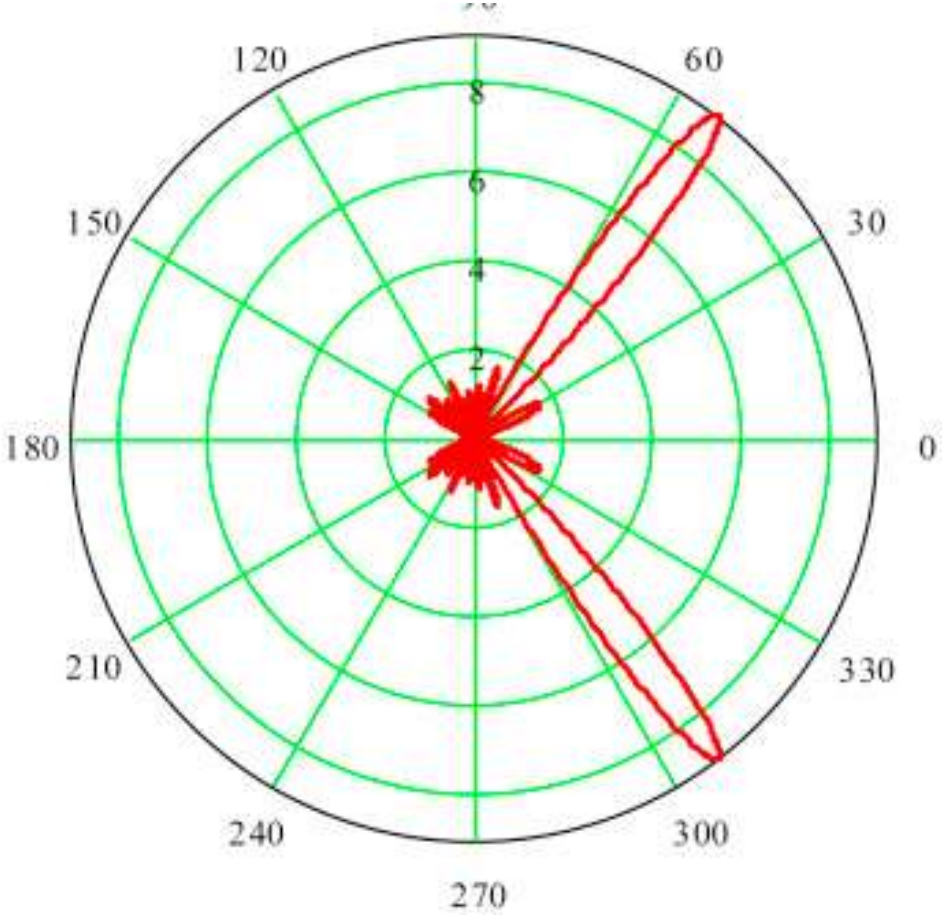
- An order of magnitude increase in spatial resolution
- Increased Direction Finding (DF) accuracy
- Simultaneous azimuth and elevation DF
- Operation with short duration signals
- No requirement for a particular array geometry

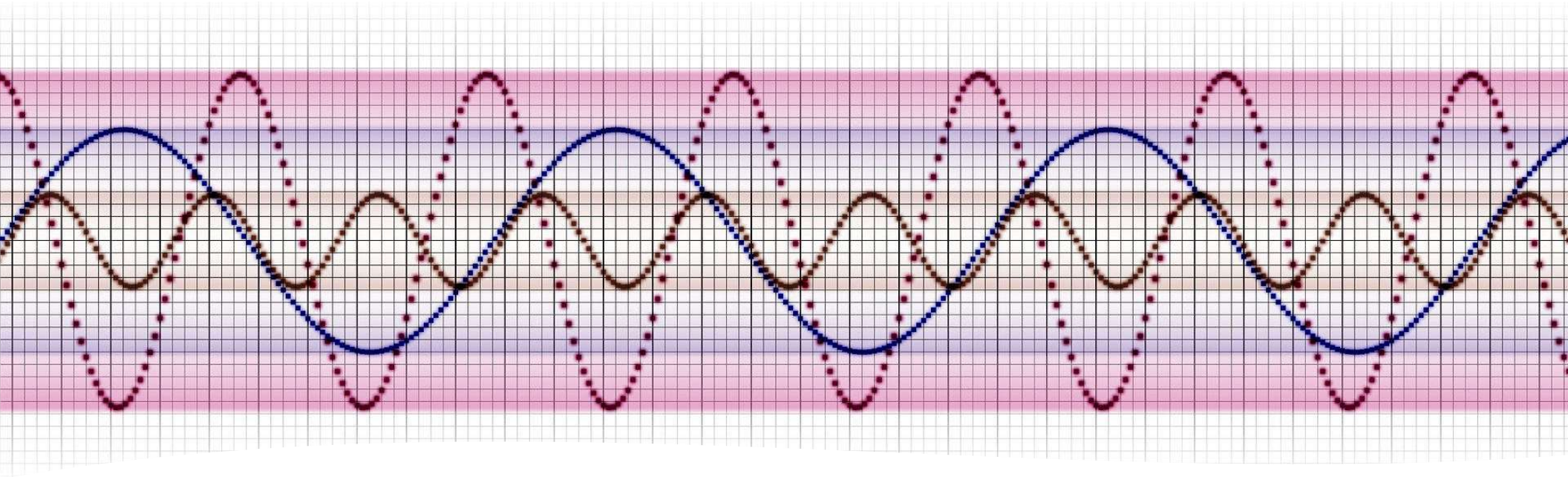


ADAPTIVE DIGITAL BEAMFORMING (ADBF)

- 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

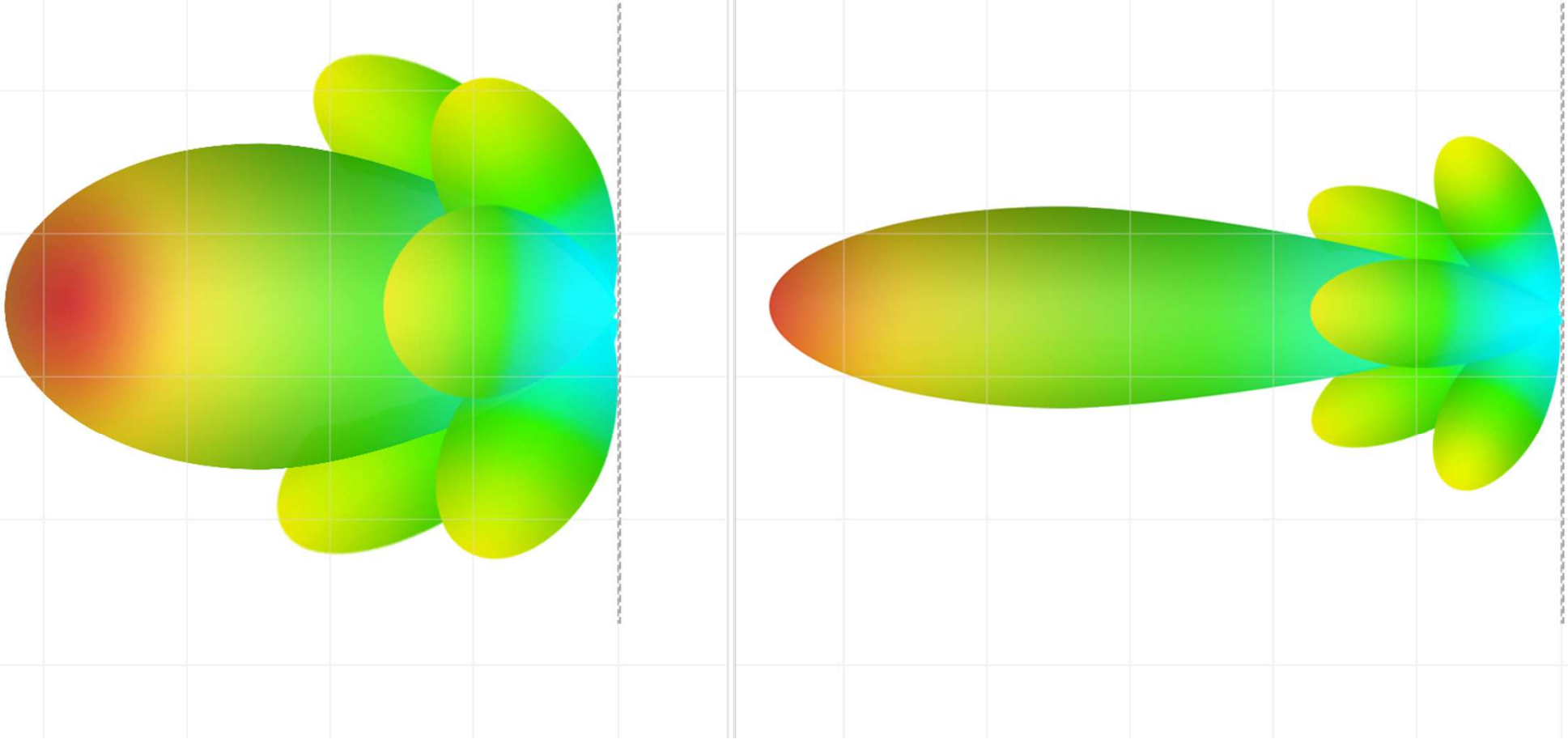




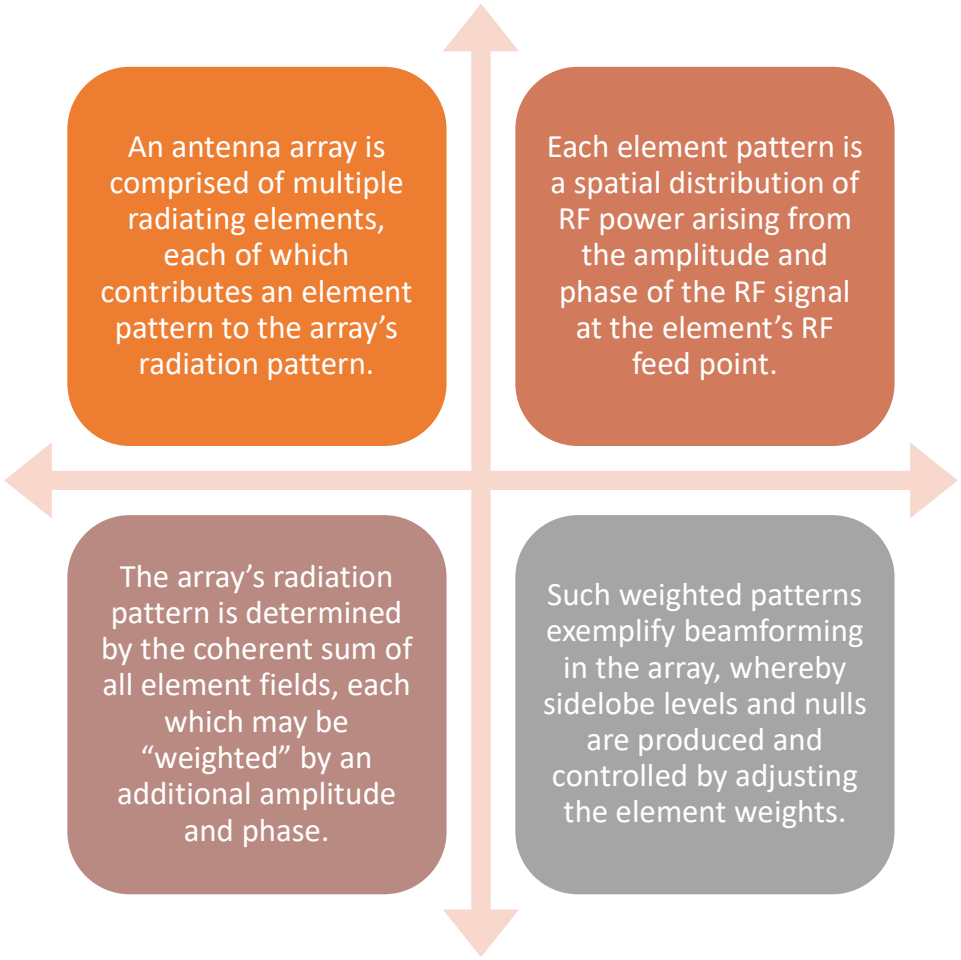
Beamforming

- 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).

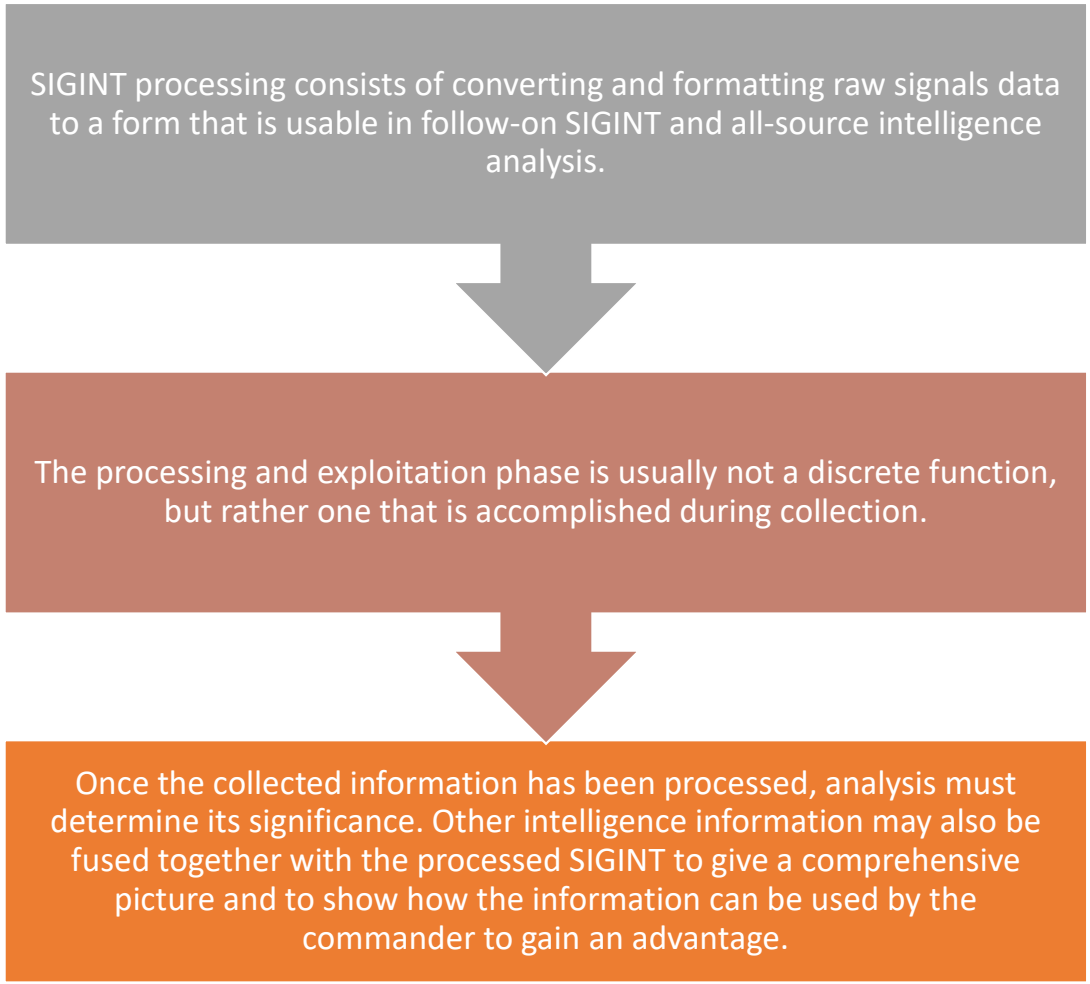
Basically, adaptive beamformers are designed to adjust to differing situations in order to maximize or minimize SINR, which helps measure the quality of wireless communication.

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.


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

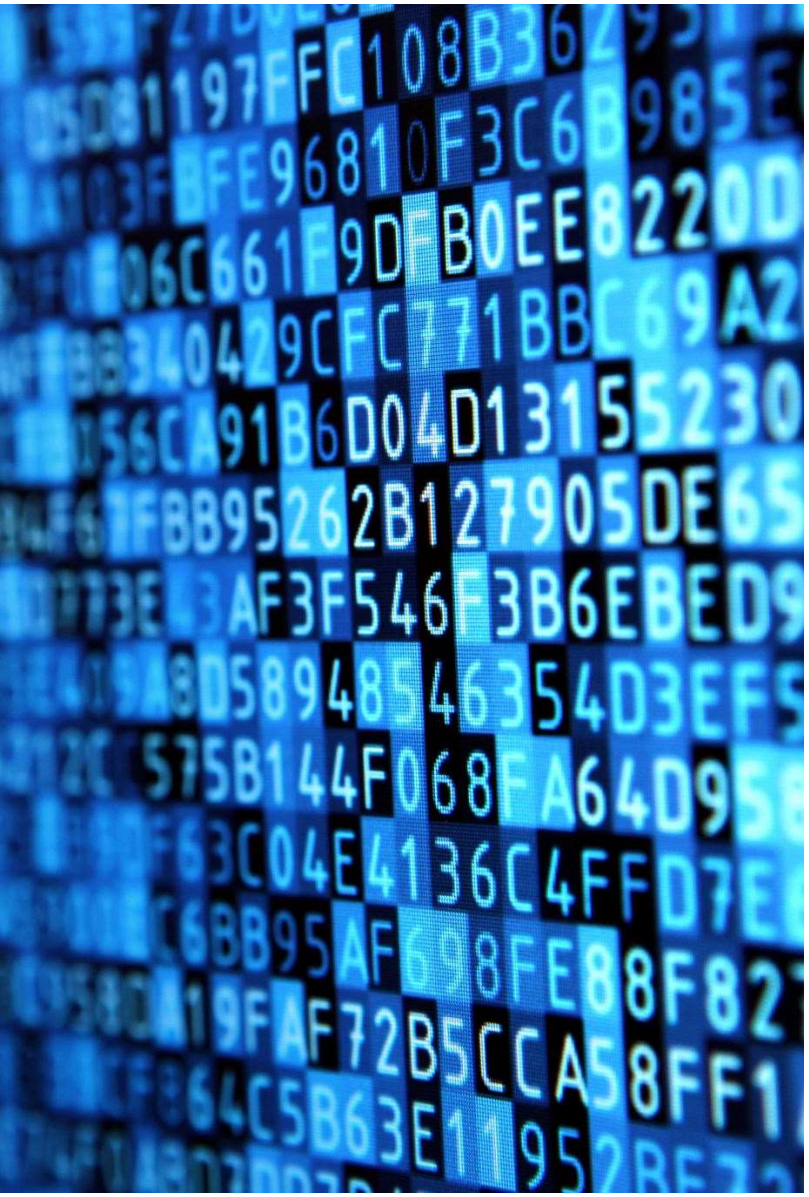
- Linguistic analysis is the transcription and translation of foreign language intercepts into for example English, German or Japanese.

- 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.

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

Signaling Channel Interception

A given digital communications link can carry thousands or millions of voice communications, especially in developed countries.

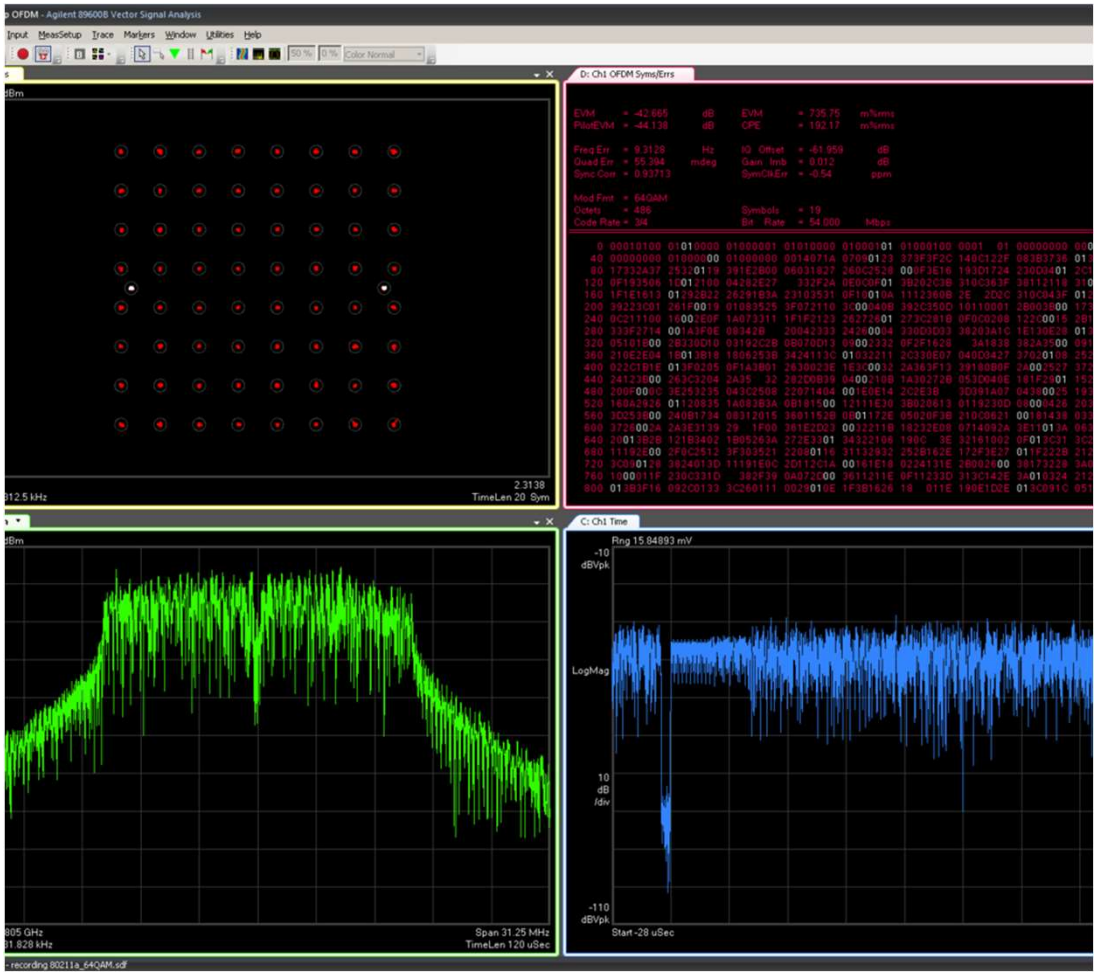
Without addressing the legality of such actions, the problem of identifying which channel contains which conversation becomes much simpler when the first thing intercepted is the signaling channel that carries information to set up telephone calls.

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.

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

Principles of Collection

- Signals are derived from many sources, but the specific steps taken to winnow large data streams to those that are manageable and potentially productive are the same regardless of the source.

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)

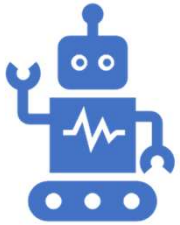
- Electronic Warfare Support Electronic warfare support (ES) includes actions tasked by or under the direct control of an operational commander to search for, intercept, identify, and locate sources of intentional and unintentional radiated enemy electromagnetic signals for the purpose of immediate threat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

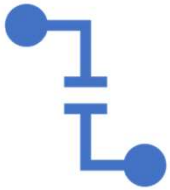
For example, EA may be conducted to interfere with the adversary's use of an emitter the same time as SIGINT operations are designed to exploit the adversary's use of the same emitter.

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.

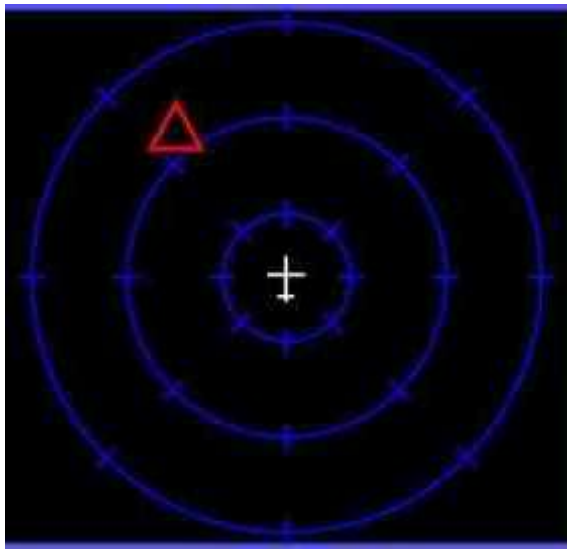
Threats and Enemy Capabilities

- 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

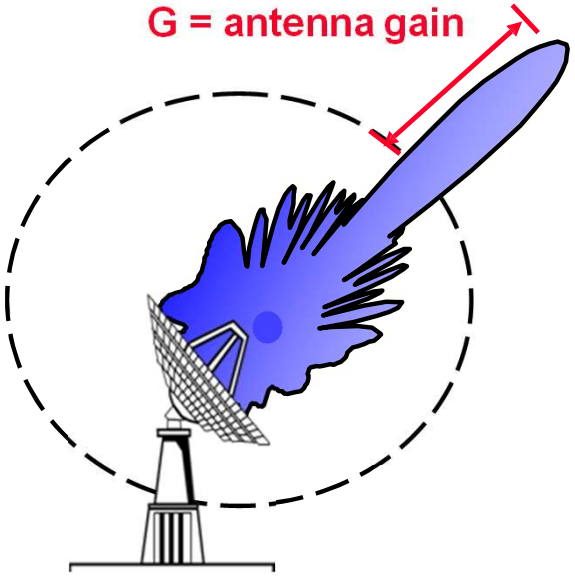
SIGINT supports targeting by providing key operational and locational intelligence on enemy C2 operations and facilities, weapons systems, force compositions, and dispositions.

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.

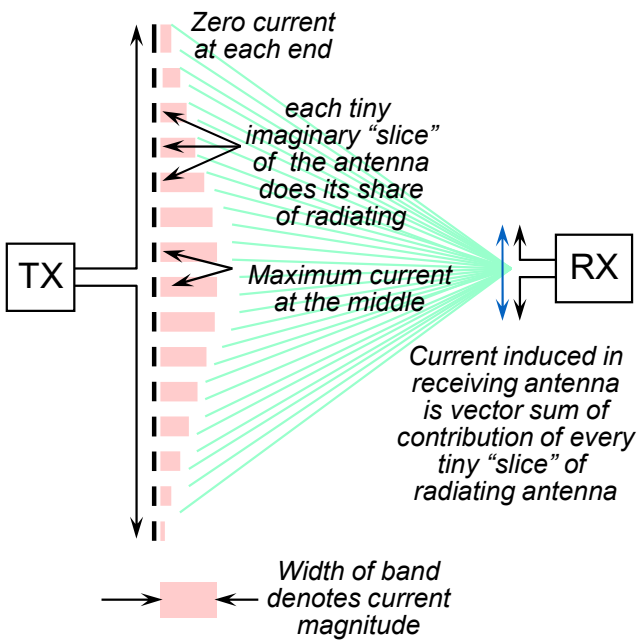
Discussions

Directional antenna



Basics of Antenna

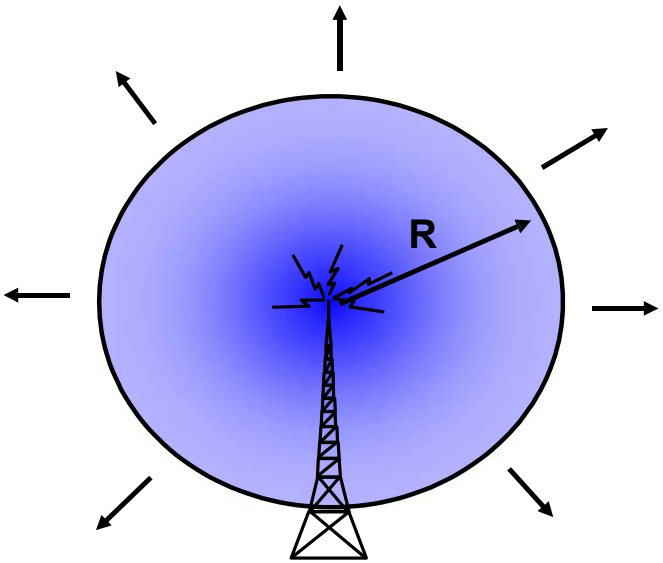
Electromagnetics: Antenna and Radiation Modeling



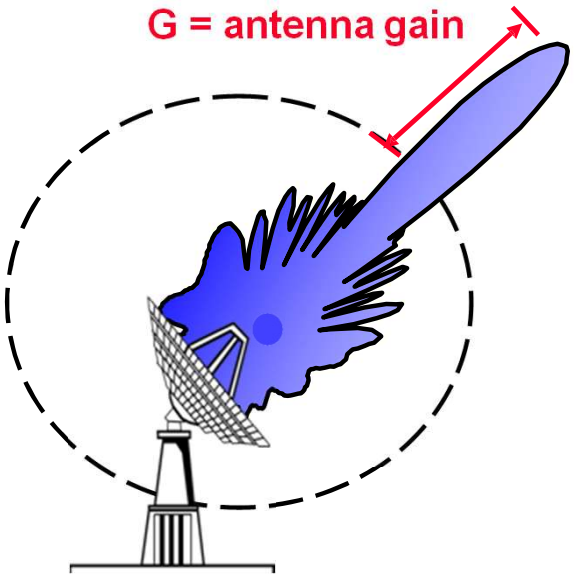
- Maxwell's equations describe how standing waves of current on antennas cause electromagnetic fields to radiate outward and have specific shapes
- Using NEC (numeric electric code) software it is possible to predict the shape of the radiation given off by a specific antenna, and to calculate how the radiated energy is coupled into surrounding objects
- Even the incidental radiation to and from unintended "antennas" can be modeled and predicted using these techniques

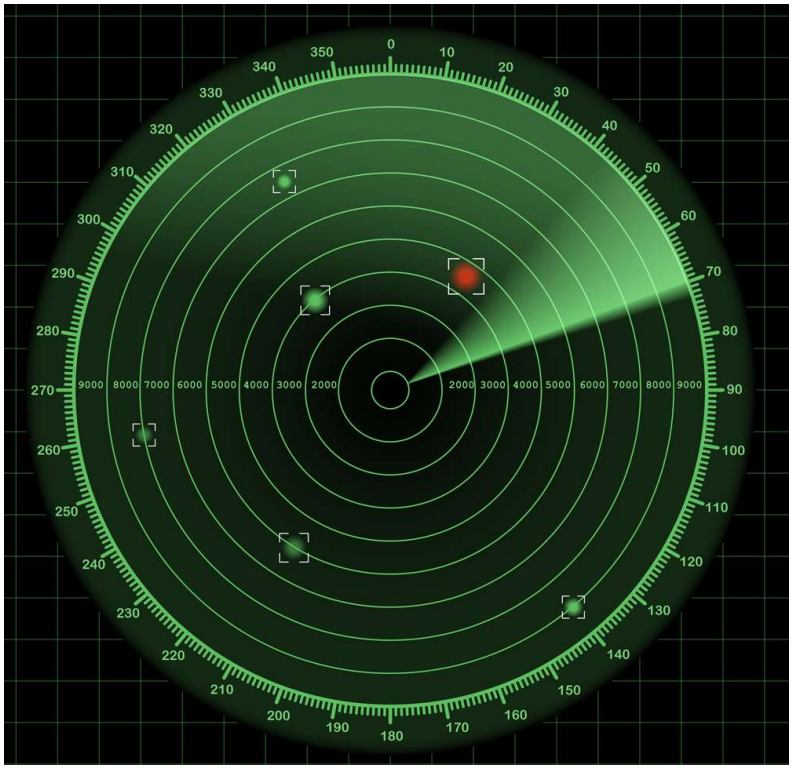
Antenna Gain

Isotropic antenna



Directional antenna





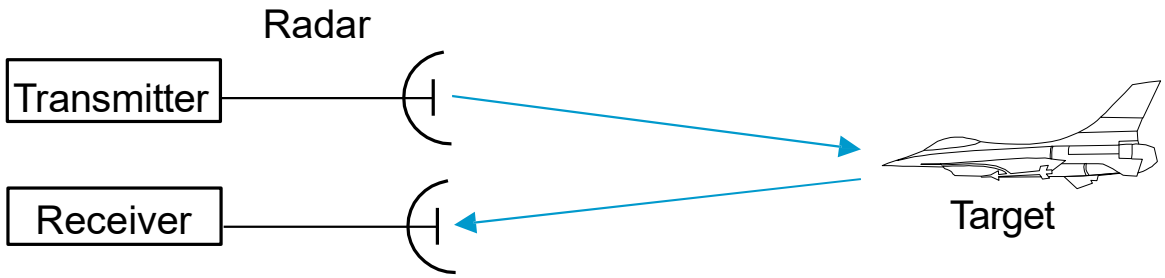
Basics of Radar

Radar Functions

- Normal radar functions:
    1. range (from pulse delay)
    2. velocity (from Doppler frequency shift)
    3. angular direction (from antenna pointing)
- Signature analysis and inverse scattering:
    4. target size (from magnitude of return)
    5. target shape and components (return as a function of direction)
    6. moving parts (modulation of the return)
    7. material composition

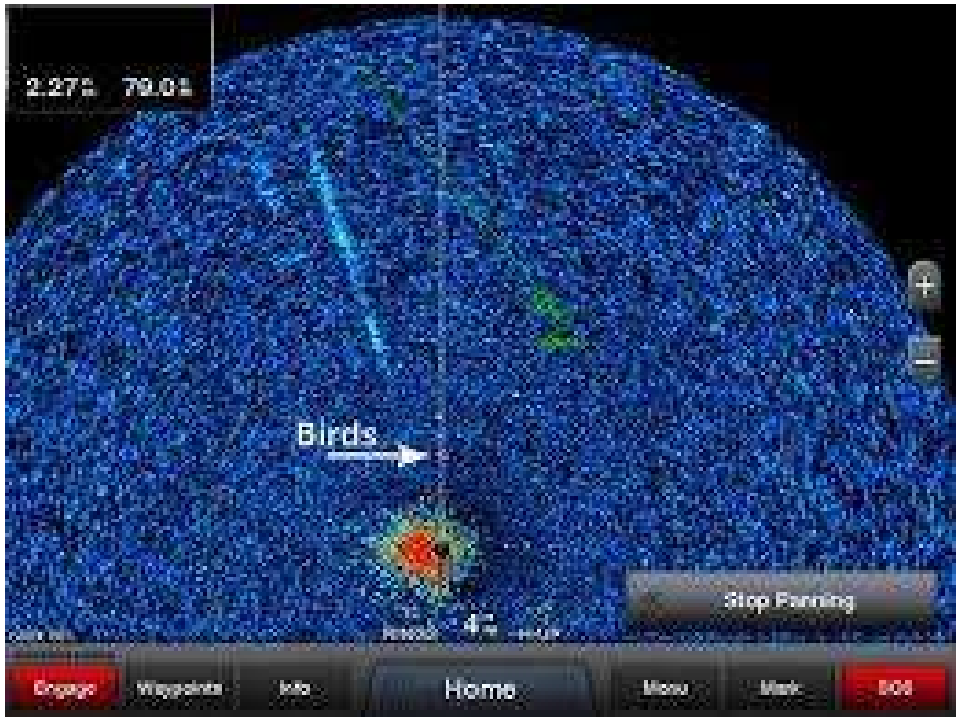
- The complexity (cost & size) of the radar increases with the extent of the functions that the radar performs.

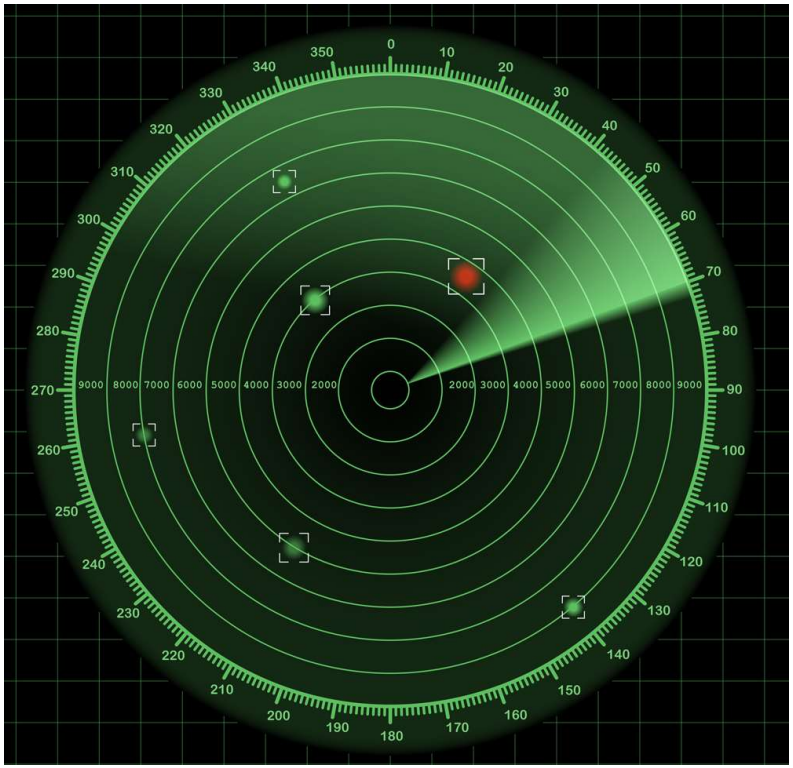
Simplified Radar



- A portion of the transmitted energy is intercepted by the target and reradiated in all directions
- The energy that is reradiated back to the radar is of prime interest to the radar
- The receiving antenna collects the returned energy and delivers it to the receiver, where it is processed to:
  - Detect the target
  - Extract its location and relative velocity
- Direction, or angular position, of the target may be determined from the direction of arrival of the returned signal, assuming a narrow antenna beam
- If relative motion exists between the target and radar, the shift in carrier frequency of the reflected wave (Doppler Effect) is a measure of relative radial velocity of the target and can be used to distinguish moving targets from stationary objects.

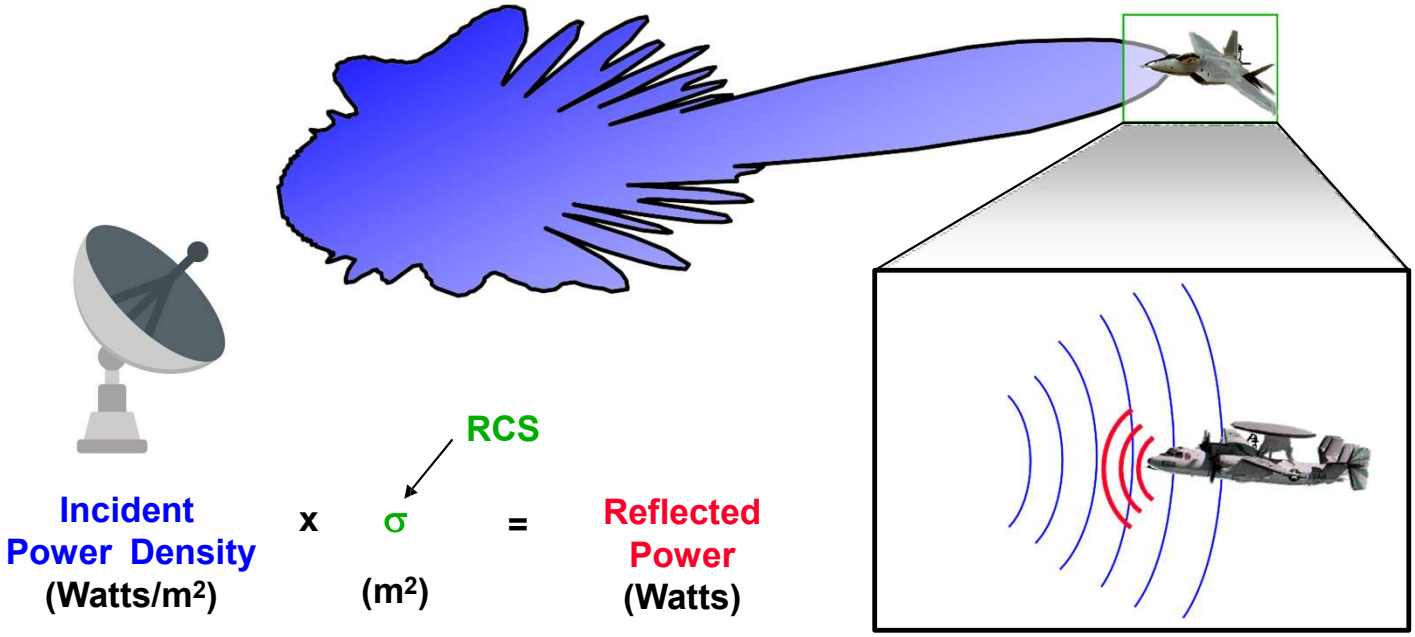
Birds as a Targets





Radar Cross Section (RCS)

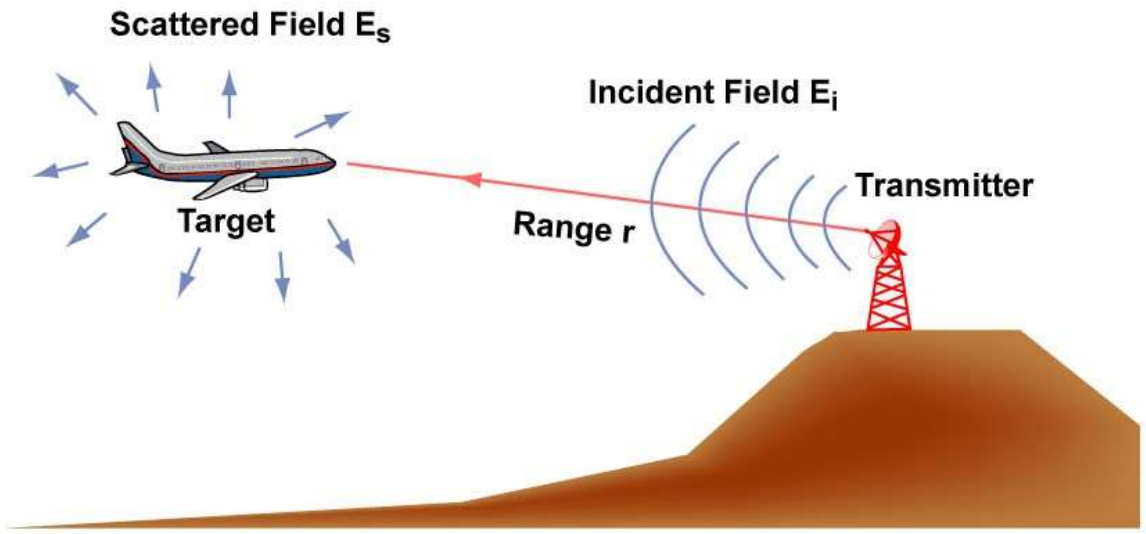
Radar Cross Section (RCS)



Radar Cross Section (RCS, or s) is the *effective* cross-sectional area of the target as seen by the radar

measured in m^2, or dBm^2

Definition of Radar Cross Section (RCS or σ)

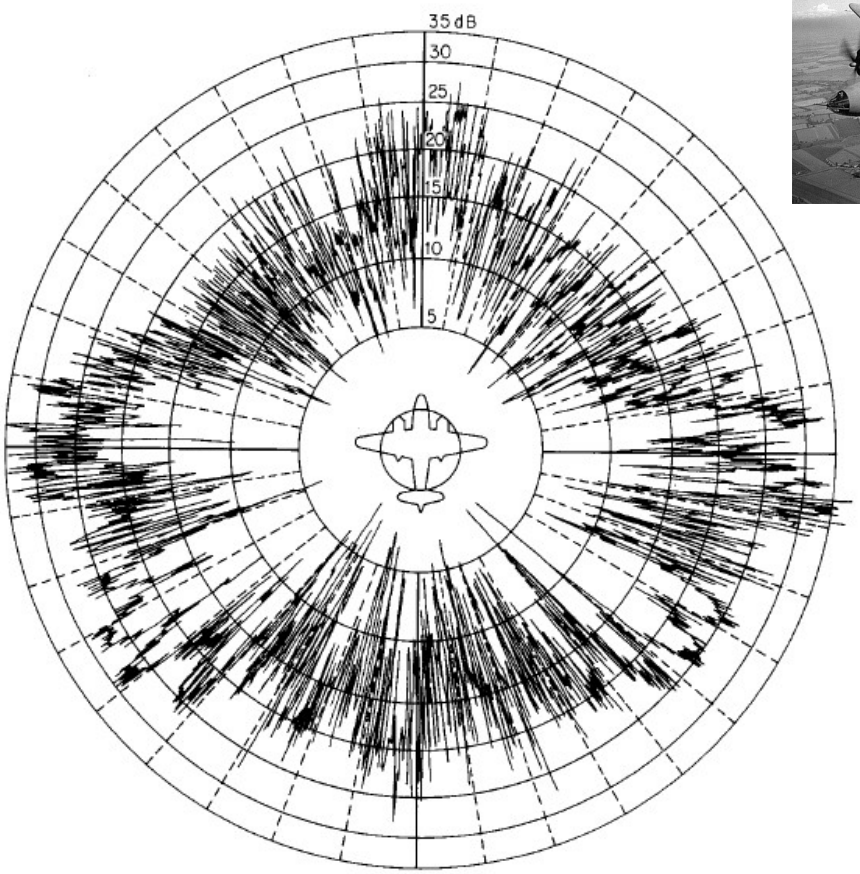


$$\text{RCS} = \lim_{r \to \infty} 4\pi r^2 \frac{|E_s|^2}{|E_i|^2} \quad \text{(Unit: Area)}$$

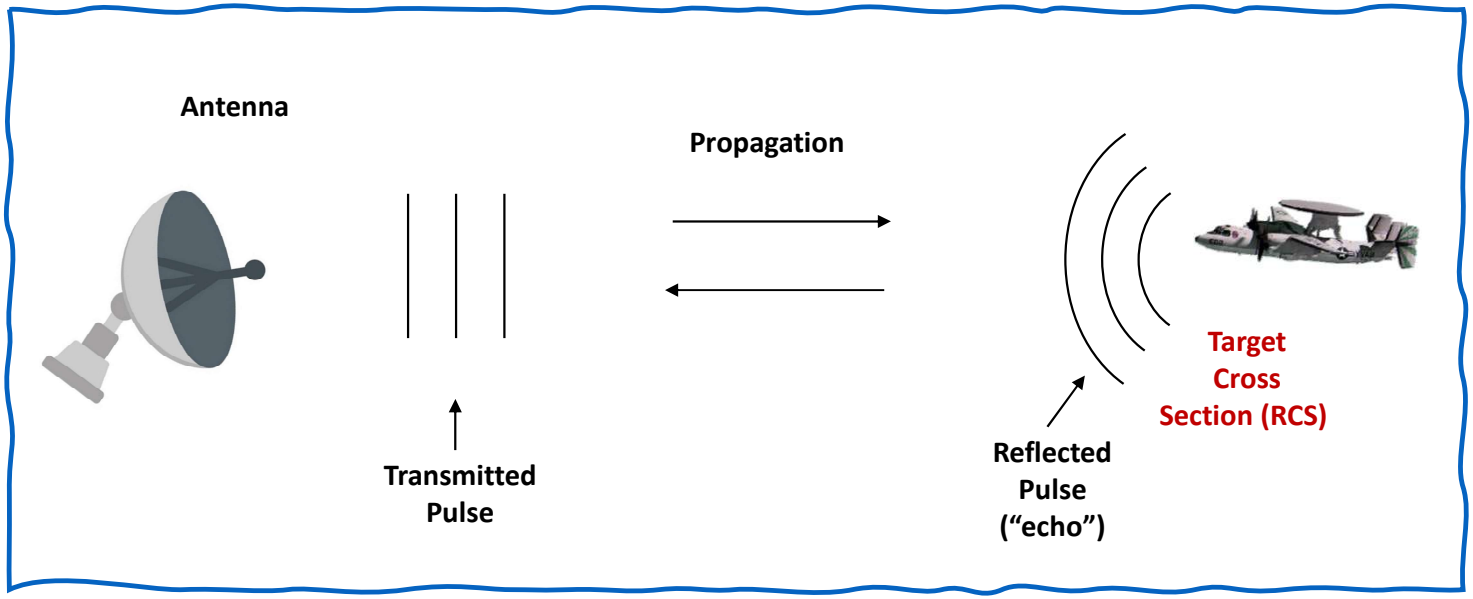
Figure by MIT OCW.

Radar Cross Section is the area intercepting that amount of power which, if radiated isotropically, produces the same received power in the radar.

Radar Cross Section of B-26 Bomber



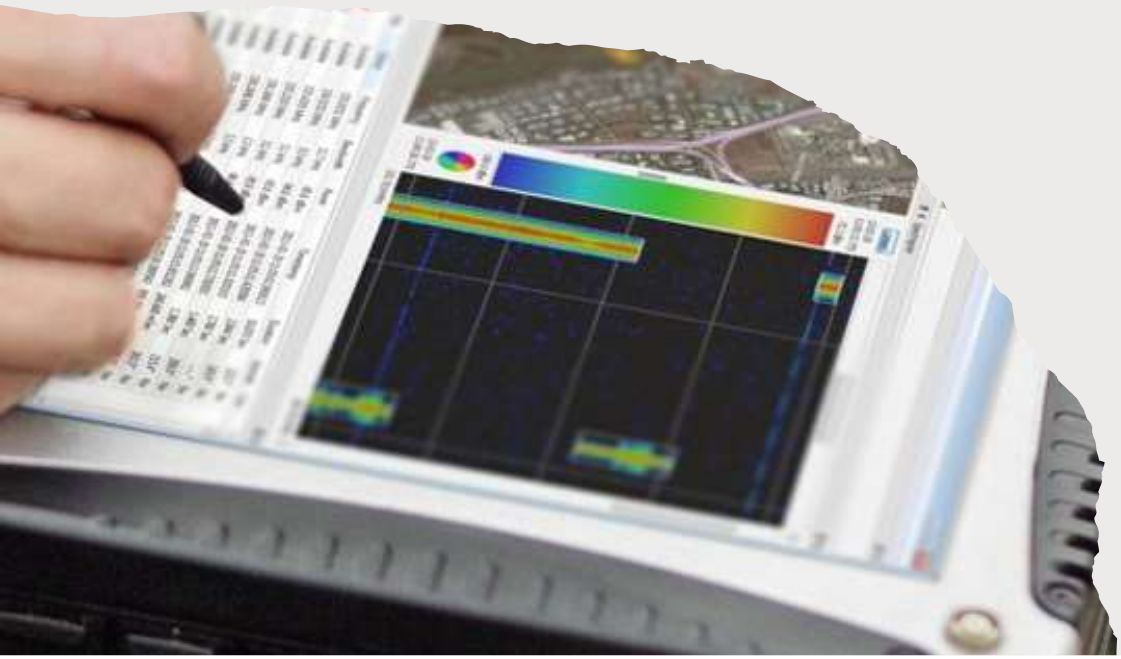
RADAR
RAdio Detection And Ranging



Radar observables:

- Target range
- Target angles (azimuth & elevation)
- Target size (radar cross section)
- Target speed (Doppler)
- Target features (imaging)

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.

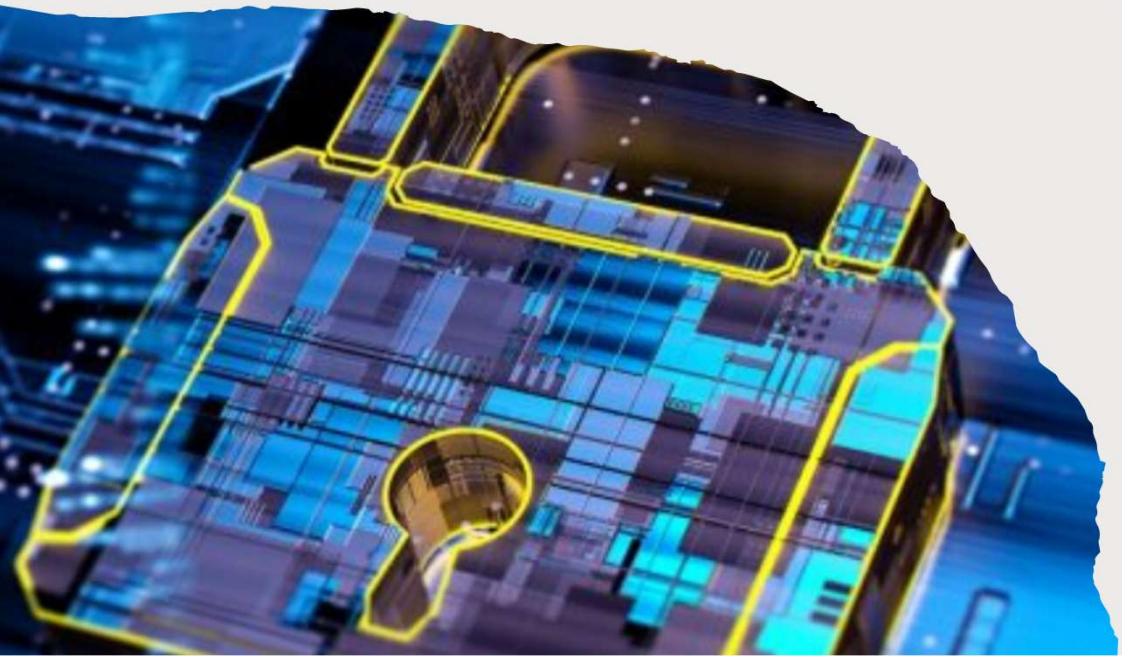
- SIGINT system combines precision RF, SDR and Direction Finding (DF) hardware with the next generation of the software.

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 Analysis



- 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)

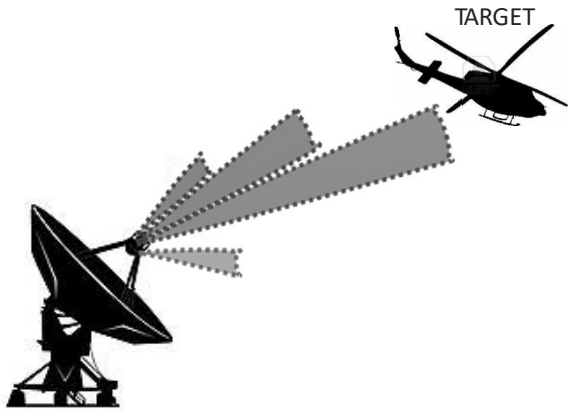
- DSP/FPGA for electronic intelligence
-
- Developing electronic intelligence systems using signal processing hardware: FPGA, DSP and I/O modules
- Mix FPGA with DSP processors, and to integrate that processing power with very fast communications ADCs, capable of sampling IF signals directly
- Most modern 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.



Operational ELINT

OPERATIONAL ELINT AIMS AT DELIVERING INTELLIGENCE USEFUL FOR MILITARY OPERATIONS. THE TIMELINESS OF THIS INTELLIGENCE IS CRITICAL.

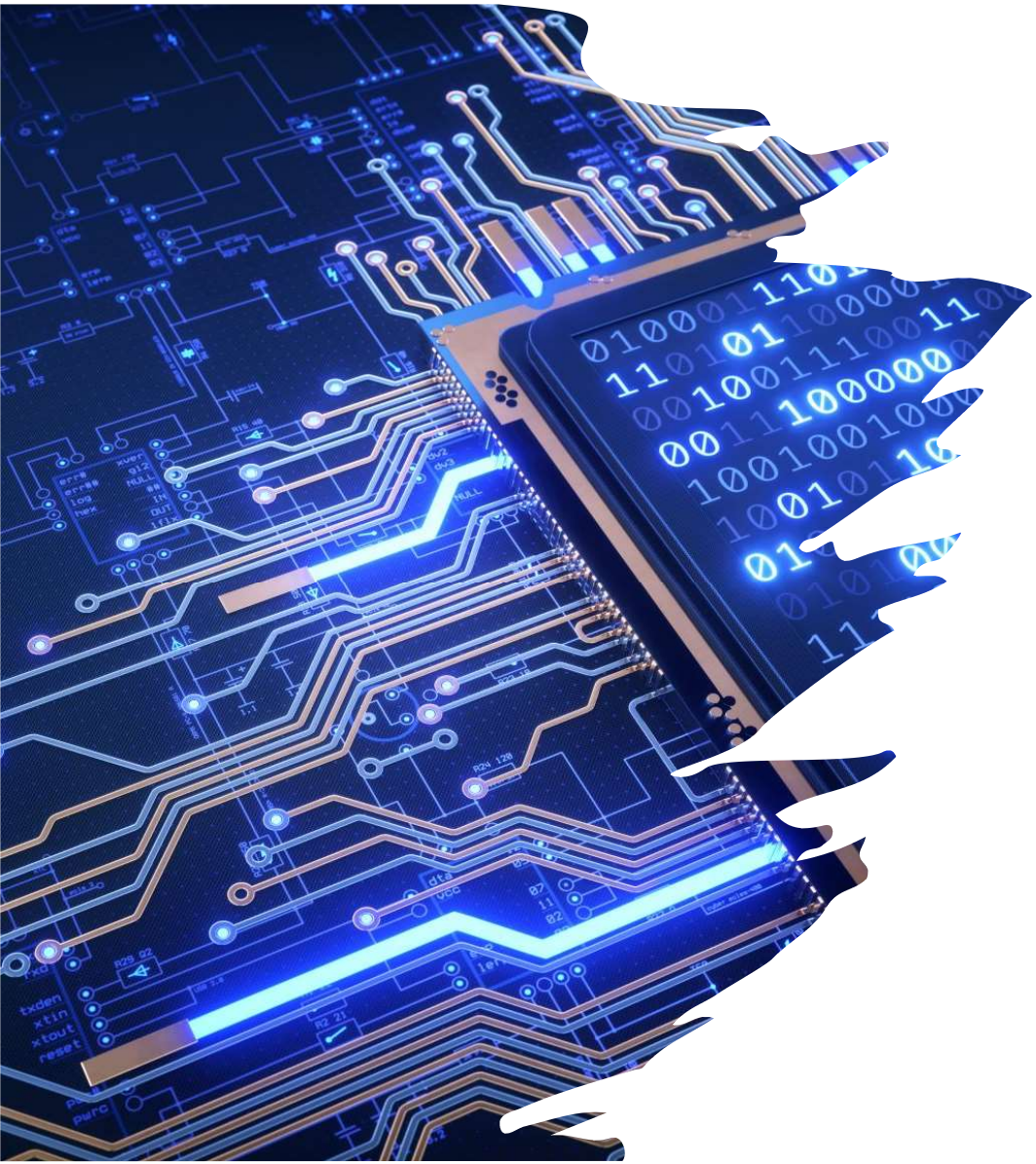
FOR INSTANCE, OPERATIONAL ELINT WOULD FOCUS ON DETECTING WHAT RADARS ARE IN A REGION, AND WHERE THEY ARE, INSTEAD OF LOOKING IN DETAIL INTO THEIR SIGNALS

Example of SIGINT Capabilities

Ground SIGINT Elements

Air-Platform SIGINT Elements

Ship-Based SIGINT Element



Signals intelligence operational platforms

- Signals intelligence operational platforms are employed by nations to collect signals intelligence, which is intelligence-gathering by interception of signals, whether between people (i.e., COMINT or communications intelligence) or between machines (i.e., ELINT or electronic intelligence), or mixtures of the two.

- As sensitive information is often encrypted, signals intelligence often involves the use of cryptanalysis.

Ground platforms

Strategic ground platforms
Tactical ground platforms

Ship platforms

Submarine platforms

Aircraft platforms

Tactical aircraft platforms
Strategic aircraft platforms

Satellite platforms

SIGINT Organizations and Groups

- Radio Battalion provides tactical SIGINT, electronic warfare, communications security monitoring and analysis, and special communications.

- Tactical Electronic Warfare Squadron conducts tactical electronic reconnaissance and ELINT operations including:

    - ELINT collection operations to maintain the electronic order of battle, including identification of selected emitters and location o nonfriendly emitters.

    - Threat warnings for friendly aircraft, ships, and ground units. Intelligence support to prevent, delay, or interrupt detection and tracking by enemy early warning, acquisition, and fire or missile control radars of aviation combat element (ACE) operations or tactical jamming aircraft in support of strike aircraft.

Roles and Responsibilities

- Collecting, analyzing, processing, and reporting communications intelligence (COMINT).
- Performing direction finding (DF) and advanced identification techniques.
- Managing the tasking and positioning of organic SIGINT mission equipment.
- Providing electronic intelligence (ELINT) processing, analyzing, and reporting.
- Developing and maintaining SIGINT data bases SIGINT units deployed, or which may be deployed, in the theater of operations.

Planning and Operations

- SIGINT Functional Planning
- SIGINT Operational Planning

SIGINT Functional Planning

- SIGINT Concept of Operations
- Enemy Characteristics
- Topography
- Planning Responsibilities
- Coordination of SIGINT Operations

SIGINT Operational Planning

- Planning and Direction
- Collection
- Processing and Exploitation
- Production
- Dissemination
- Utilization

The Intelligence Cycle

- The intelligence cycle is the process through which intelligence is obtained, produced, and made available to users.
- In depicting this cycle, the United States Intelligence Community uses a five-step process.
- Other nations may describe this cycle differently; however, the process is largely the same.

The Steps in the Intelligence Cycle

PLANNING AND DIRECTION

COLLECTION

PROCESSING

PRODUCTION

DISSEMINATION

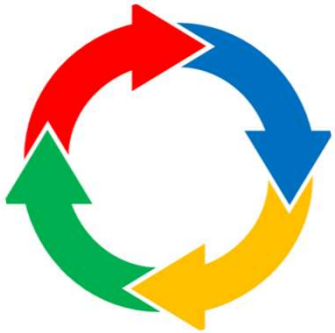
The Steps in the Intelligence Cycle

1.) PLANNING AND DIRECTION

- When tasked with a specific job, the planning begins on what to do and how. The team will list what is known about the issue and what they need to find out. Also, they discuss ways to gather the necessary intelligence.

2.) COLLECTION

- Information is overtly (openly) and covertly (secretly) collected. Reading foreign newspapers and magazine articles, listening to foreign radio, and watching overseas television broadcasts are examples of "overt" (or open) sources. Alternatively, covert sources can include information collected with listening devices and hidden cameras.



3.) PROCESSING

- All the information is collected is cataloged, organized, and made accessible to analysts. This information could be anything from a translated document to a description of a satellite photo.

4.) ANALYSIS AND PRODUCTION

- During this step, a closer look at all the information is taken. Analysts determine how it fits together, while concentrating on answering the original task. They assess what is happening, why it is happening, what might occur next.

5.) DISSEMINATION

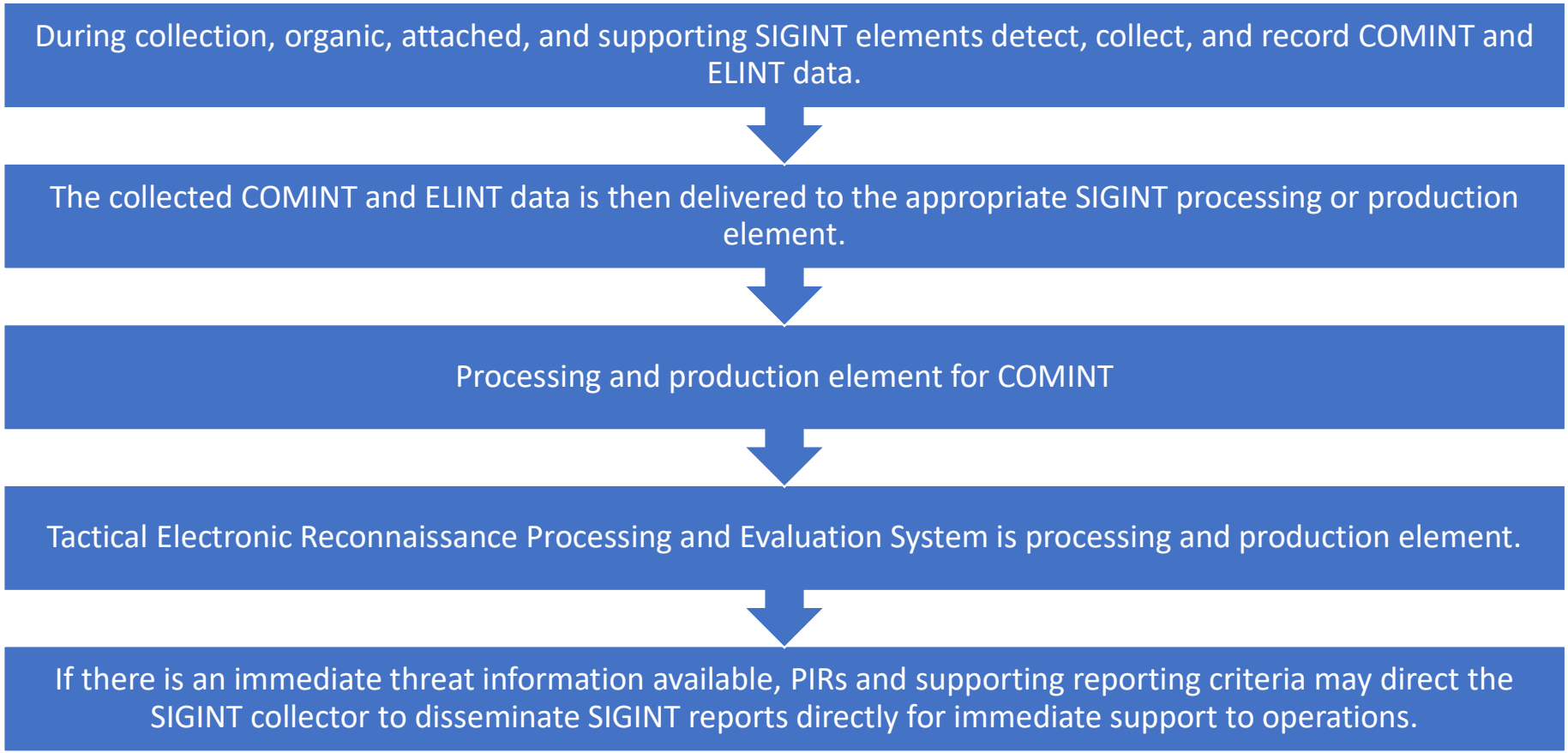
- The final written analysis is provided to the stakeholder. After reading the final analysis and learning the answer to the original question, the stakeholder may come back with more questions.

Planning and Direction

- SIGINT direction is a continuous process that encompasses the tactical and technical employment of SIGINT assets.
- It begins on receipt of a warning order, initiating directive, or establishment of a planning objective and continues until termination of the mission.
- SIGINT unit commanders closely coordinate their operations with the intelligence group and pertinent external intelligence and SIGINT elements.

- Planning and direction involves
  - Determining priority intelligence requirement (PIR), and intelligence requirement (IR), and SIGINT requirements to support them.
  - Preparing supporting SIGINT collection, production, and dissemination plans. Issuing orders and requests to SIGINT units.
  - Checking continuously on the productivity and effectiveness of SIGINT collectors, producers, disseminators, and other SIGINT elements and agencies.

Collection


During collection, organic, attached, and supporting SIGINT elements detect, collect, and record COMINT and ELINT data.
The collected COMINT and ELINT data is then delivered to the appropriate SIGINT processing or production element.
Processing and production element for COMINT
Tactical Electronic Reconnaissance Processing and Evaluation System is processing and production element.
If there is an immediate threat information available, PIRs and supporting reporting criteria may direct the SIGINT collector to disseminate SIGINT reports directly for immediate support to operations.

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.

Production

- The production stage involves converting the SIGINT analysis into appropriately tailored SIGINT reports and all-source intelligence product that can be easily understood by the commander and other users.

- Specifically formatted standardized messages, graphics, and other intelligence products are required to familiarize these user with layout and content and to ensure rapid usage and automated processing of finished reports.

Dissemination

- Dissemination is the process through which SIGINT products are delivered to users
- Example:
  - Commander, subordinate commanders and their staffs, and others as appropriate
  - Joint force commander
  - Joint components, and various theater and national organizations and intelligence agencies.
- SIGINT products are disseminated via dedicated SIGINT or general-purpose channels according to available resources, the classification of the product, and the intelligence dissemination plan.
- These products include time-sensitive voice reports, text reports, videos, data base updates, and web-based resources.

- Several intelligence disciplines are used by adversaries to acquire information concerning the United States.

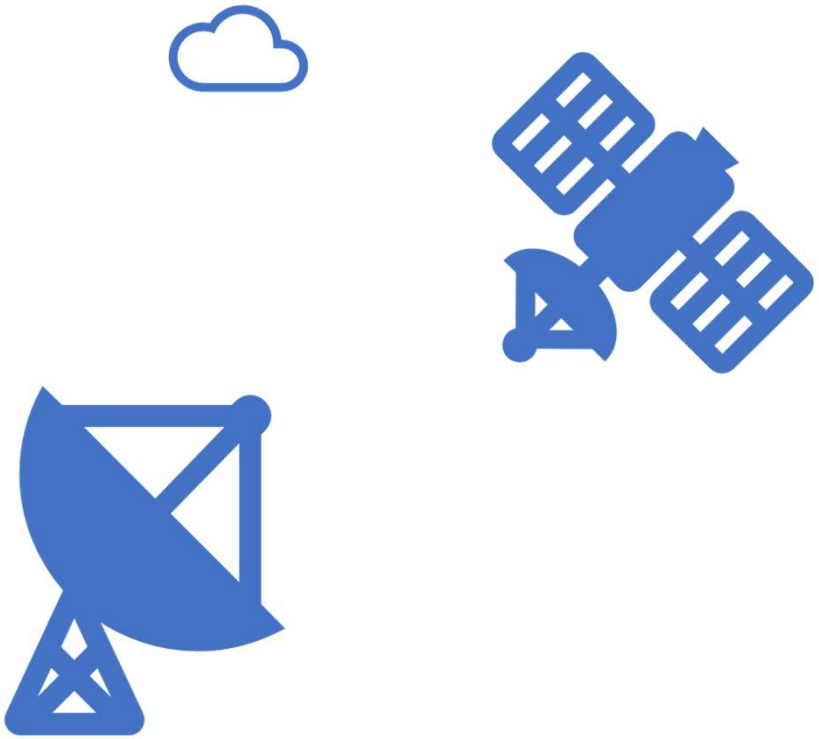
- These disciplines include human intelligence HUMINT), signals intelligence (SIGINT), imagery intelligence (IMINT), measurement and signatures intelligence (MASINT), and open-source intelligence (OSINT).

- Each of these disciplines is used by adversaries to some degree.

- Most nations, and many subnational and private organizations, have HUMINT capabilities that they use to collect data on their adversaries and competitors.

SIGINT Technologies

- Signals intelligence is derived from signal intercepts comprising, either individually or in combination, all communications intelligence (COMINT), electronic intelligence (ELINT), and foreign instrumentation signals intelligence (FISINT), however transmitted.

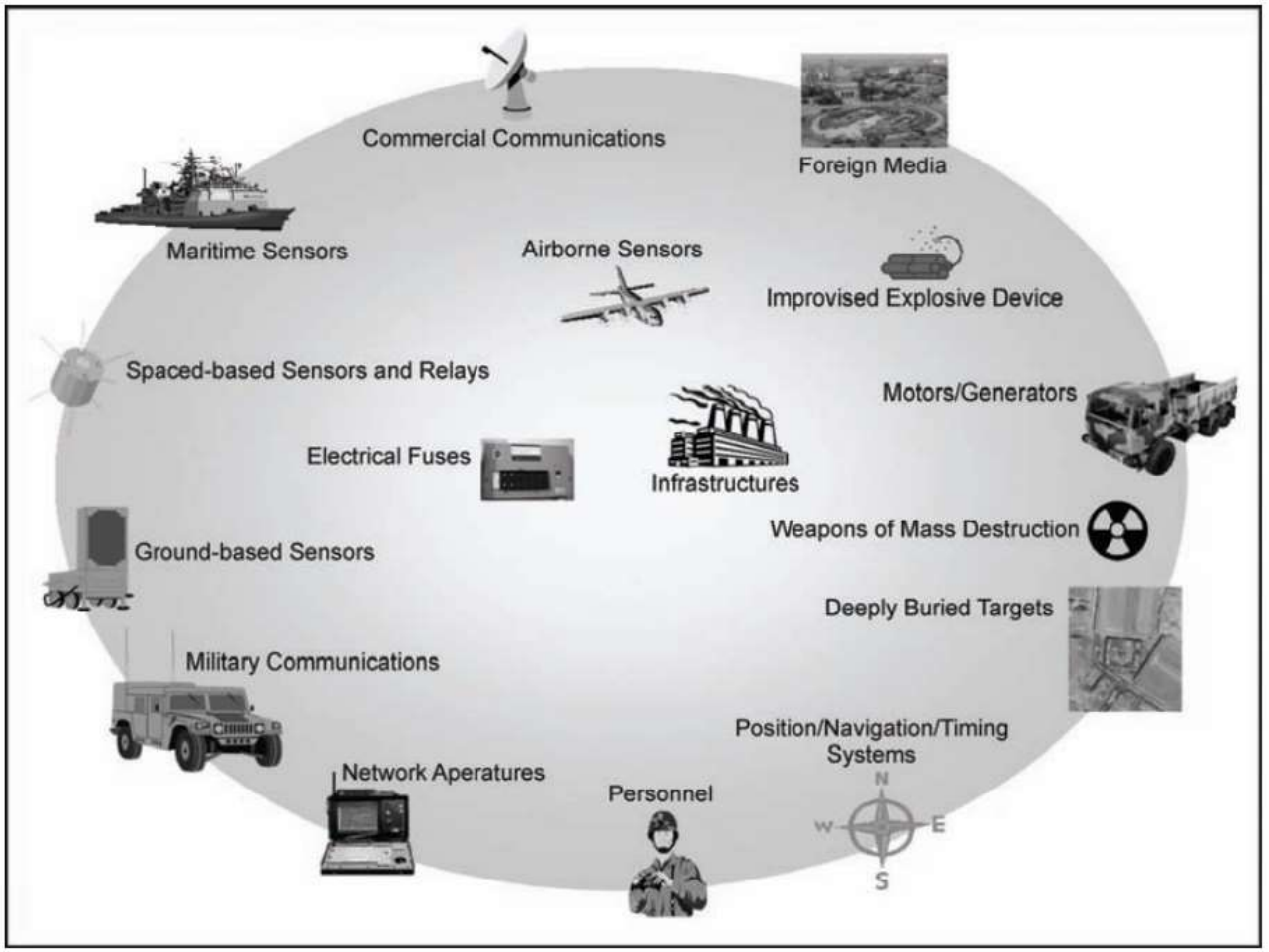


COMMUNICATIONS
INTELLIGENCE (COMINT)

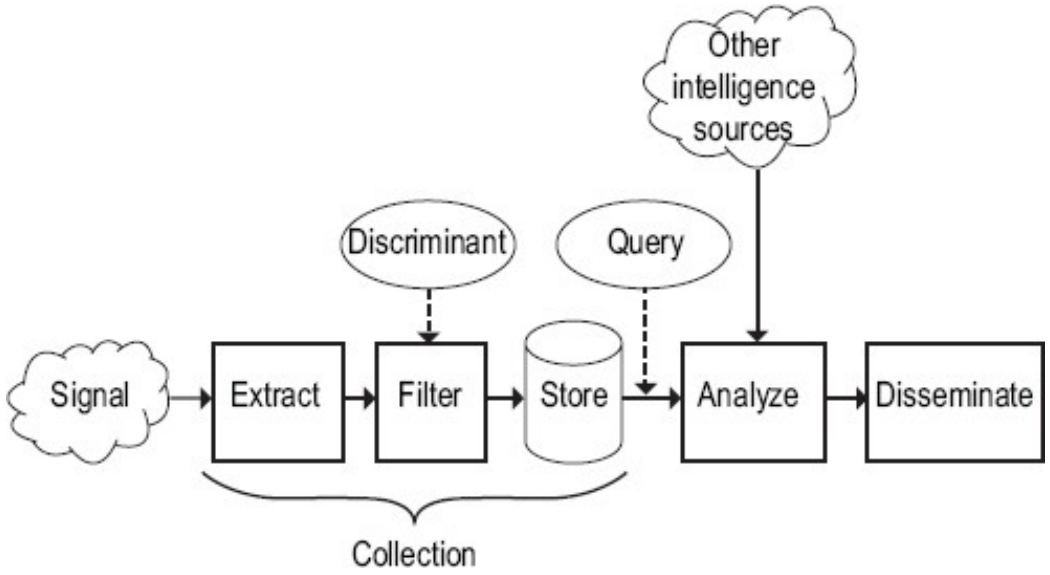
ELECTRONIC
INTELLIGENCE (ELLNT)

FOREIGN SIGNALS
INTELLIGENCE (FISINT)

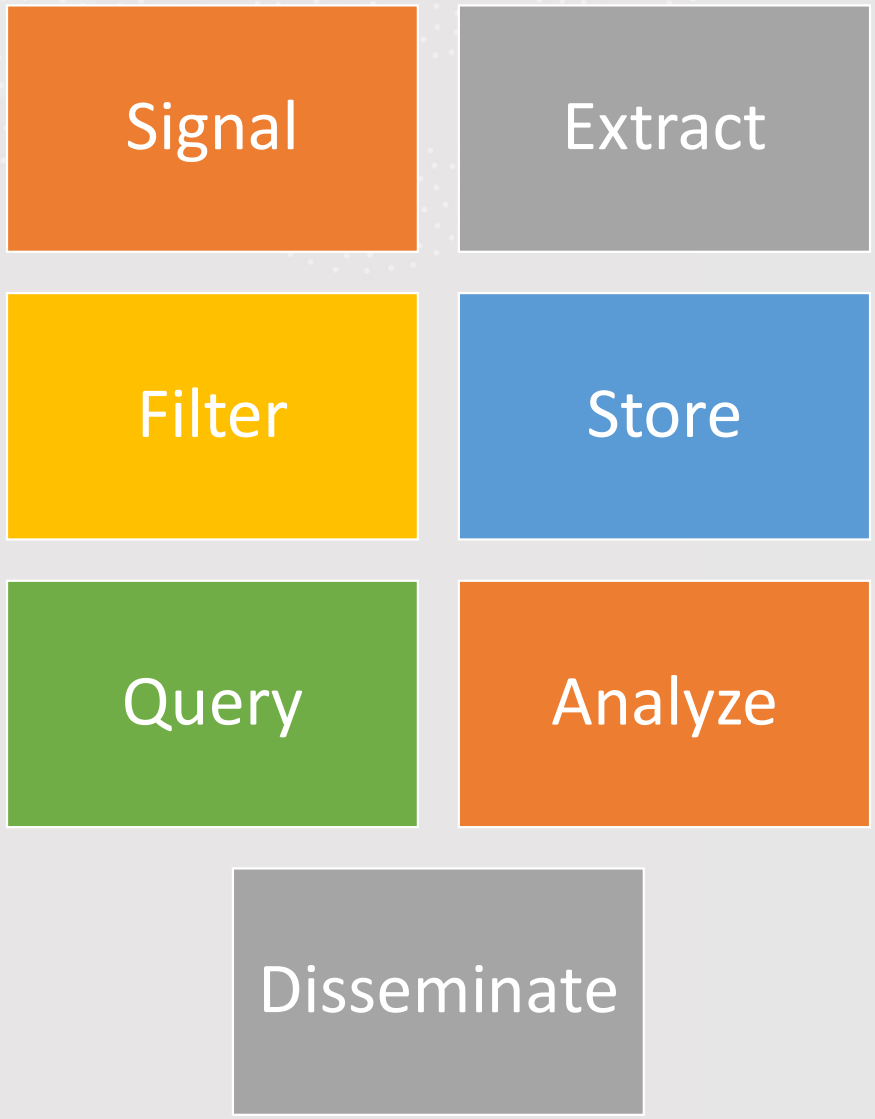
Electromagnetic Spectrum Targets



A Conceptual Model of Signals Intelligence



Elements of Signals Intelligence



Traditional SIGINT

- *Extract*. The first step is to obtain the signal from a source, convert it into a digital stream, and parse the stream to extract the kind of information being sought, such as an email message or the digital audio of a telephone call. Extraction interprets layers of communications and Internet protocols, such as Optical Transport Network (OTN), Synchronous Digital Hierarchy (SDH), Ethernet, Internet Protocol (IP), Transmission Control Protocol (TCP), Simple Mail Transport Protocol (SMTP), or Hypertext Transport Protocol (HTTP). In cases where business records are sought, this step extracts and reformats relevant SIGINT data from a business record format used by the business.

- *Filter*. This step selects, from all the items extracted, items of interest that should be retained. It is sometimes controlled by a "discriminant," which the IC agency running the collection provides to describe in precise terms the properties of an item that should be retained.

- *Store*. Retained items are stored in a database operated by the U.S. government. This is the point at which collection is deemed in this model to occur for the retained data. By contrast, the previous steps are fleeting, with data processed in near real-time (keeping data only for short periods of time—minutes to hours—for technical reasons) as fast as it is supplied, with all but the items to be retained discarded. Items collected from separate sources are usually combined into a modest number of large databases to facilitate searching and analysis.

Modern SIGINT

- In modern communication systems, traffic from many sources and destinations is aggregated into a single channel. For example, the radio signals to and from a base station serving all cell phones in a cell are all on the same radio channels, and all the IP packets between two routers may be carried on the same fiber.

- With rare exceptions, there is no single physical access point comparable to the central office connection of a landline telephone at which to observe only the items of interest and nothing more.

- Reflecting this reality, the committee's definition of "collection" says that SIGINT data is collected only when it is stored, *not* when it is extracted. Put another way, every piece of data that passes by a potential monitoring point must be machine-filtered as part of the extraction process to determine whether it is potentially relevant or can be thrown away without further examination.

Hypothetical Call Detail Records as They Might Appear in a Signals Intelligence Database

Caller	Called	Call Start Time	Call Duration
+1-617-555-0131	+1-703-555-0198	2020:10:3:15:45:10	3:41
+1-703-555-0198	+1-703-555-0013	2020:10:3:15:49:10	1:10
+1-415-555-0103	+963 99 2210403	2020:10:3:16:01:43	73:43
+1-603-555-0141	+1-603-555-0152	2020:10:3:22:10:03	3:01
+1-617-555-0183	+1-413-555-0137	2020:10:3:22:33:48	7:03
+1-802-555-0141	+1-802-555-0108	2020:10:3:22:41:17	3:02

Dissemination

- The last step in the SIGINT process is dissemination. SIGINT analysts will routinely disseminate the results of their work to others, both inside and outside the IC. For example, NSA analysts working on a specific terrorism investigation might disseminate their findings to other analysts and collectors who are working on related issues or directly to policy makers who may choose to take action based on the SIGINT.

- Like the initial collection, SIGINT dissemination is governed by various laws and regulations designed to protect the sources and methods involved in the collection as well as the privacy and civil liberties of the subjects of the collection, especially if the intelligence involves U.S. persons.5 Specifically to the latter, and pursuant to U.S. Signals Intelligence Directive (USSID) 18,6 such reports will normally cloak the identity of U.S. persons until a reader of the report specifically asks for the identity to be disclosed and provides a valid reason for the release, such as initiating a further investigation.
- This process is designed to ensure that both the requesting agency and NSA, as the disseminator of the information, can verify that disclosing this sensitive information is appropriate and necessary to understand the foreign intelligence value of the report.

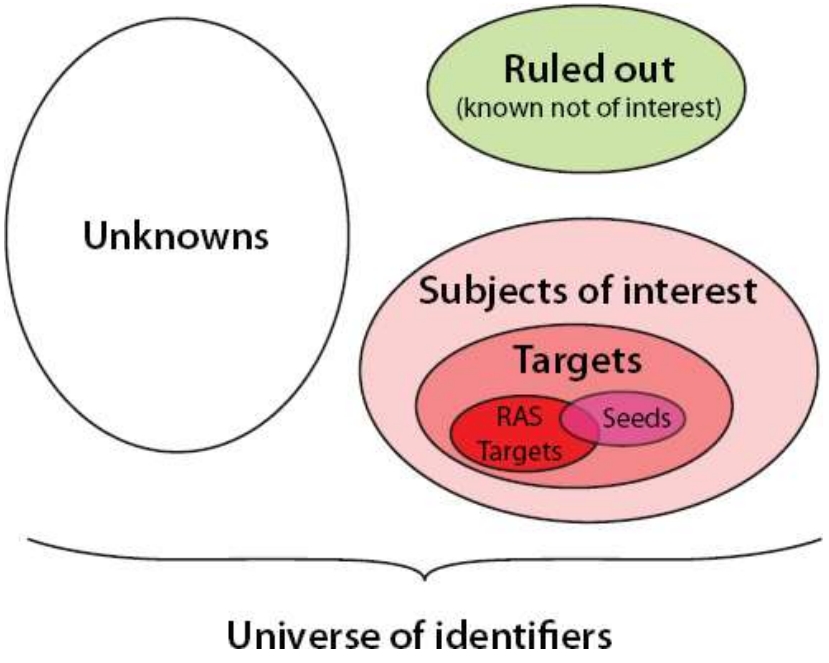
Classification of identifiers used in signals intelligence analysis

• *Subject of interest*: An identifier that may have intelligence value and is likely to be part of an intelligence investigation.

• *Target*: A subject of interest that may be a security threat.

• *Seed*: A subject of interest that is used as the starting point for an intelligence investigation.

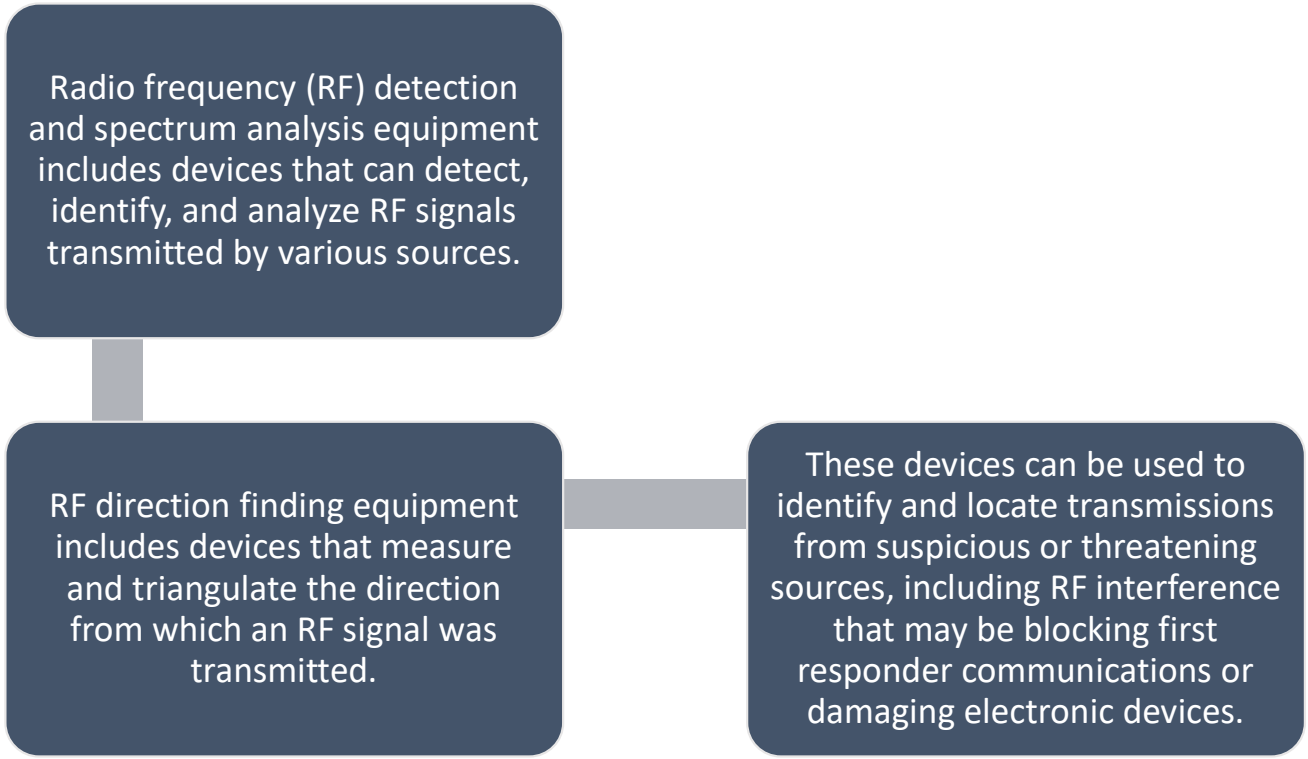
• RAS *target*: A target for which there is a reasonable and articulable suspicion that the person is associated with a foreign terrorist organization (RAS=reasonable, articulable suspicion)



Working Definitions in Signals Intelligence and Technology

identifier	A text or bit string that denotes a communication endpoint, such as a telephone number, mobile phone subscriber number, Internet Protocol (IP) address, or email address.
subject of interest	An identifier of a party (person, group) that may have intelligence value and is likely to be part of an intelligence investigation.
target (n, adj)	A subject of interest in an intelligence investigation. This term is used liberally by the Intelligence Community (IC) to denote an identifier or person that is the subject of interest or surveillance. A target need not be the principal subject of interest. For example, an associate of a known threat might be a target. Note that a target can be a computer identified by its IP address. Target identifiers may be used in selectors or discriminants to obtain, from a large collection of data, data pertaining only to the target.
seed (target)	An initial target used to start an intelligence investigation.
RAS target	A target for which there is a reasonable, articulable suspicion (RAS) that it is associated with a foreign terrorist organization. Foreign Intelligence Surveillance Act Section 215 requires a RAS target designation to permit certain queries.
query	Detailed instructions for searching a database of collected data. Note: this is consistent with computer technology usage, and is akin to an SQL query. A query may have several “terms” or “selectors”: Example: “calls made from identifier x000325 after July 2, 2013” Example: “Internet search requests using the term ‘sarin’ or emails containing ‘poison gas’
discriminant	Same meaning as query, but used in conjunction with filtering applied as part of collection. Discriminants must be simple enough to be applied in real time as signals intelligence (SIGINT) data is extracted and filtered. This word appears explicitly in Presidential Policy Directive 28 (PPD-28) as part of the definition of “targeted collection.” Example: “all the email addresses used in communications to or from Yemen”

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

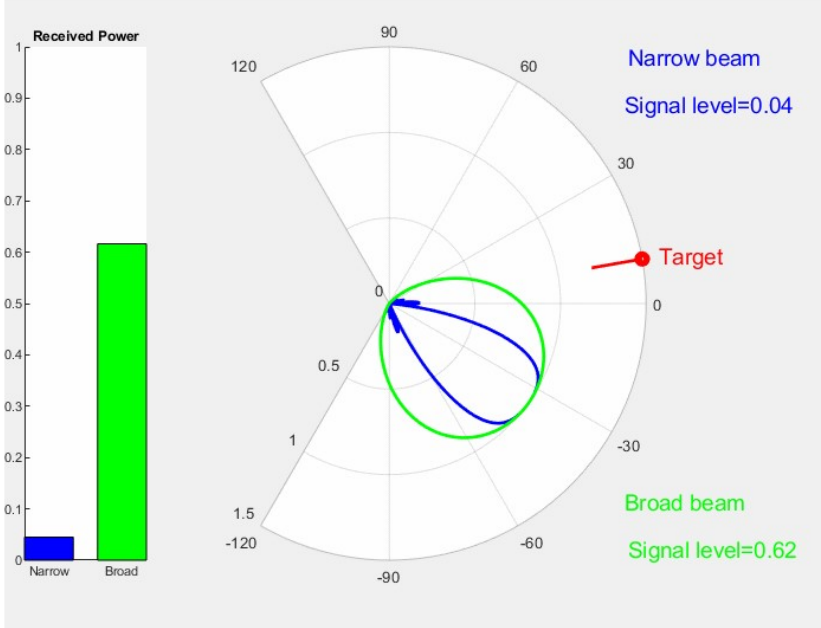
- RF direction finding is used in several applications:
  - SIGINT: such as the direction of a threat, the location and movement of enemy transmitters and the direction of enemy jammers.
  - Radio monitoring: the location of sources of interference and of illicit transmitters
  - Search and Rescue: the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

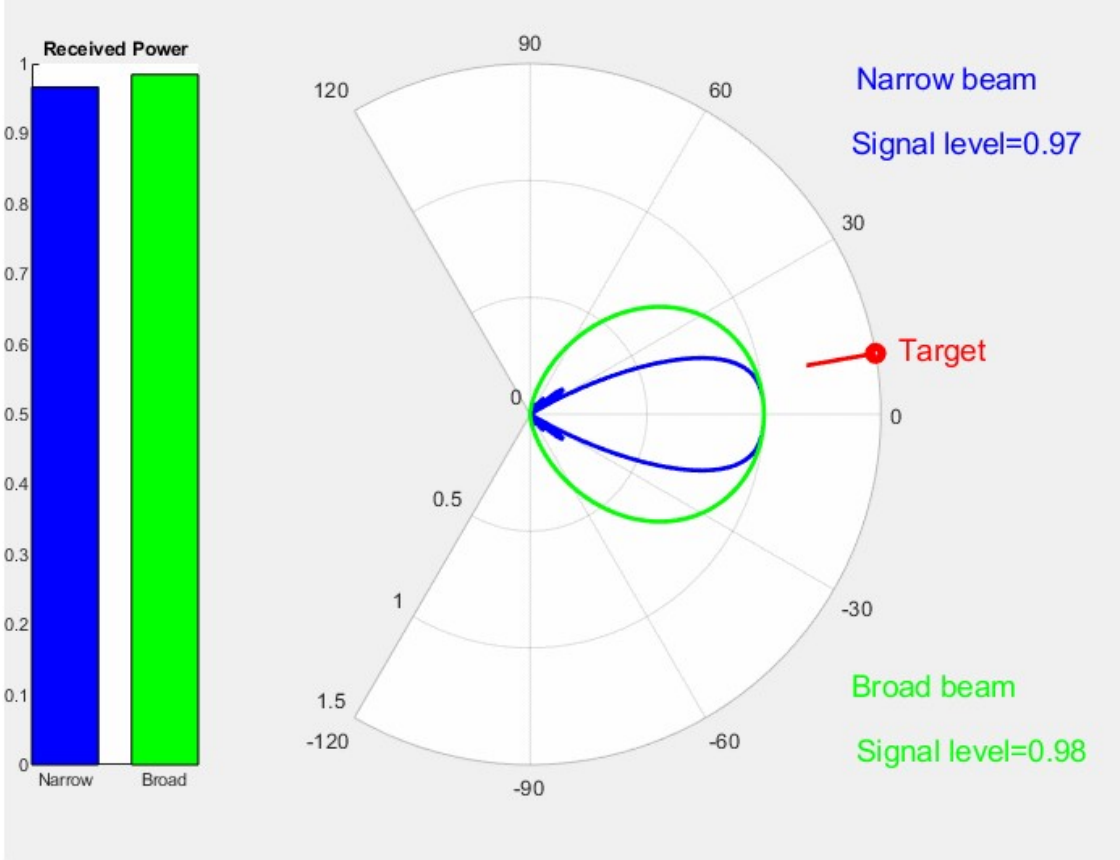
Single Receiver DF Systems: Directional Antenna Technique

- 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.

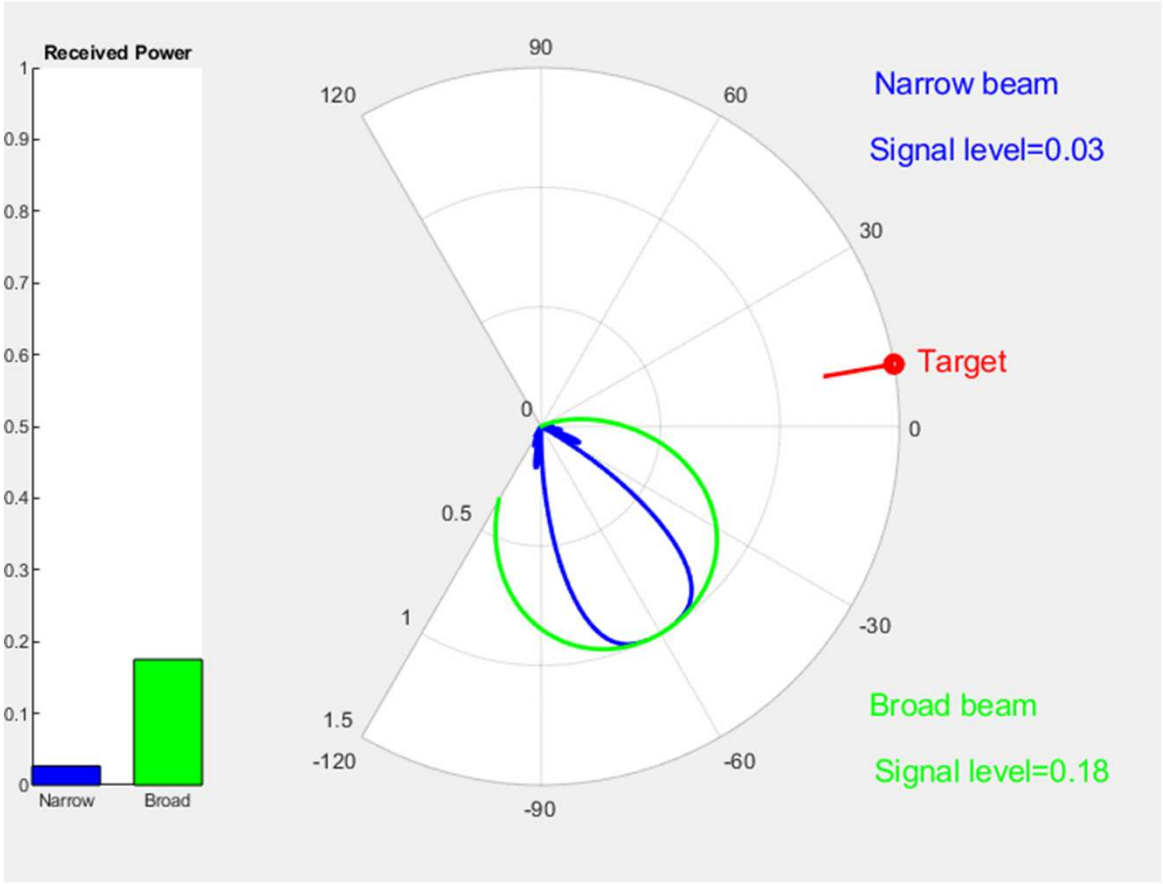
- In SIGINT applications is commonly used for broad band high frequency DF. These systems are fully motorized and use knowledge of the antenna radiation pattern to improve accuracy.

Directional Antenna Technique





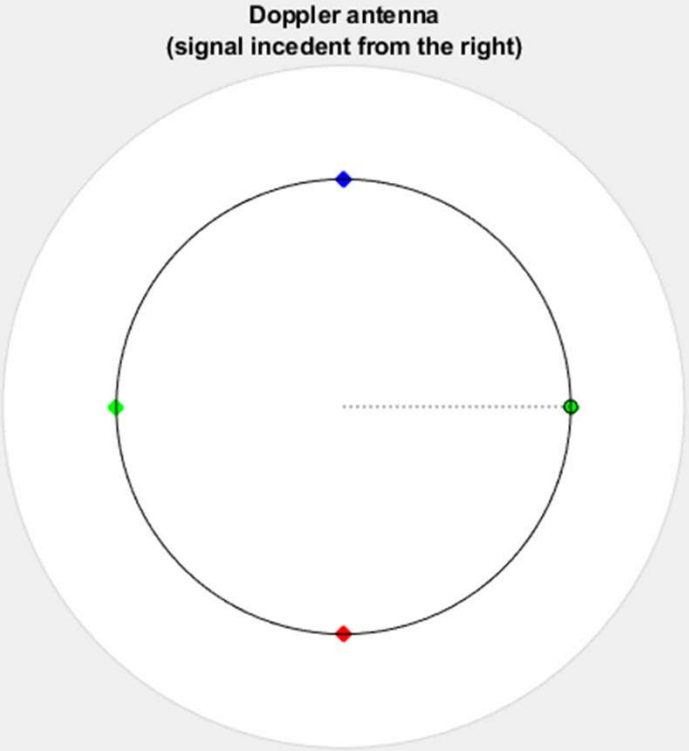
Directional Antenna Technique



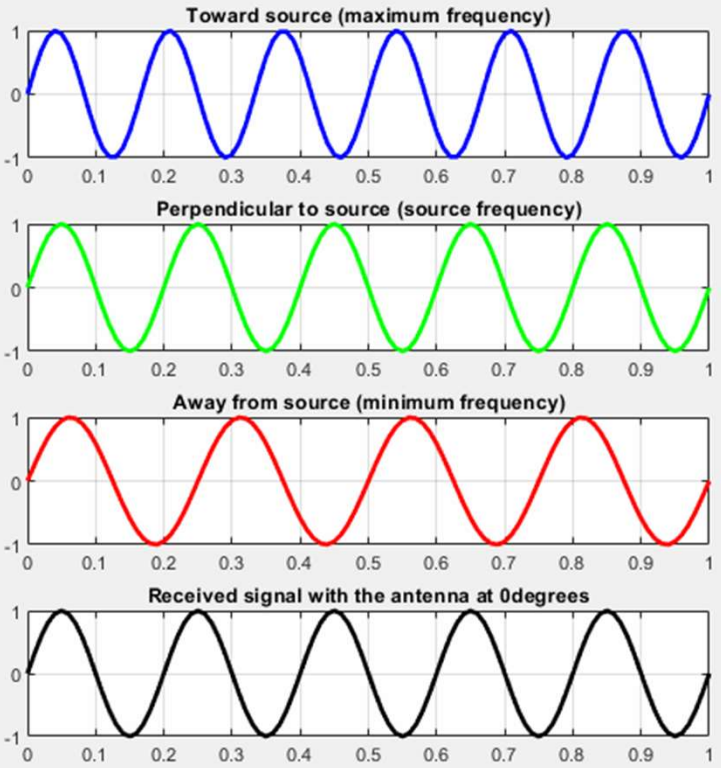
Doppler and Pseudo-Doppler Technique

- 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.

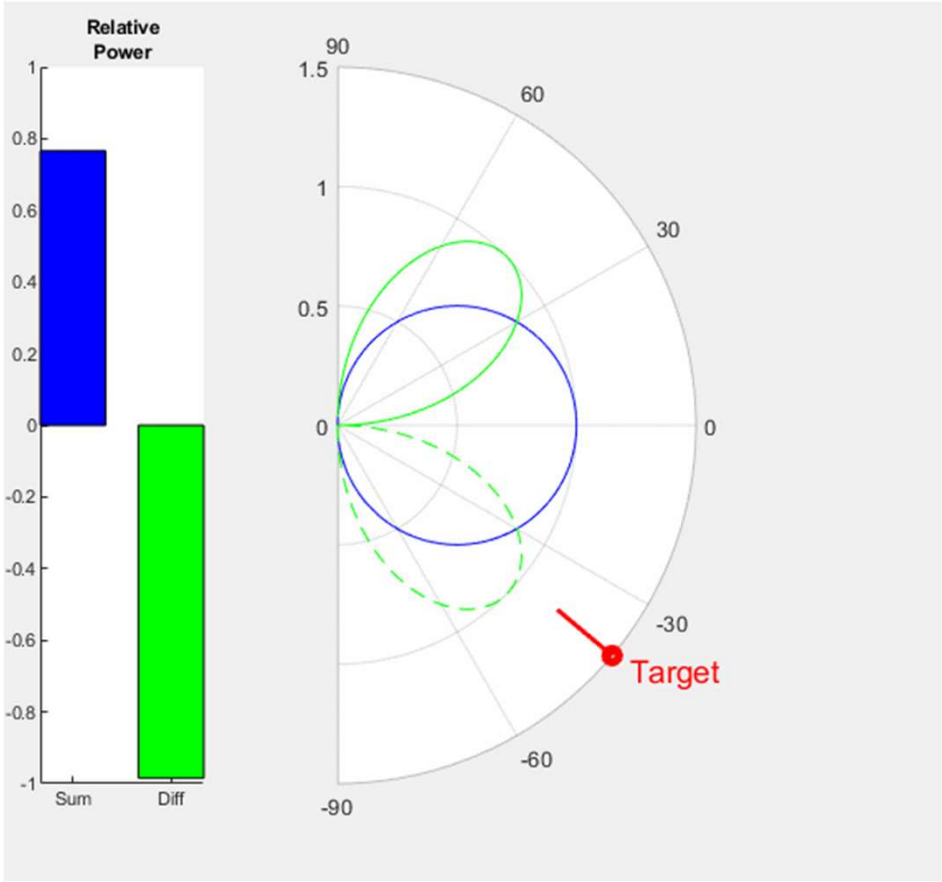


The received frequency at various positions along the trajectory of the antenna is shown in the right image of the figure. As the antenna moves away from the incident signal, the frequency increases (red graph) and as the antenna moves towards the incident signal, the frequency increases (blue graph). 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.

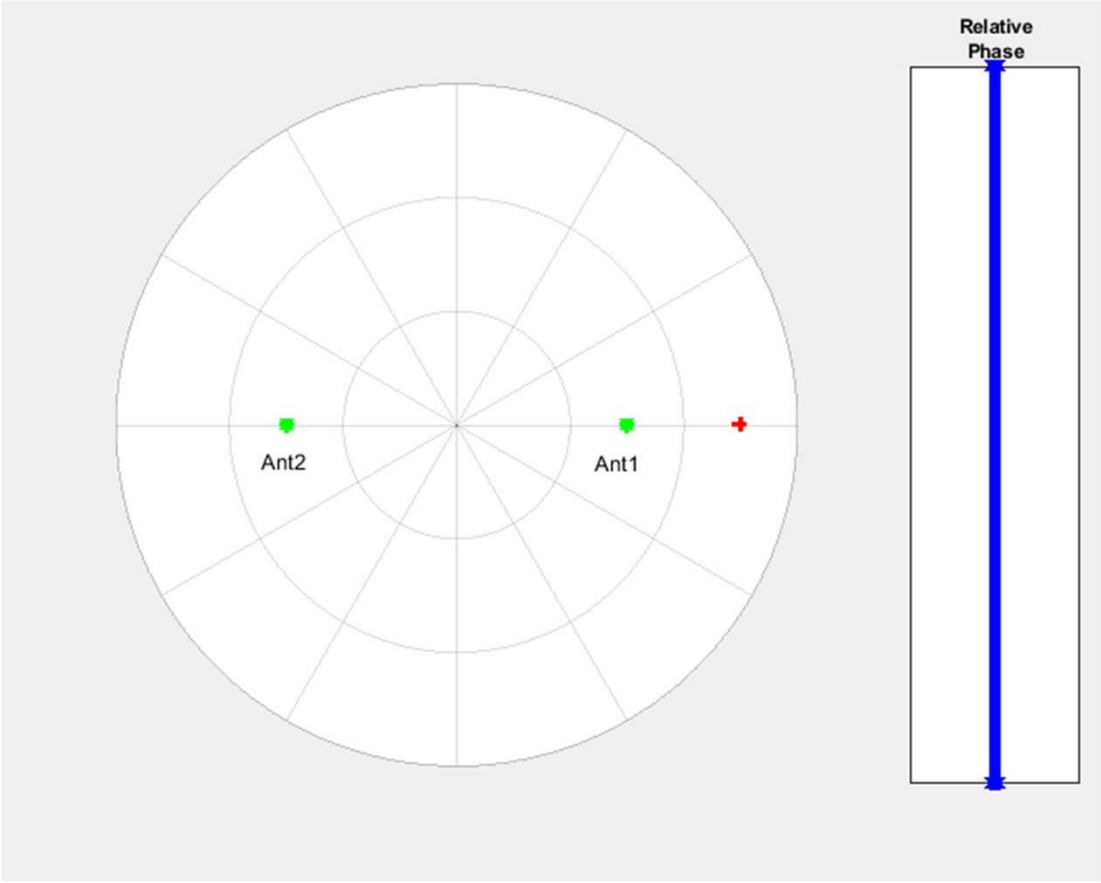
Two Receiver Systems: Mono-pulse Technique



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

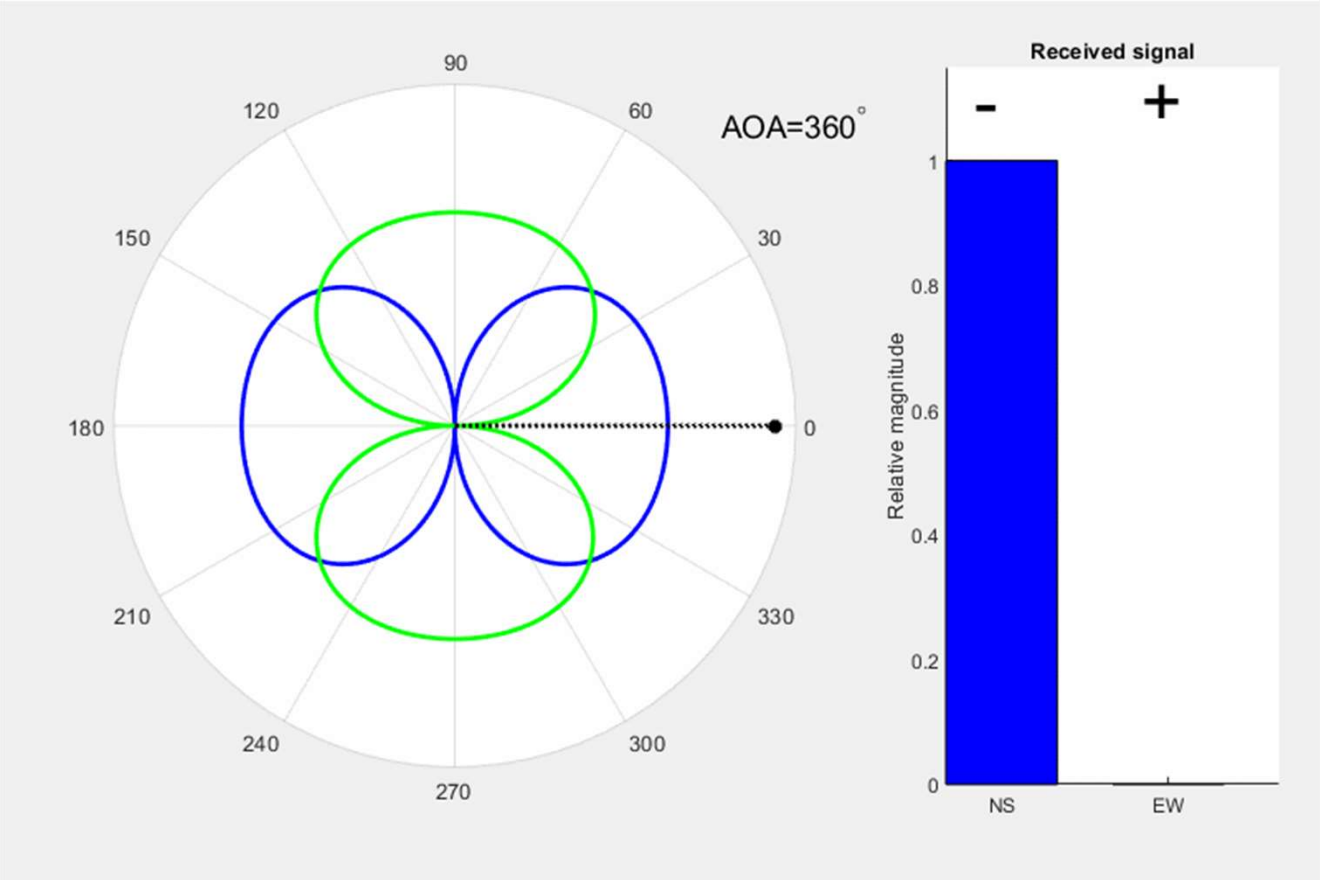
- An Adcock antenna uses two crossed loop antennas.
- The bearing of the RF signal is determined using the level of the signals received at each antenna.
- The method to process the information from a Adcock array is referred to as Watson-Watt.
- This is the best-known method of radio direction finding.

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.

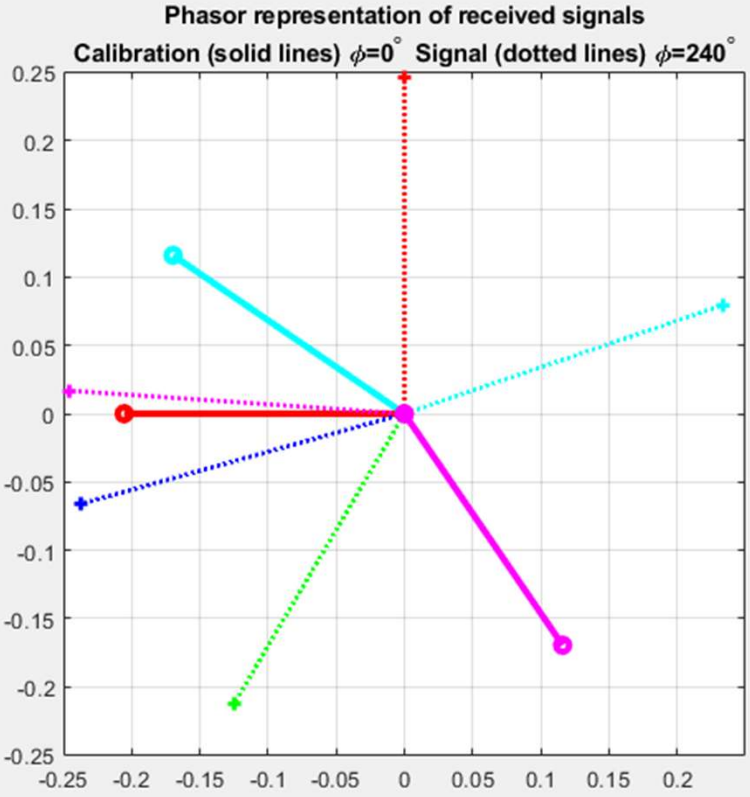
The correction function correlates the relative phases (and magnitudes for some correlators) of the received signals with the correlation table over all possible angles; the maximum of the correlation function indicates the AOA.

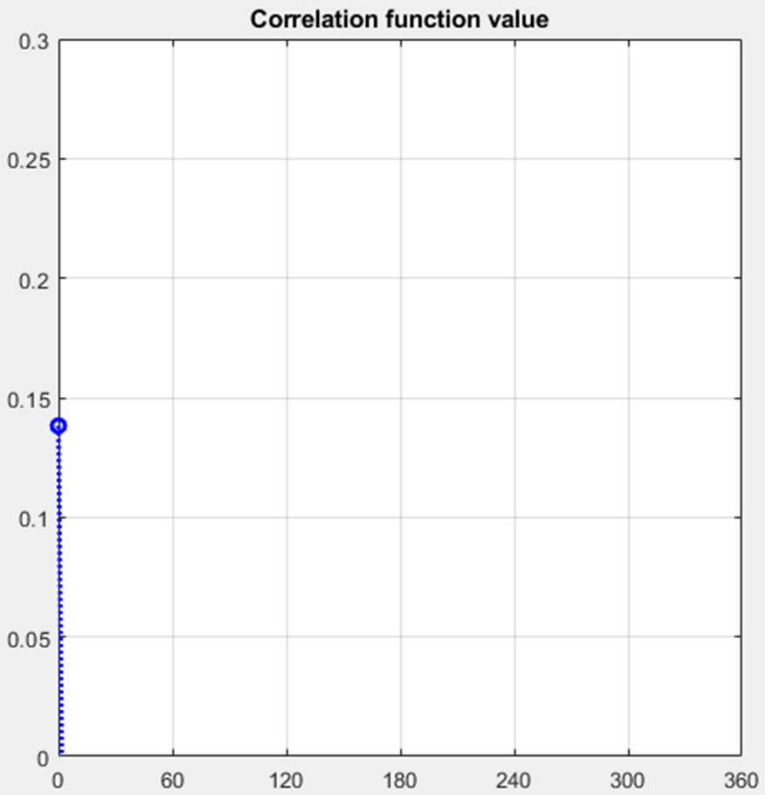
The calibration information can be obtained by calculation or by measurement of the antenna.

Correlative Array

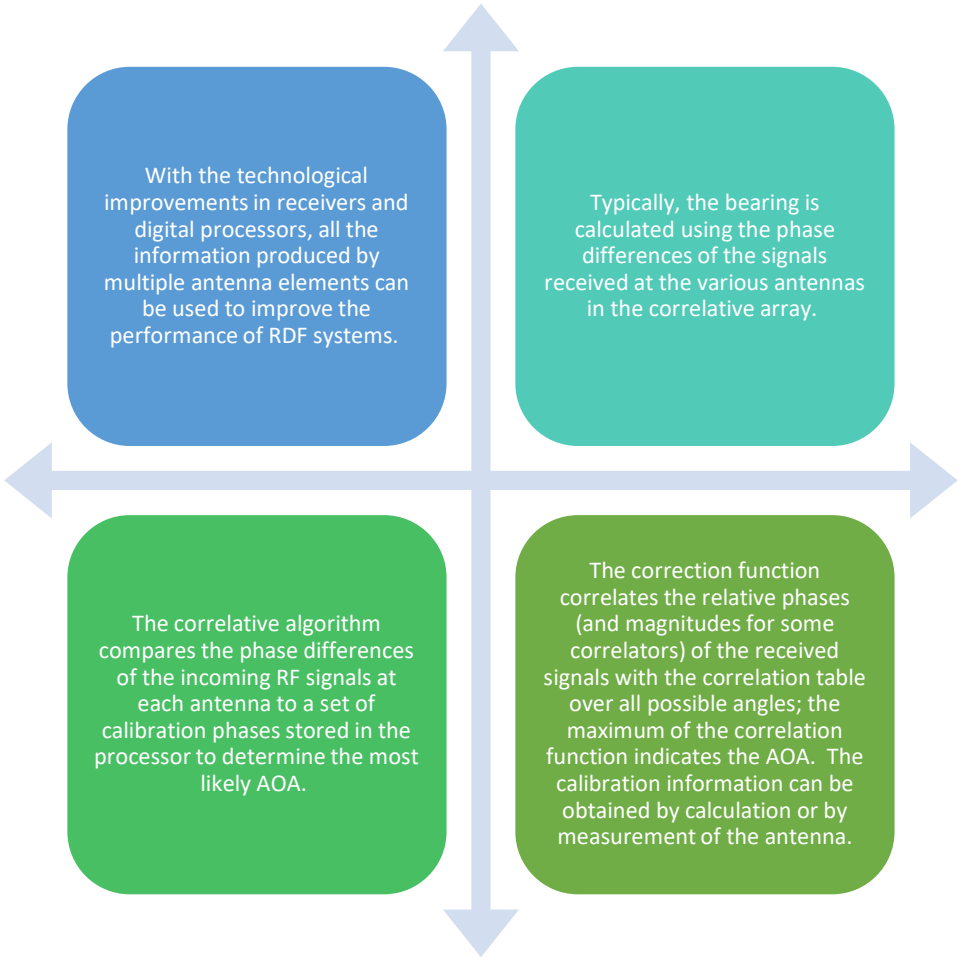
- The most common implementation of a correlative array is to have several omni directional antennas (typically four to nine antennas) in a circular pattern. In this configuration the differences in the phase of the incoming RF signal at each element is used by the correlative algorithm to determine 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

The two critical performance measures for DF systems are accuracy and sensitivity.

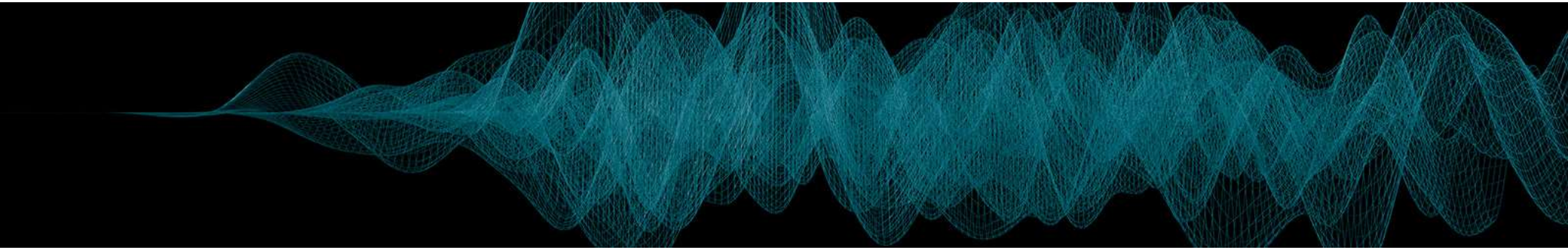
Accuracy is the measure of how accurate the bearing direction can be determined. The accuracy of a DF system is dependent on the DF processor, the specific design, the quality of the antenna elements used and the installation environment of the antenna.

Sensitivity is the measure of how well the DF system will perform in the presence of a small signal in a specified noise level. The sensitivity is dependent on the receiver noise, losses in the antenna and even the topology of the antenna elements in the array.

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.



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.

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