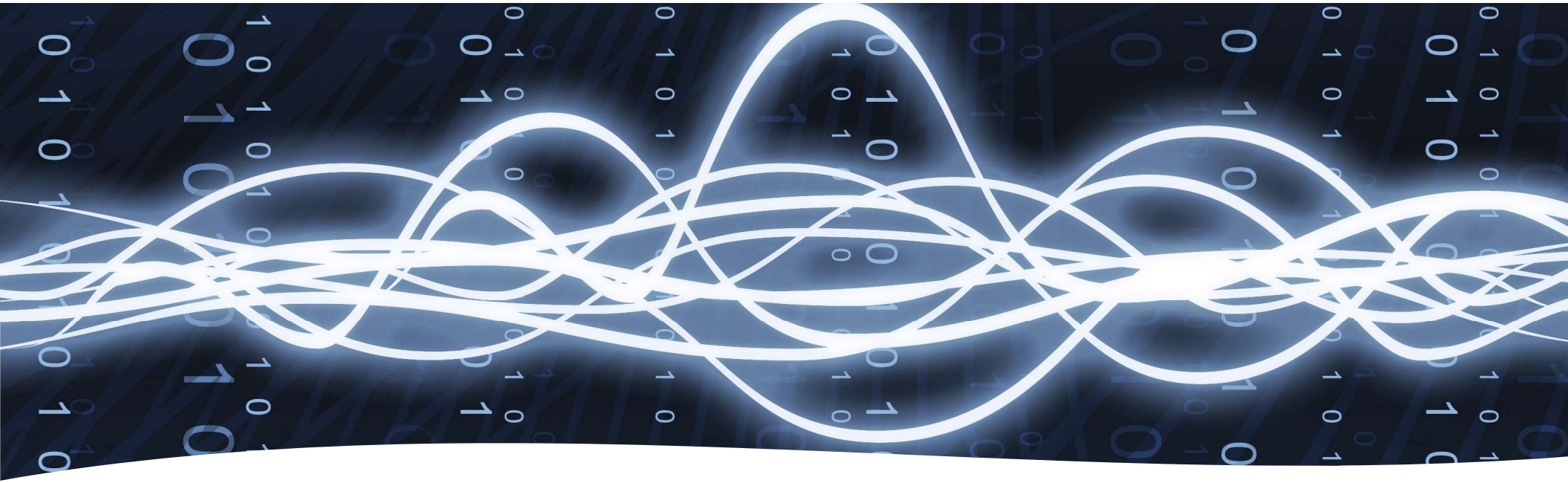
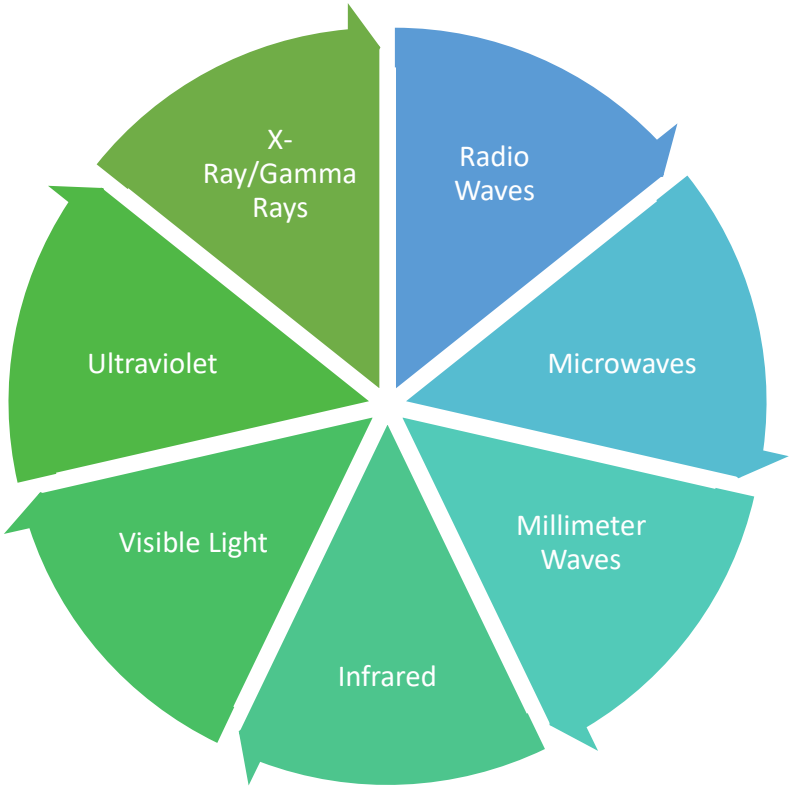


Part 2

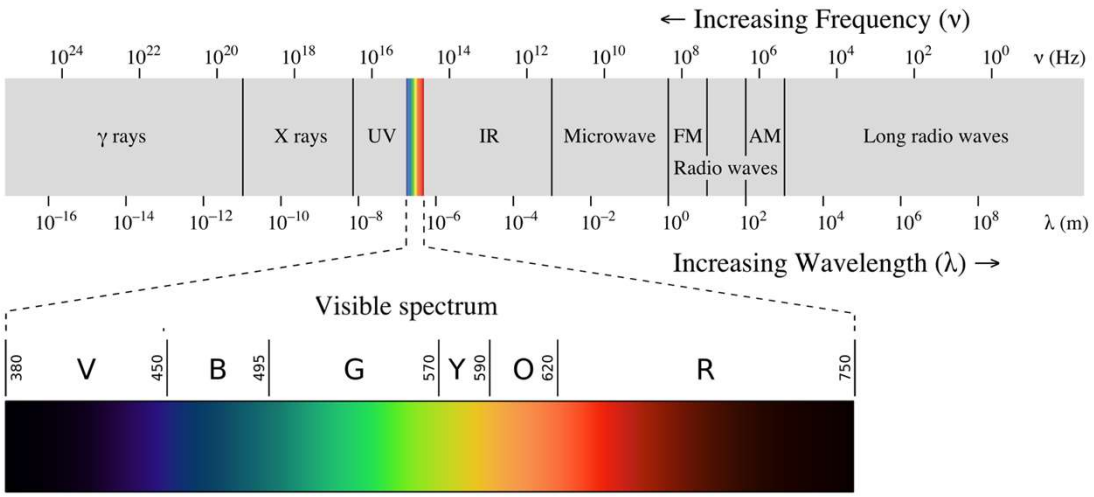
Elements of SIGINT

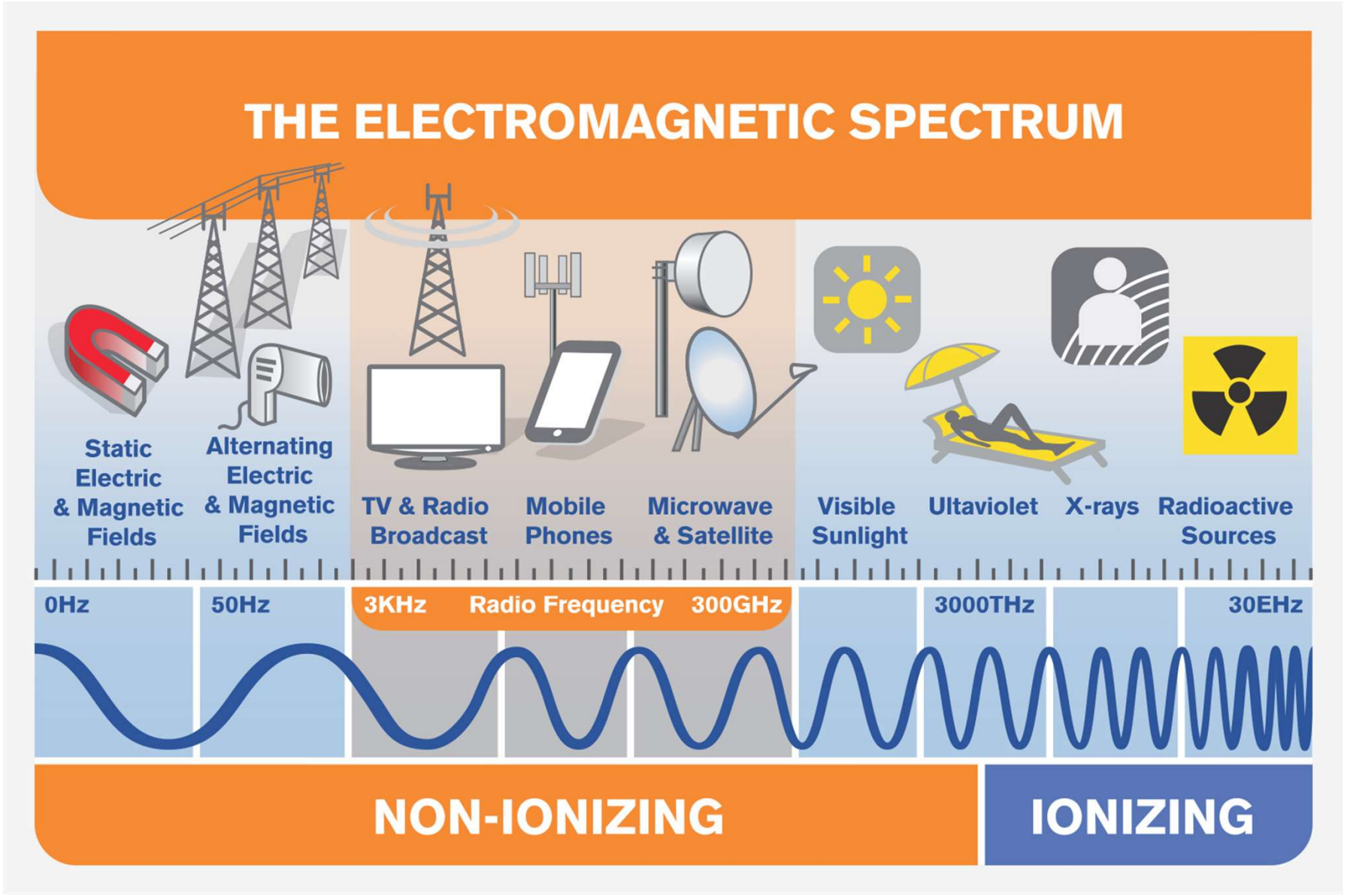
TONEX

Electromagnetic Spectrum

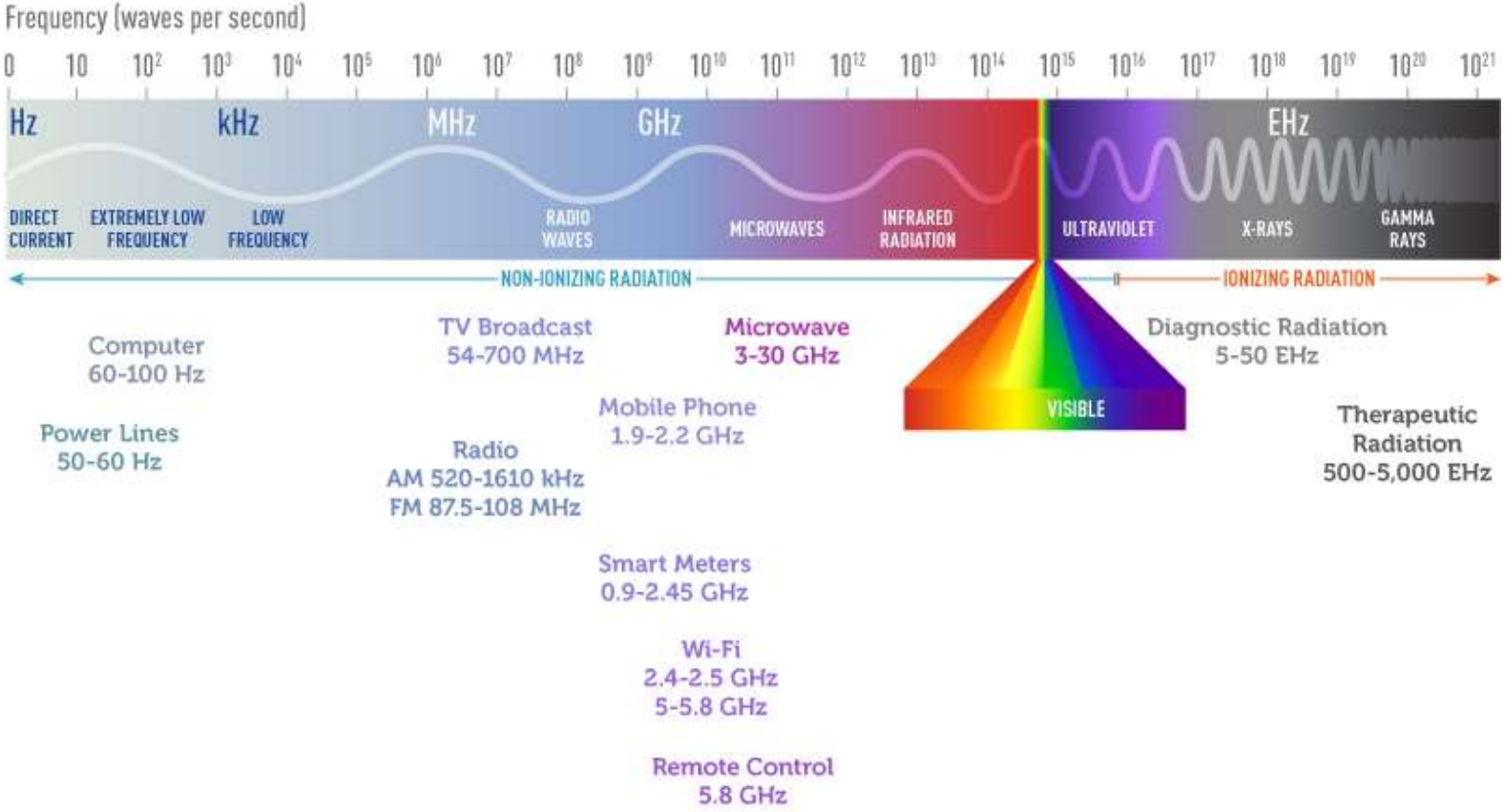


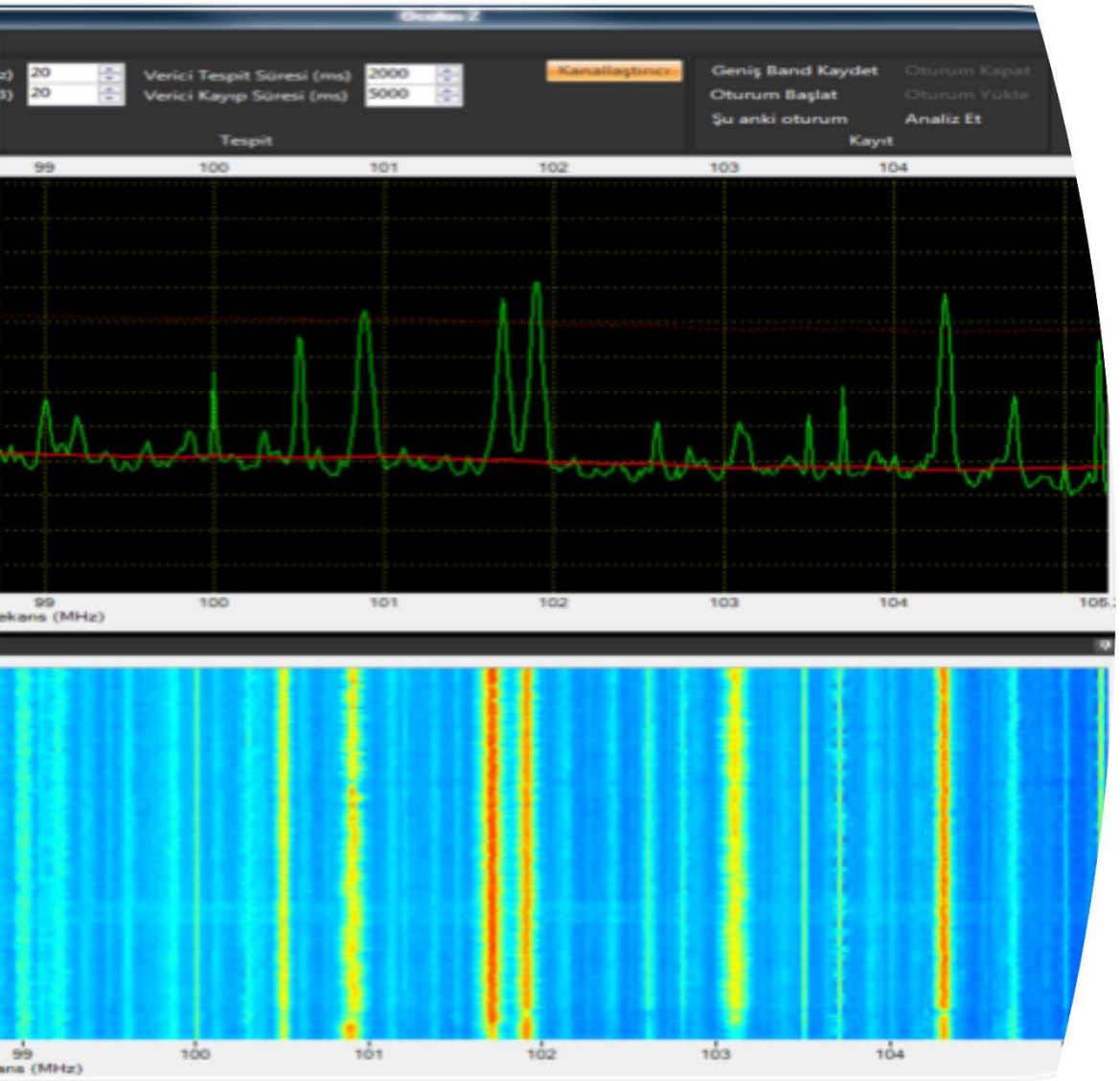
Example SIGINT




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

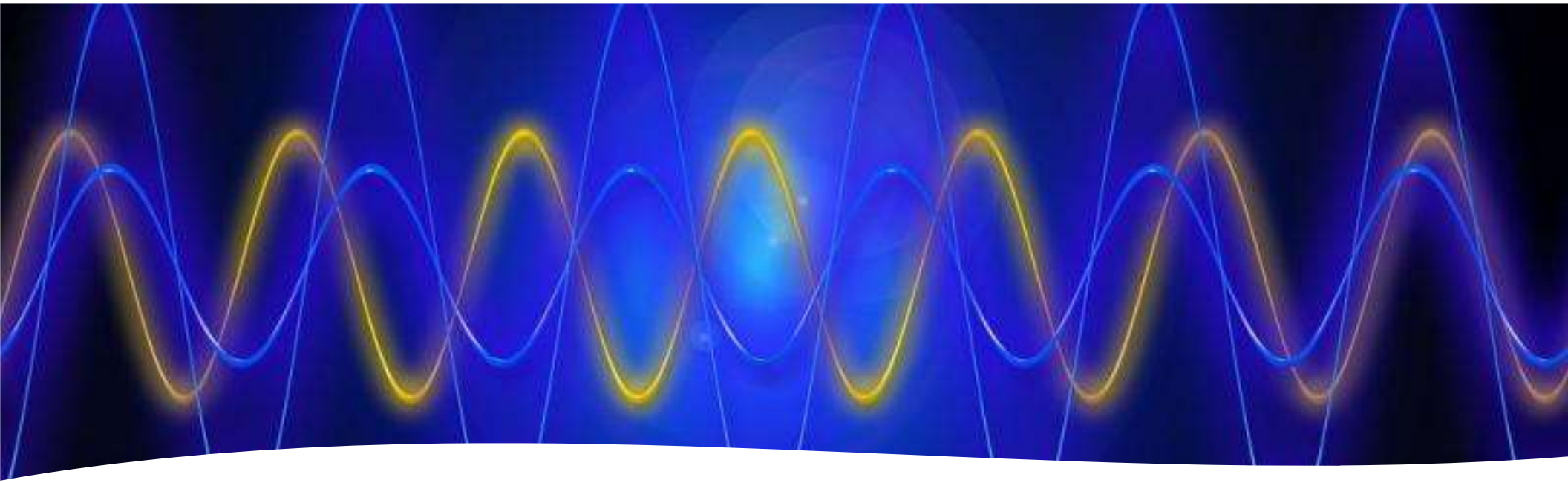
ELECTROMAGNETIC SPECTRUM





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).



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.

SIGINT Operational Platforms

Ground platforms

Strategic ground platforms
Tactical ground platforms

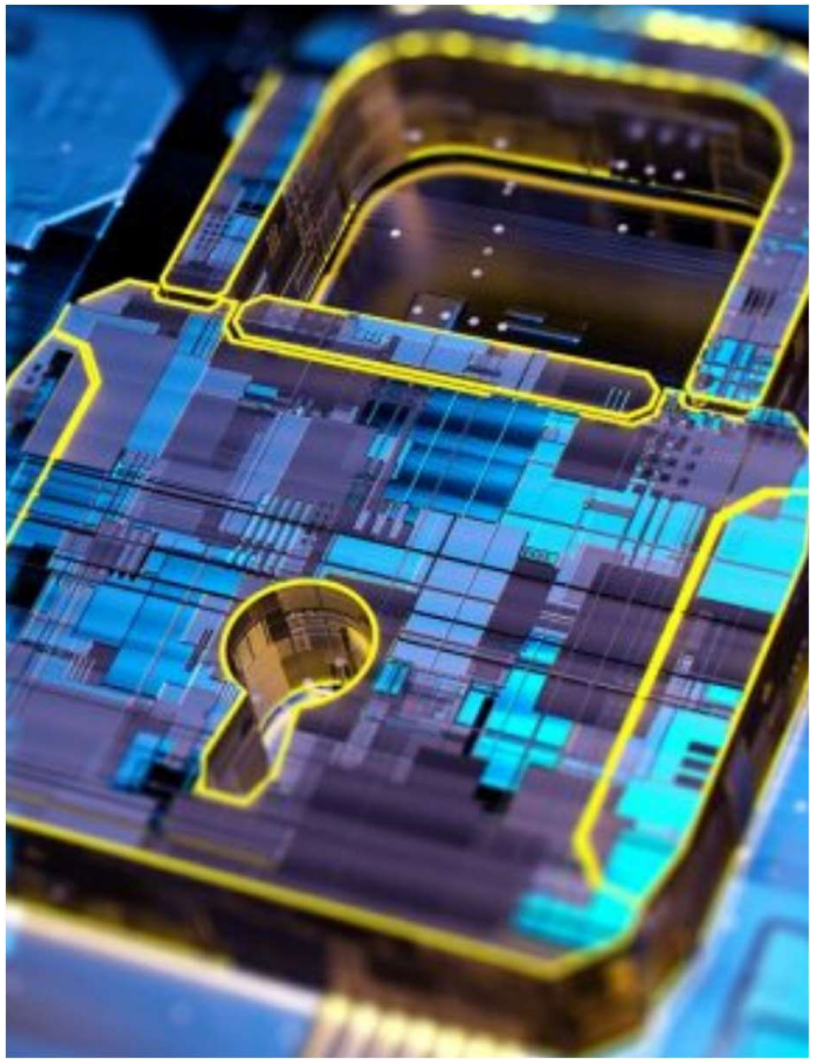
Ship platforms

Submarine platforms

Aircraft platforms

Tactical aircraft platforms
Strategic aircraft platforms

Satellite platforms



ELINT

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

ELINT using Software Defined Radio (SDR)

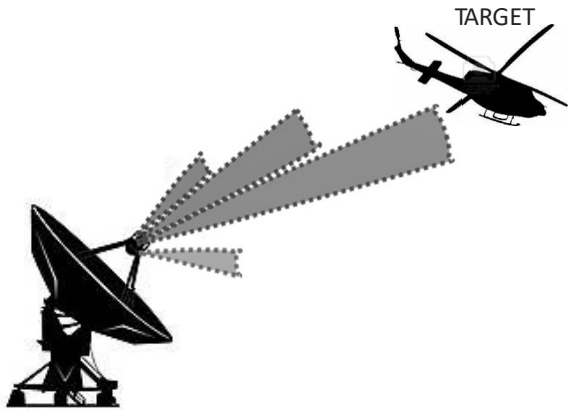
- DSP/FPGA for electronic intelligence
-
- Developing electronic intelligence systems using signal processing hardware: FPGA, DSP and I/O modules
- Mix FPGA with DSP processors, and to integrate that processing power with very fast communications ADCs, capable of sampling IF signals directly
- Most modern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

Technical ELINT

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

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

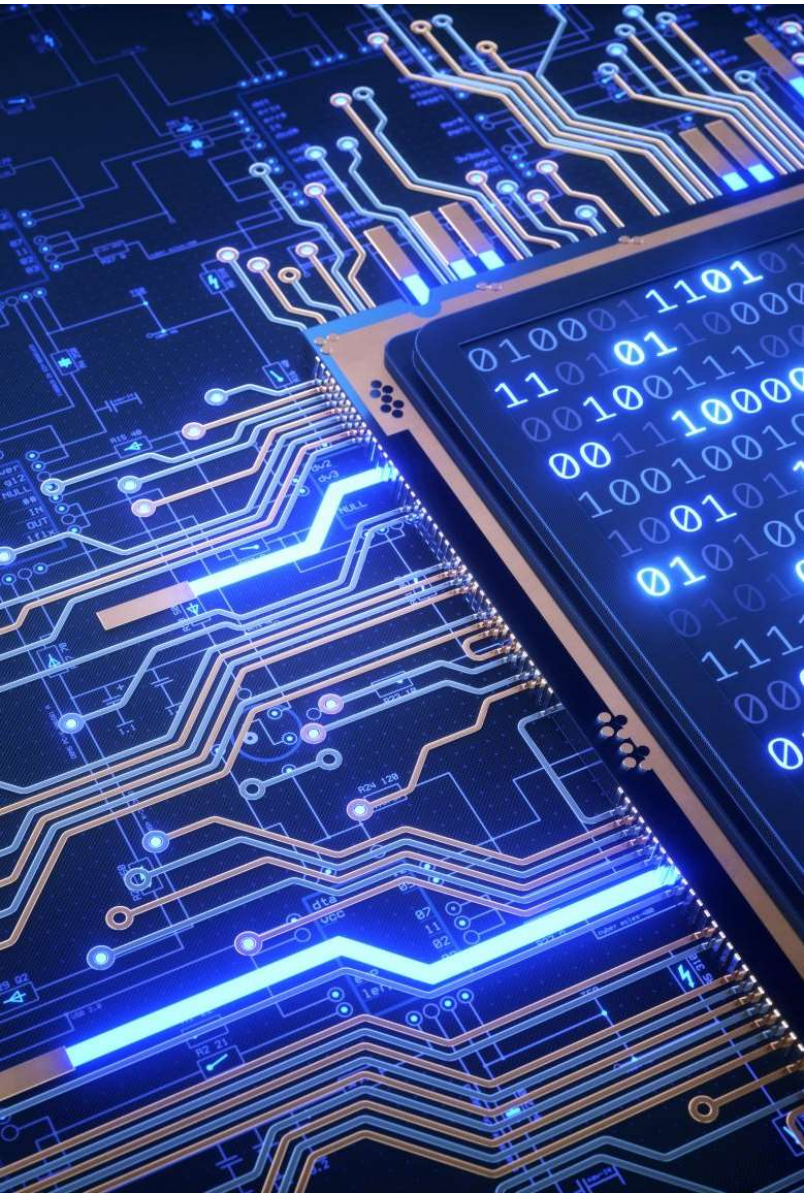
- For instance, the detection range of a radar against a given type of aircraft or missile can be computed, or the best ways to jam the radar can be determined.



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

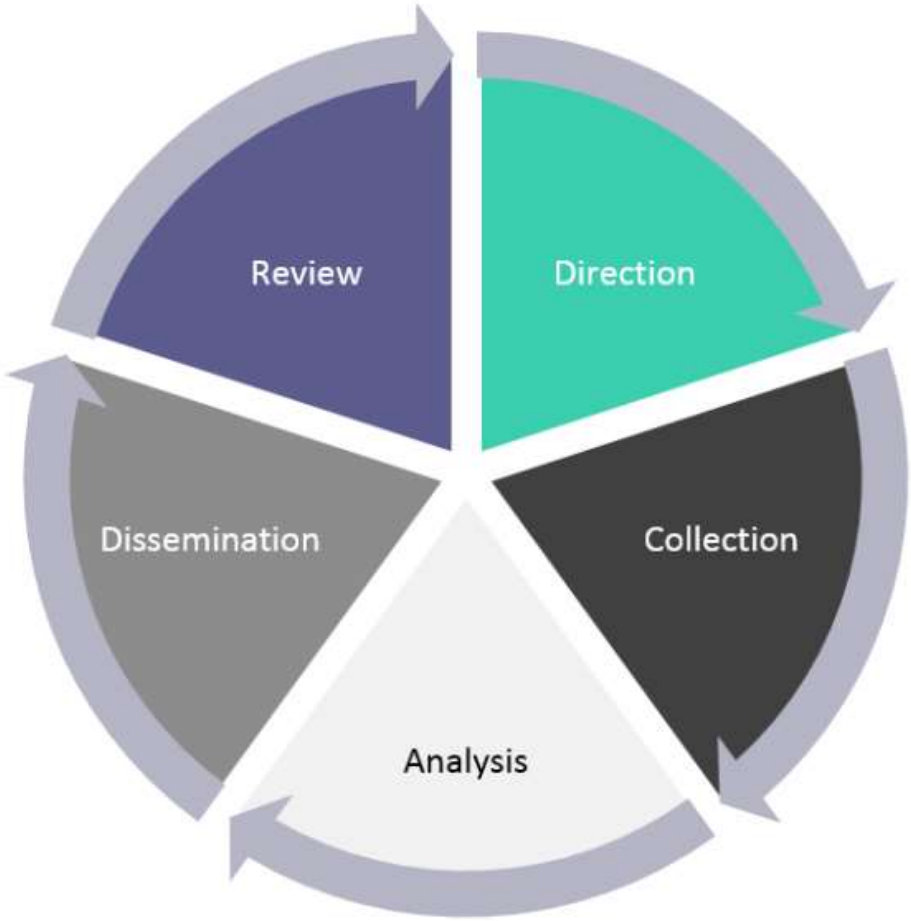


Signals intelligence operational platforms

- 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.

The Intelligence Cycle



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 Intelligence Cycle

Planning and Direction

Collection

Processing

Production

Dissemination

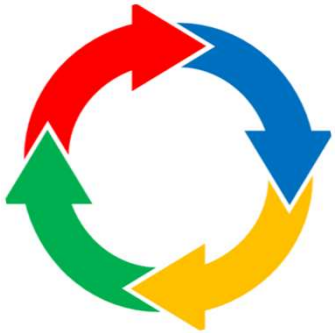
The Steps in the Intelligence Cycle

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.

Intelligence Collection Disciplines

- 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.

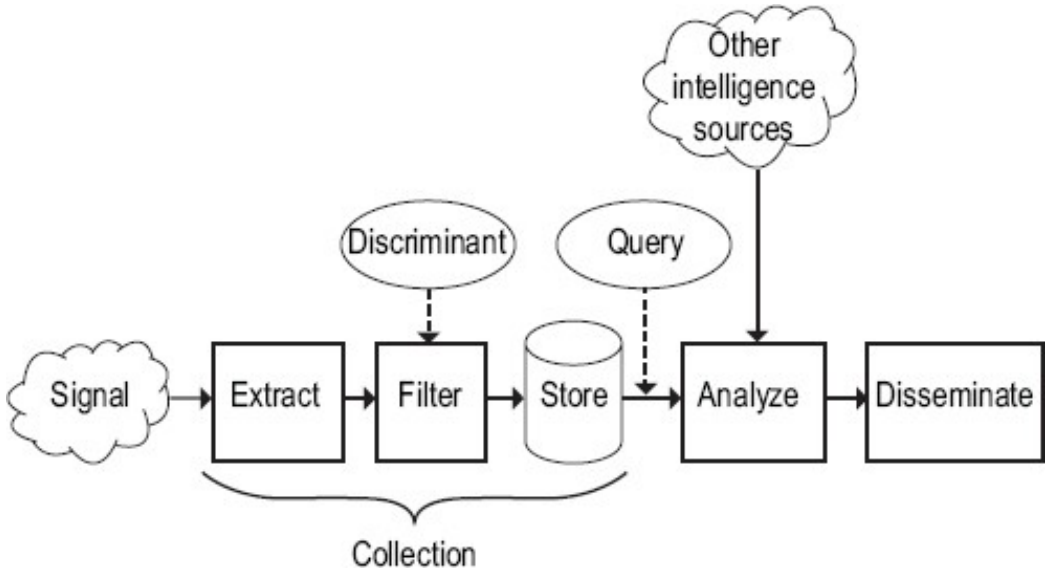
Signal Interception

COMMUNICATIONS INTELLIGENCE (COMINT)

ELECTRONIC INTELLIGENCE (ELLNT)

FOREIGN SIGNALS INTELLIGENCE (FISINT)

A Conceptual Model of Signals Intelligence



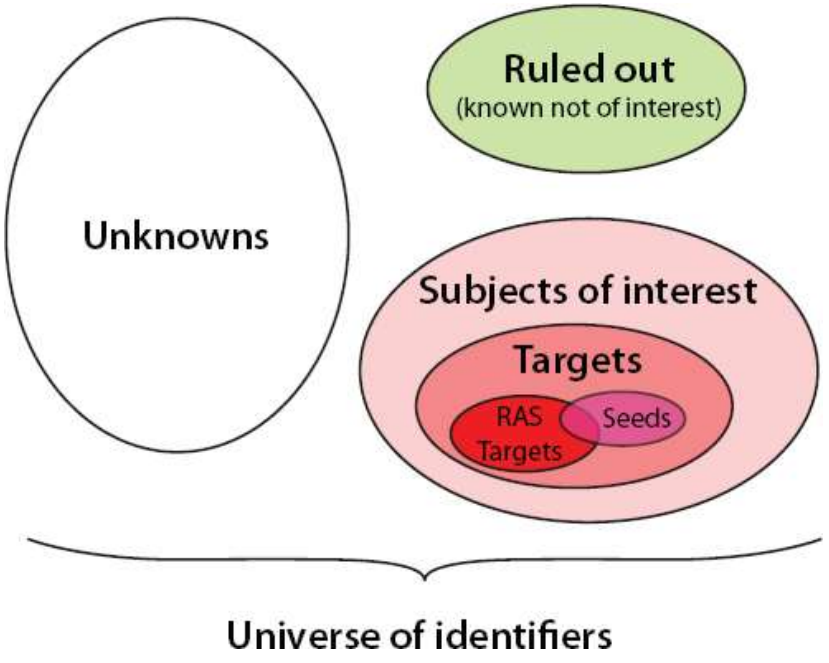
Classification of identifiers used in signals intelligence analysis

• *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.

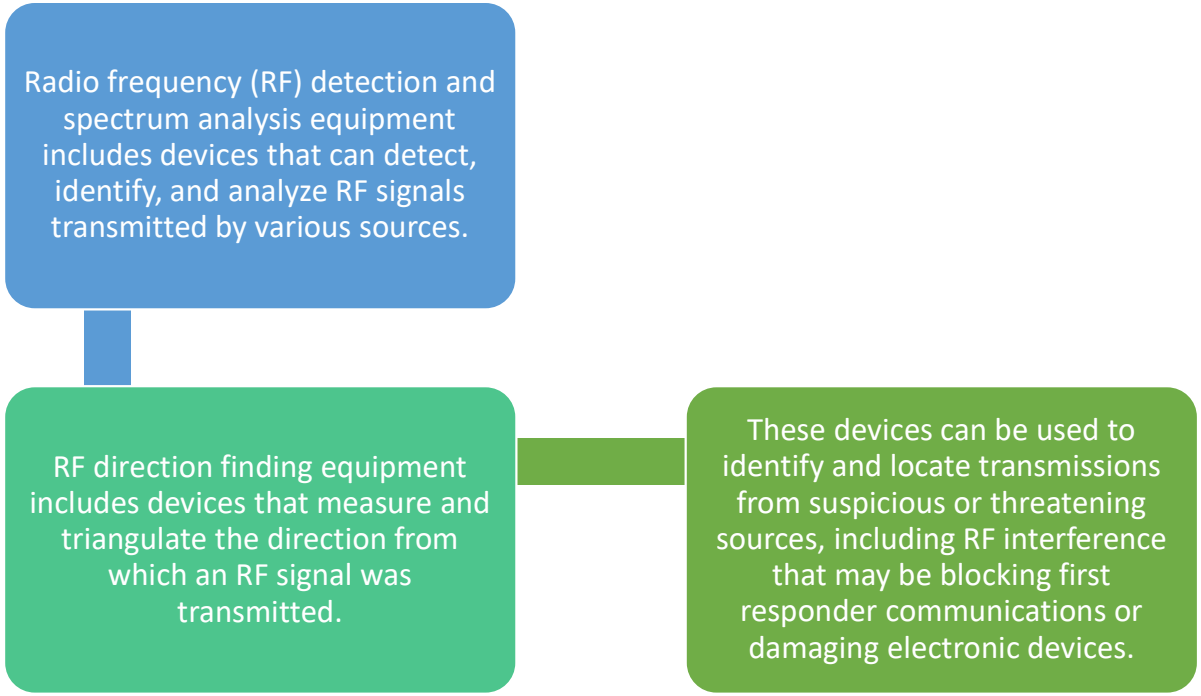
• RAS *target*: A target for which there is a reasonable and articulable suspicion that the person is associated with a foreign terrorist organization (RAS=reasonable, articulable suspicion)



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/

Find, Fix, Finish, Exploit, Analyze and Disseminate (F3EAD)

- The F3EAD cycle (Find, Fix Finish, Exploit, Analyze and Disseminate) is an alternative intelligence cycle commonly used within Western militaries within the context of operations that typically result in lethal action, such as drone strikes and special forces operations.

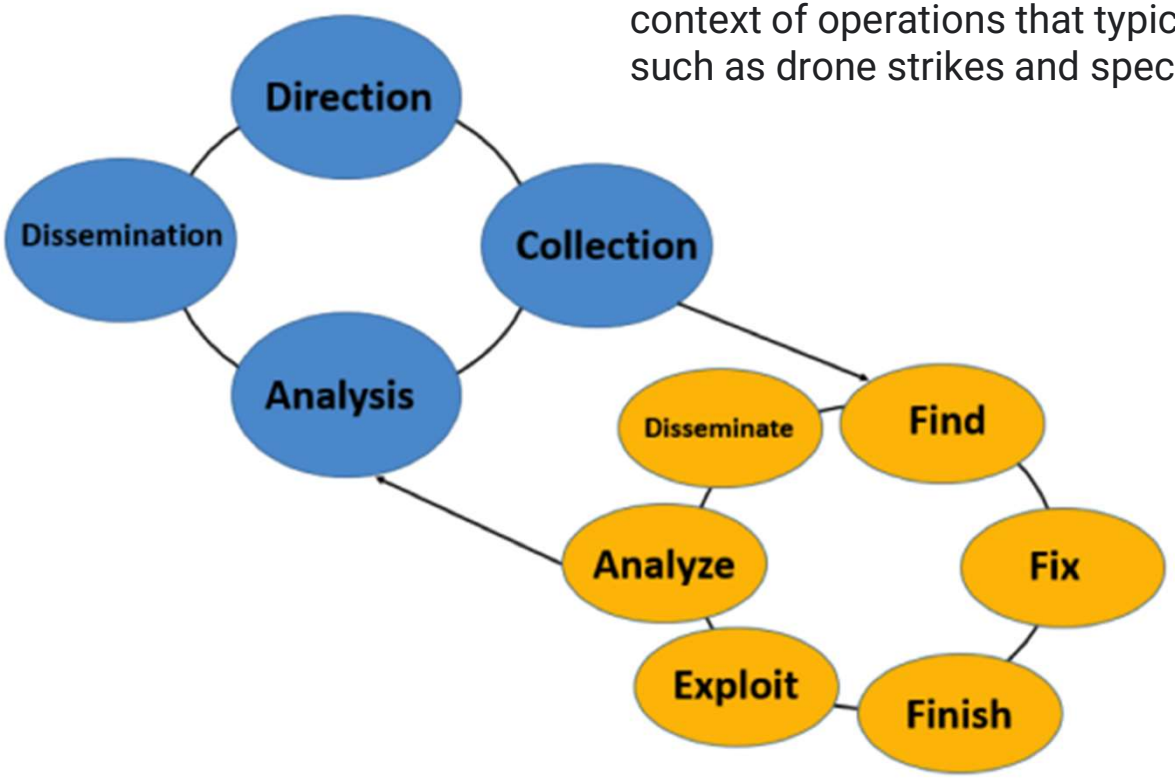
1. **Find:** essentially 'picking up the scent' of the opponent, with the classic "Who, What, When, Where, Why" questions being used within this phase to identify a candidate target
2. **Fix:** verification of the target(s) identified within the previous phase, which typically involves multiple triangulation points. This phase effectively transforms the intelligence gained within the "Find" phase into evidence that can be used as basis for action within the next stage
3. **Finish:** based on the evidence generated from the previous two phases the commander of the operation imposed their will on the target
4. **Exploit:** deconstruction of the evidence generated from the finish phase
5. **Analyze:** fusing the exploited evidence with the wider intelligence picture
6. **Dissemination:** finally publishing the results of the research to key stakeholders

THE INTELLIGENCE CYCLE	
Phase	**Action**
Direction	Board level identification of APT groups as the core cyber security threat to the business
Collection	The company's threat intelligence team collects data gathered from internal response cases and fuses it with data provided by the external threat intelligence provider.
Analysis	A full fusion and analysis of collected data over a strategic period of time (6 months to 1 year)
Dissemination	Results communicated back to the board and the wider threat intelligence community around the specific APT threat that has targeted the company

FIND, FIX, FINISH, EXPLOIT, ANALYZE AND DISSEMINATE (F3EAD)	
Phase	**Action**
Find	Suspect activity identified on several hosts
Fix	Multiple common indicators of suspicious activity identify a cluster of infected hosts
Finish	Hosts are taken offline, and employees are given new machines
Exploit	Based on analysis of malware found within the infected hosts several specific Indicators of Compromise (IOCs) are identified by the team
Analyse	Fusing the IOCs found 'in house' with the IOCs provided by the third part intelligence provider feeds into the wider picture of the APT threat and leads to further identification of anomalous behavior on the company's network
Disseminate	The results of the analysis are disseminated to both tactical consumers and the strategic sponsors of the project i.e. the members of the 'c suite' with an interest in the issue

F3EAD

The F3EAD cycle (**Find, Fix, Finish, Exploit, Analyze and Disseminate**) is an alternative intelligence cycle commonly used within Western militaries within the context of operations that typically result in lethal action, such as drone strikes and special forces operations.



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)

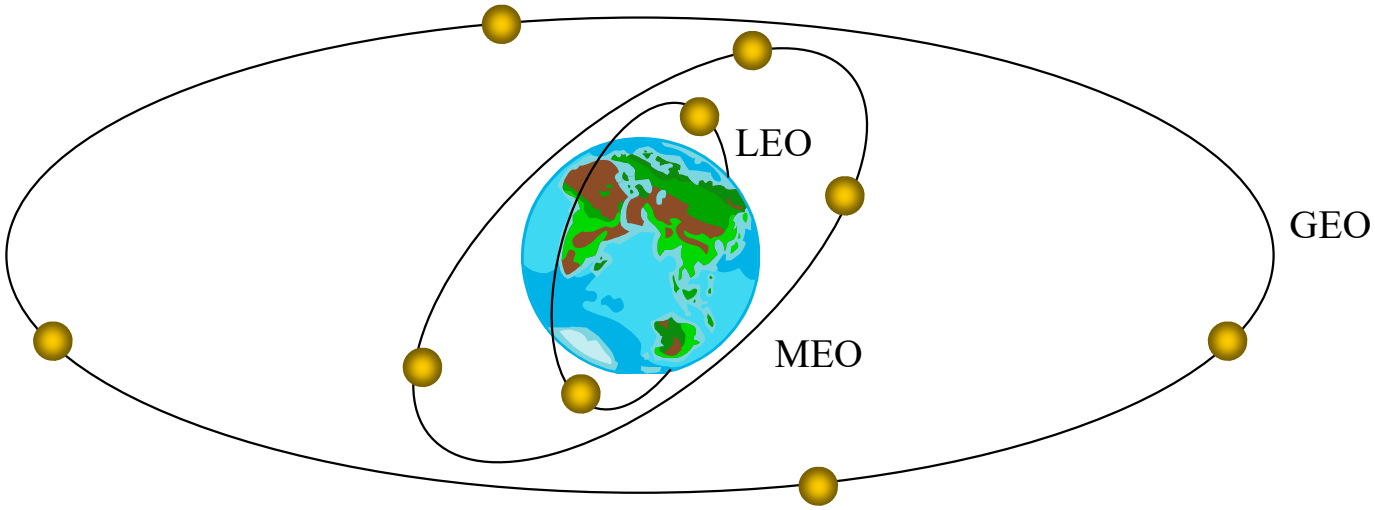
Electronics intelligence (ELINT)

Foreign Instrumentation Signals Intelligence Foreign instrumentation signals intelligence (FISINT)

SIGINT Planforms and Applications

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

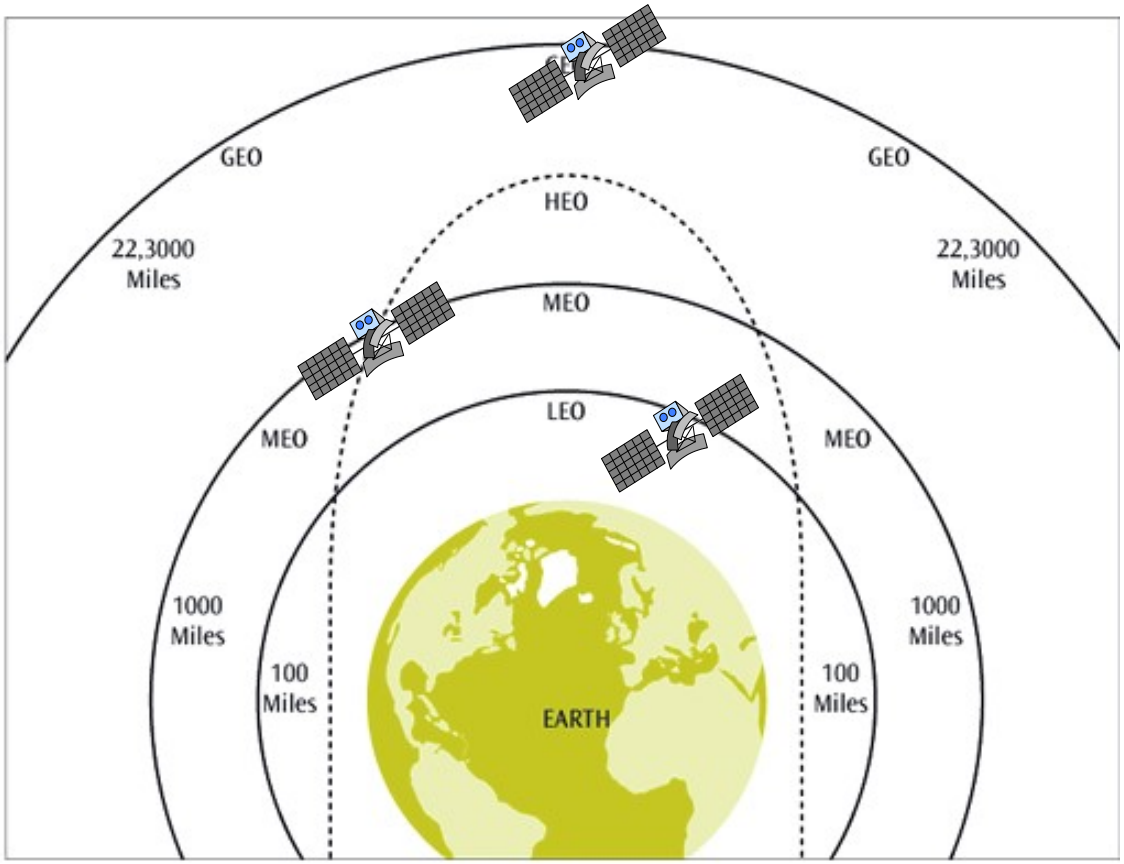
Satellite Orbits



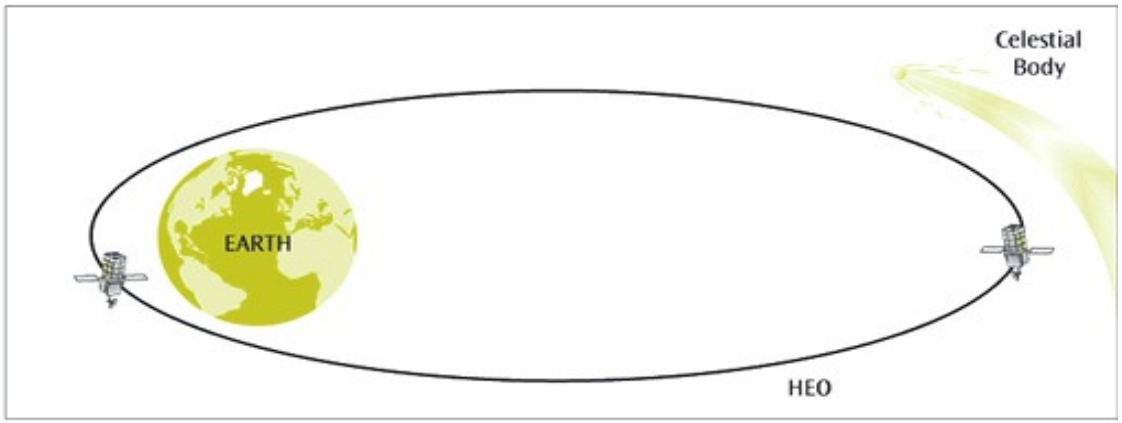
LEO: Low Earth Obit
MEO: Medium Earth Orbit
GEO: Geostationary Earth Orbit

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

Satellite orbits: LEO, MEO, GEO and HEO



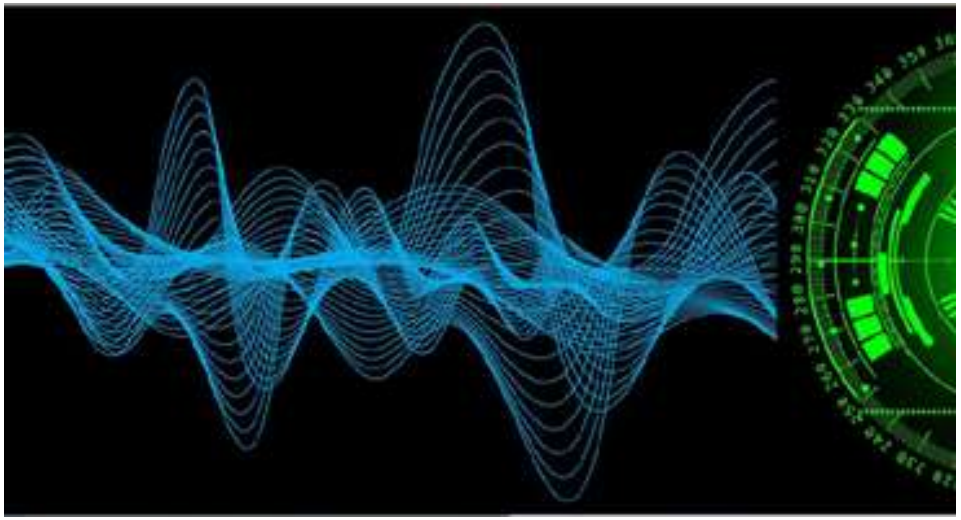
HEO Polarization Highly Elliptical Orbit



What is a Signal?

- A signal is any representation that can be interpreted by someone or some thing that has contextual awareness (codification) to either take an action or not take an action on.

- Usually, signals are combined with timing intervals to help convey or not-convey a message. If you look at a traffic light, you'll notice that red means stop, yellow means yield, and green means proceed.



Signal Analysis

- **Signal**

- **Analysis**

- A process in the production step of the intelligence cycle in which intelligence information is subjected to systematic examination in order to identify significant facts and derive conclusions.

What is Intelligence?

- Intelligence is information that can be derived from the sampling or collection of data or metadata to put into action either (manually or automated) to meet a specific objective.

- One of the many goals with appropriate use of intelligence is to find or "dig" through information that is otherwise ***unknown*** using different methods and other historically known information.

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 Function

- Intelligence function involves the collection, analysis, and dissemination of information to decision makers.

- The **intelligence function** comprises the gathering, evaluation and dissemination of information relevant to decision-making, and may include prediction based on such information, as well as planning for future contingencies.

- Intelligence analysts use all available sources of such information to understand problems of interest to decision makers.

- These sources include human intelligence, imagery, and a variety of other kinds of intelligence in addition to signals intelligence (SIGINT).

Tactical and Strategic Information

- The intelligence process seeks information about both tactical matters (i.e., specific dangerous persons, groups, or plots, such as known terrorist organizations or plans to bomb subways or investigations of recent bombings) and strategic matters (i.e., a broad picture of a threat, such as a country's plans to build nuclear weapons).

- Increasingly, this is not a sharp distinction, because context is often important to understanding a tactical threat, and tactical information is required to respond to strategic threats.

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.

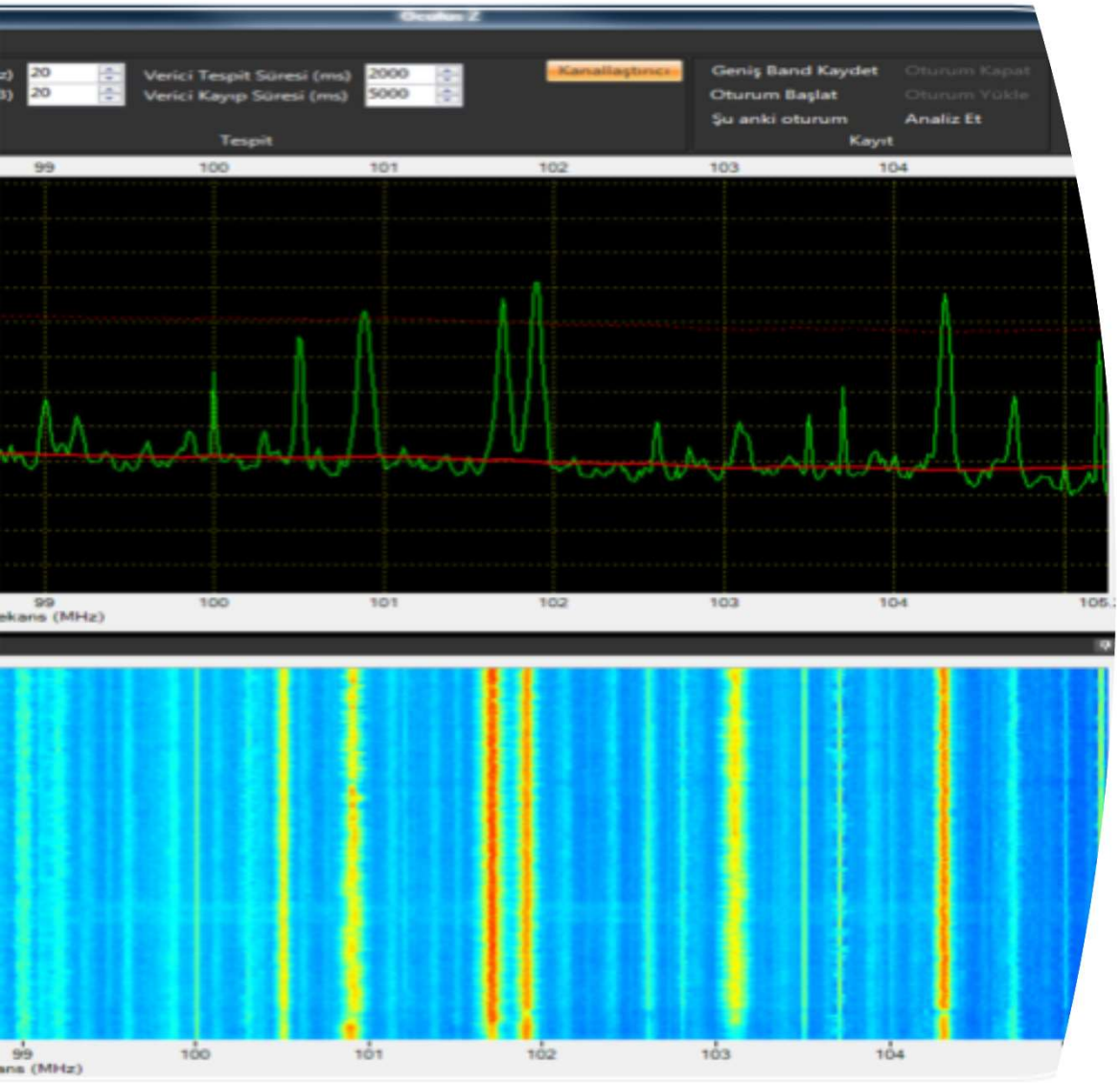
Principles of Collection

- 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.

Six Basic Intelligence Sources

There are six basic intelligence sources, or collection disciplines:

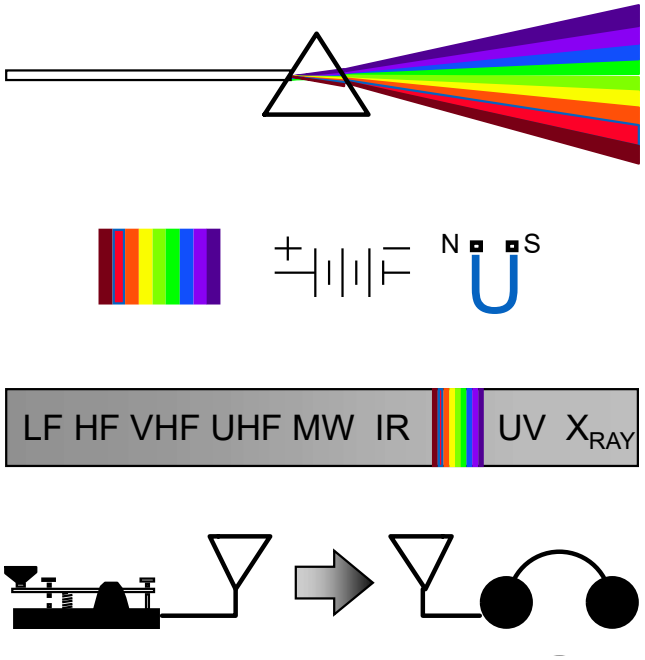
- SIGINT—Signals Intelligence
- IMINT—Imagery Intelligence
- MASINT—Measurement and Signature
- HUMINT—Human intelligence
- OSINT—Open-Source Intelligence
- GEOINT—Geospatial Intelligence



SIGINT

- 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).
- In U.S. National Security Agency (NSA) is responsible for collecting, processing, and reporting SIGINT.
- The National SIGINT Committee within NSA advises the Director, NSA, and the DNI on SIGINT policy issues and manages the SIGINT requirements system.

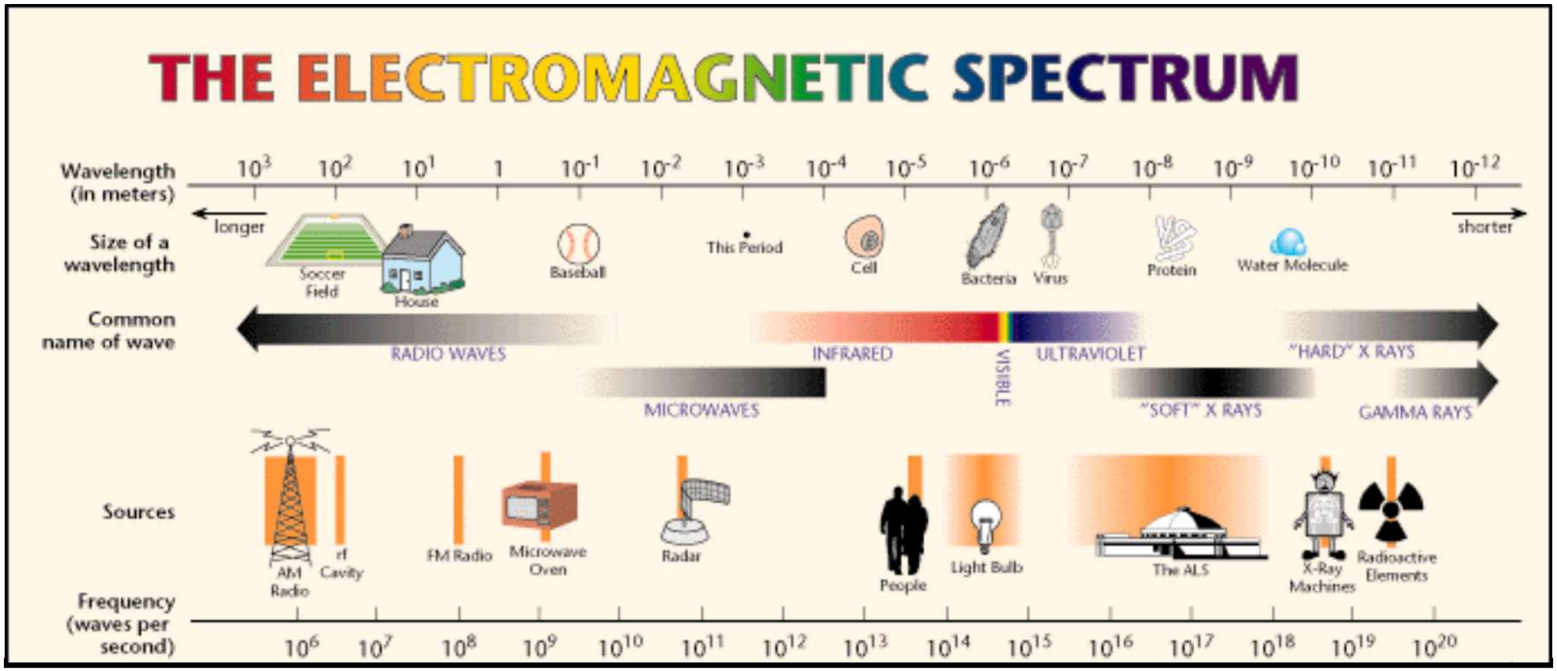
How Did We Get Here?



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
- **1890's** First successful demos of radio transmission

Electromagnetic Waves

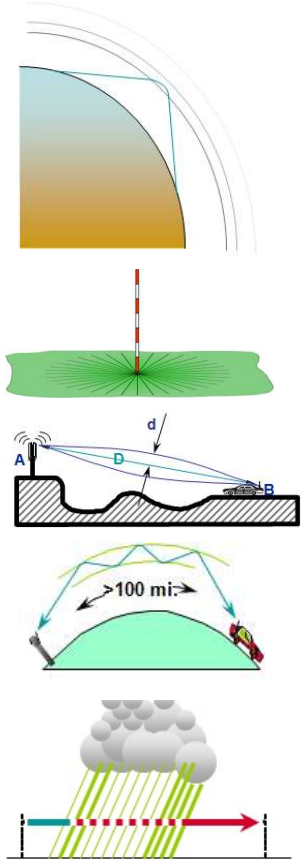


Courtesy Berkeley National Laboratory

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

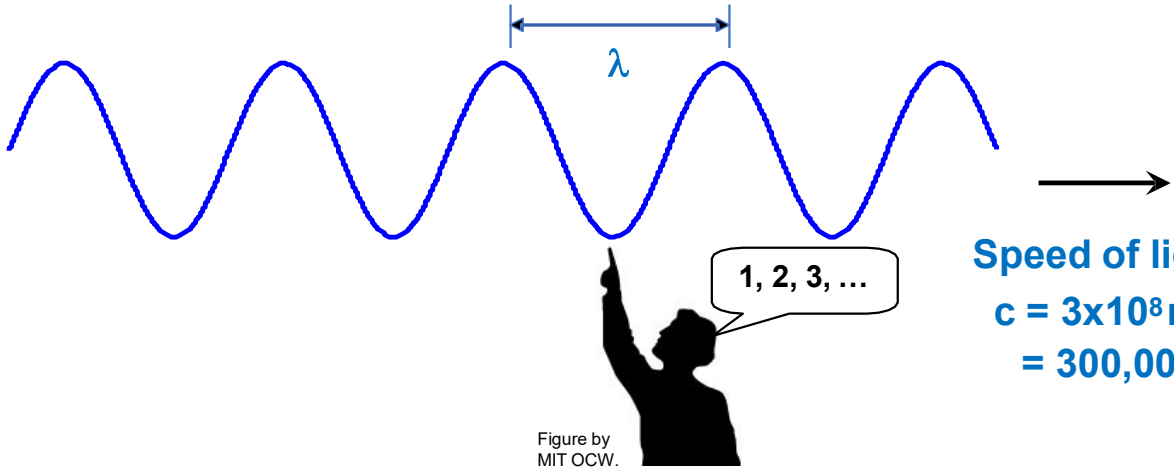


Figure by MIT OCW.

Speed of light, c

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

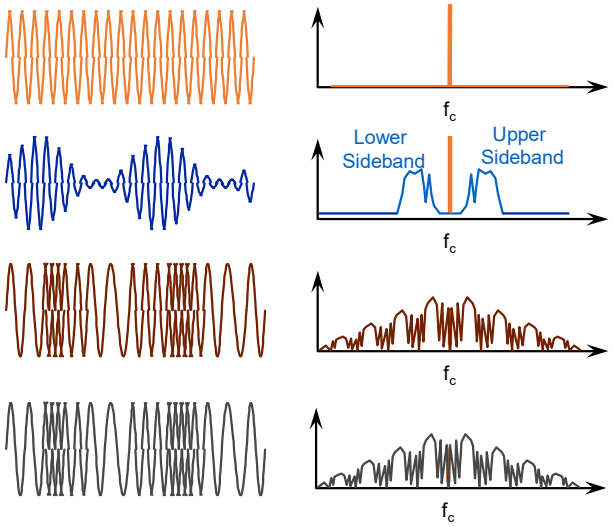
= 300,000,000 m/sec

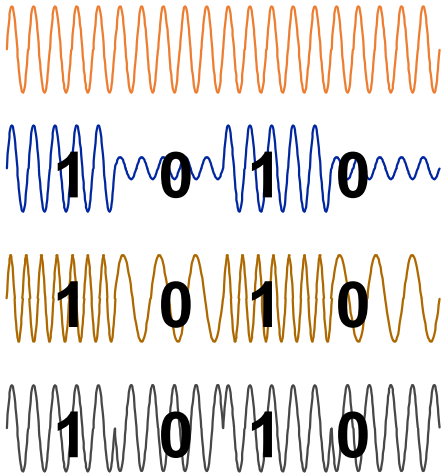
$$\text{Frequency (1/s)} = \frac{\text{Speed of light (m/s)}}{\text{Wavelength } \lambda \text{ (m)}}$$

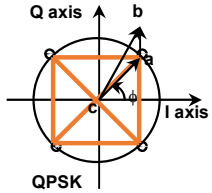
Examples:

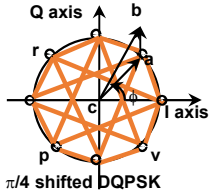
Frequency	Wavelength
100 MHz	3 m
1 GHz	30 cm
3 GHz	10 cm
10 GHz	3 cm

Basics of Communications Signals

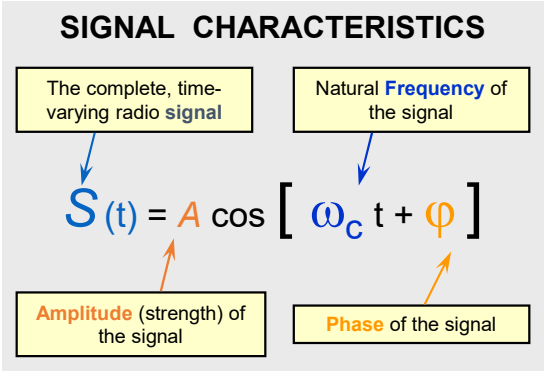




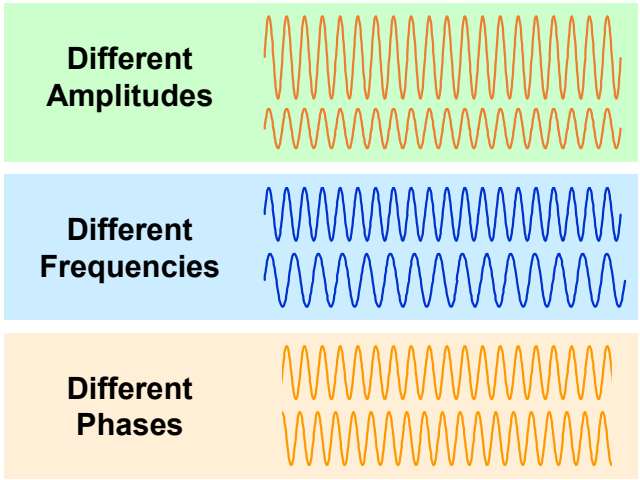




Characteristics of a Communication Signal

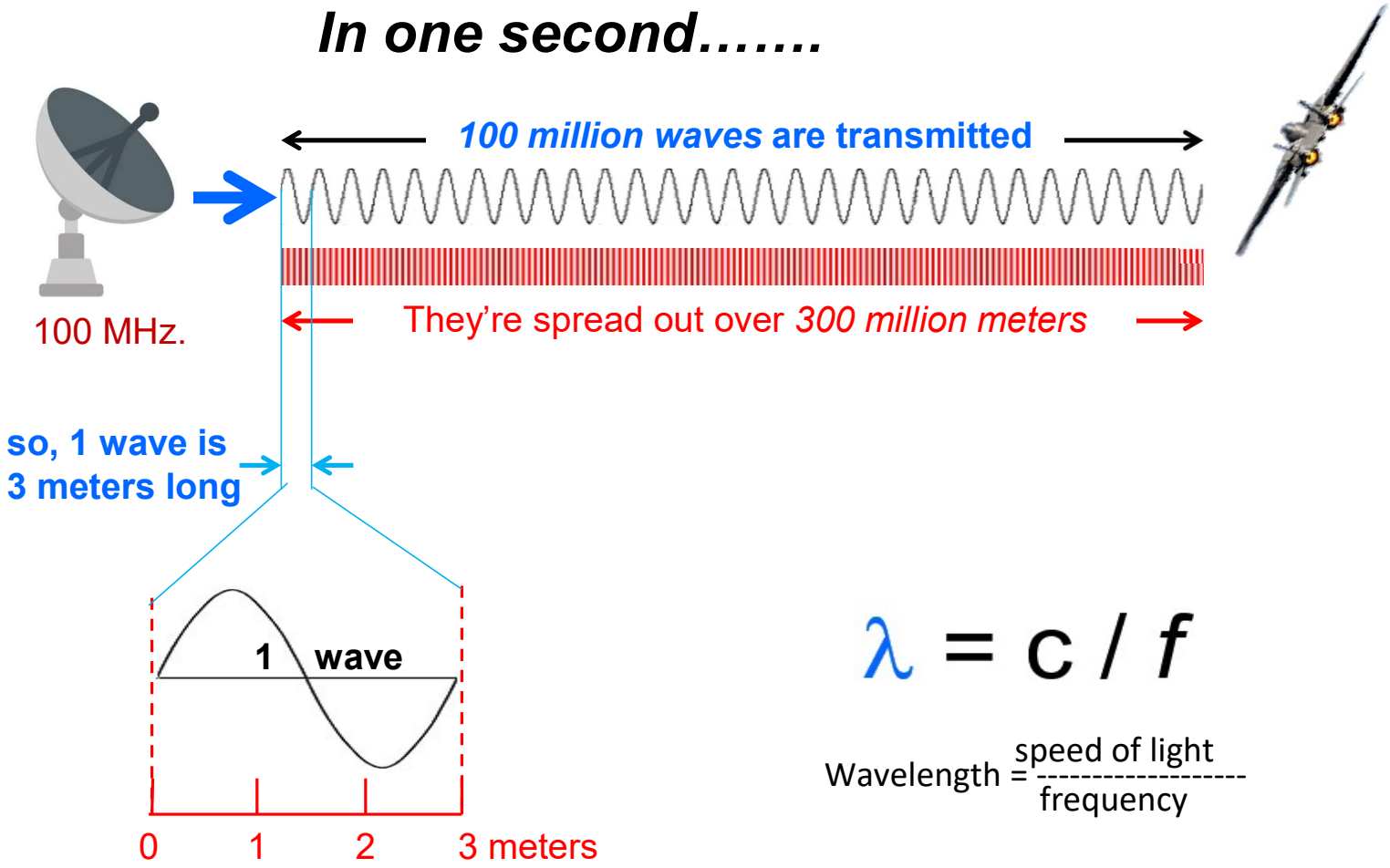


Compare these Signals:



- 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

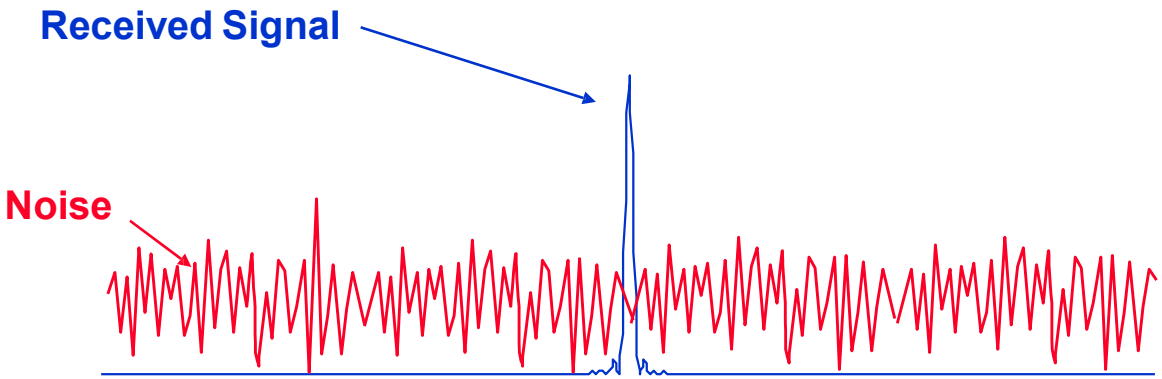
Frequency vs. Wavelength Example



$$\lambda = c / f$$

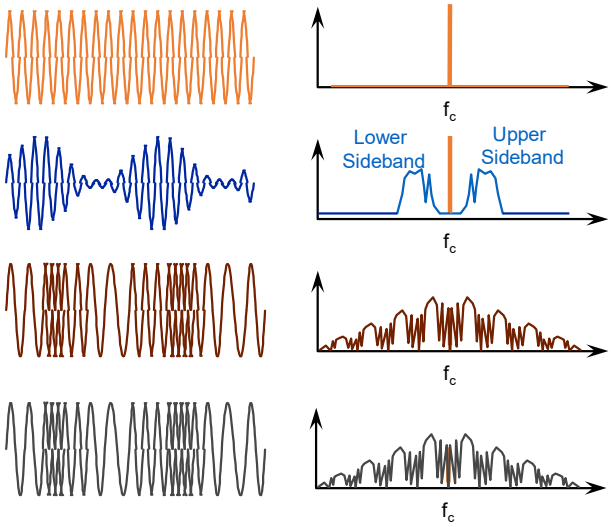
$$\text{Wavelength} = \frac{\text{speed of light}}{\text{frequency}}$$

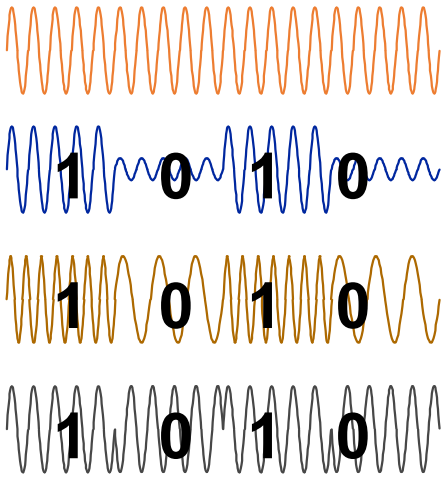
Signal-to-Noise Ratio

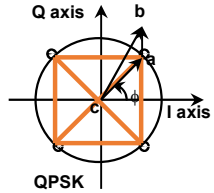


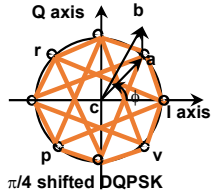
$$\text{SNR} = \frac{\text{Received Signal Energy}}{\text{Noise Energy}}$$

Basics of Signal Theory

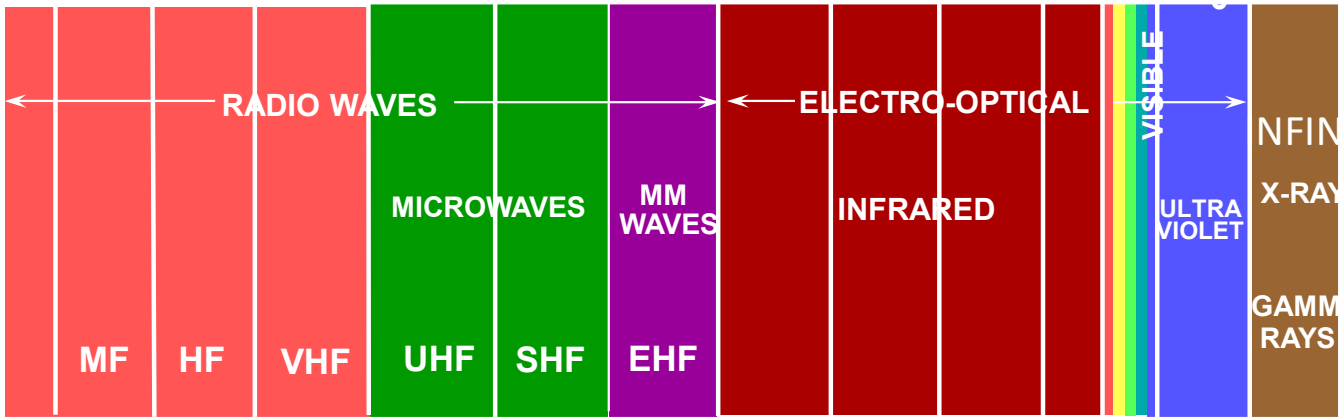








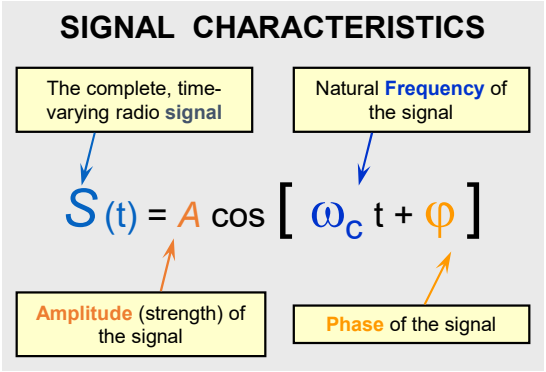
EM SPECTRUM



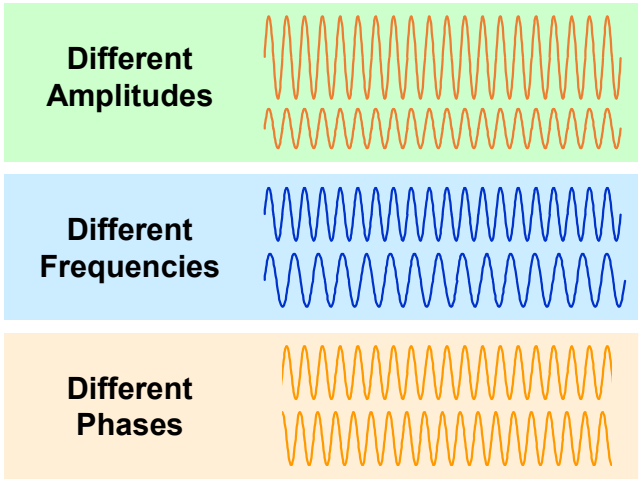
As you move along the spectrum, the behavior and usefulness of the frequency bands for specific applications changes.

The long wavelengths of HF range allows us to bounce signals off the ionosphere. The extremely short wavelengths of the x-ray and gamma ray allow us to “see” into objects.

Characteristics of a Communication Signal



Compare these Signals:

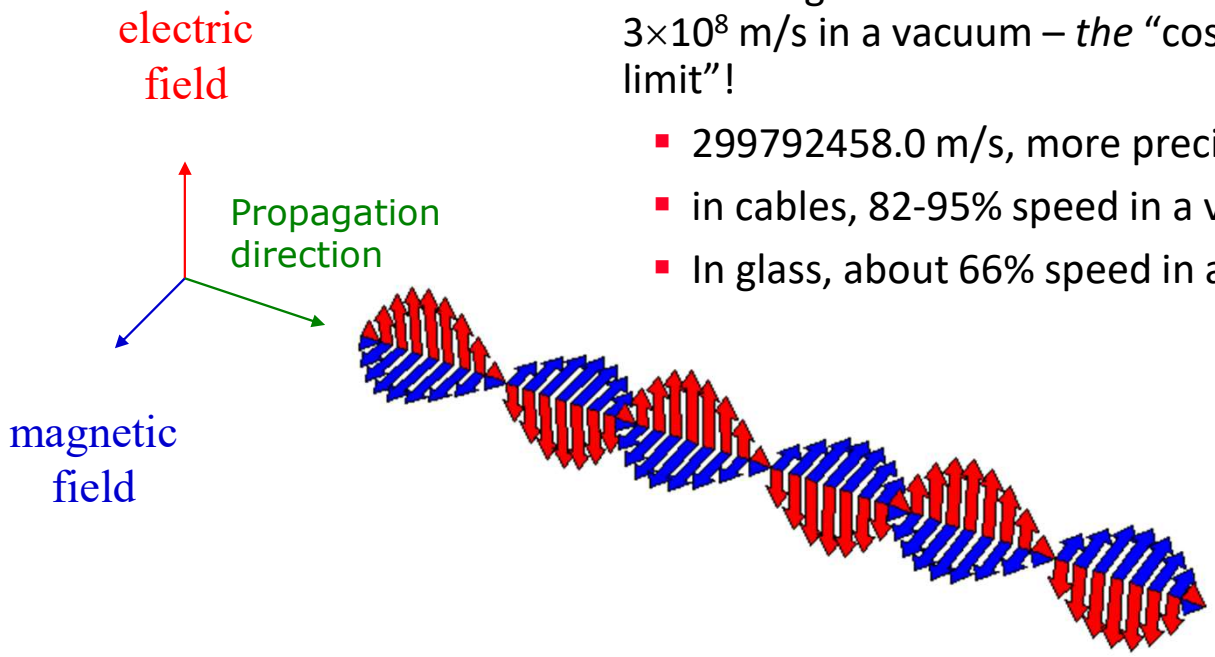


- The purpose of telecommunications is to send information from one place to another
- Our civilization exploits the transmissible nature of radio signals, using them in a sense as our "carrier pigeons"
- To convey information, some characteristic of the radio signal must be altered (I.e., 'modulated') 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

RF Basics

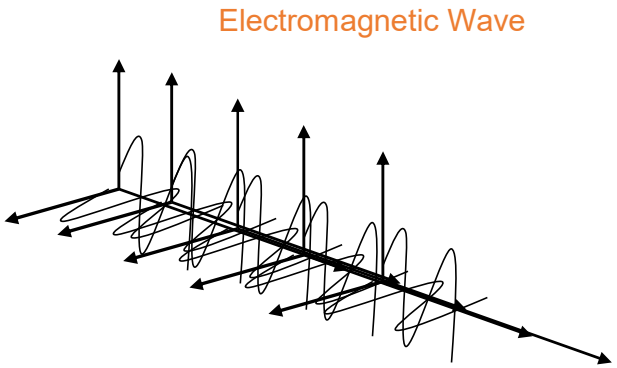
- **RF** refers to radio frequency, the mode of communication for wireless technologies of all kinds, including AM/FM radio, TV, VHF/UHF radio systems, cellular phones, radar, ham radio, GPS, WiFi, Satellite communications, industrial communications and two-way radio, remote sensing, medical treatments, and even dielectric and induction heating in manufacturing processes
- Radio signals are electromagnetic waves which travel at the speed of light, approximately 186,000 miles per second (300,000 km/s) in the atmosphere or space.
- In more dense material, that speed is lower – for example, about 200,000 km/s in glass fiber or in water
- RF waves are invisible to the human eye, except for a very small part of the spectrum which we call “visible light”.

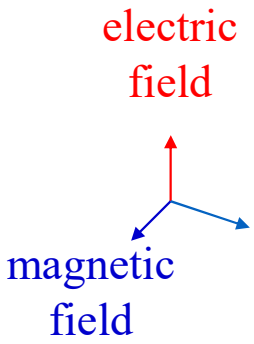
Electromagnetic Radiation

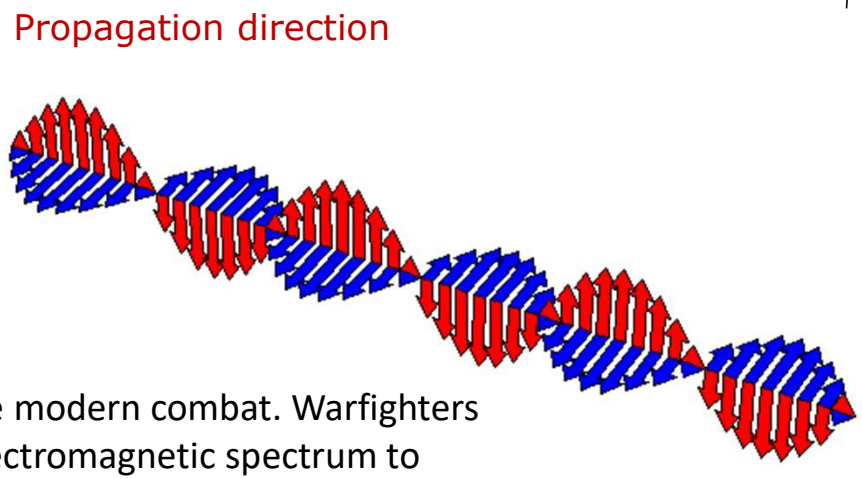


- Interrelated electric and magnetic fields traveling through space
- Electromagnetic radiation travels at about c = 3×10^8 m/s in a vacuum – *the* "cosmic speed limit"!
  - 299792458.0 m/s, more precisely
  - in cables, 82-95% speed in a vacuum
  - In glass, about 66% speed in a vacuum

Electromagnetic Spectrum and Propagation Direction







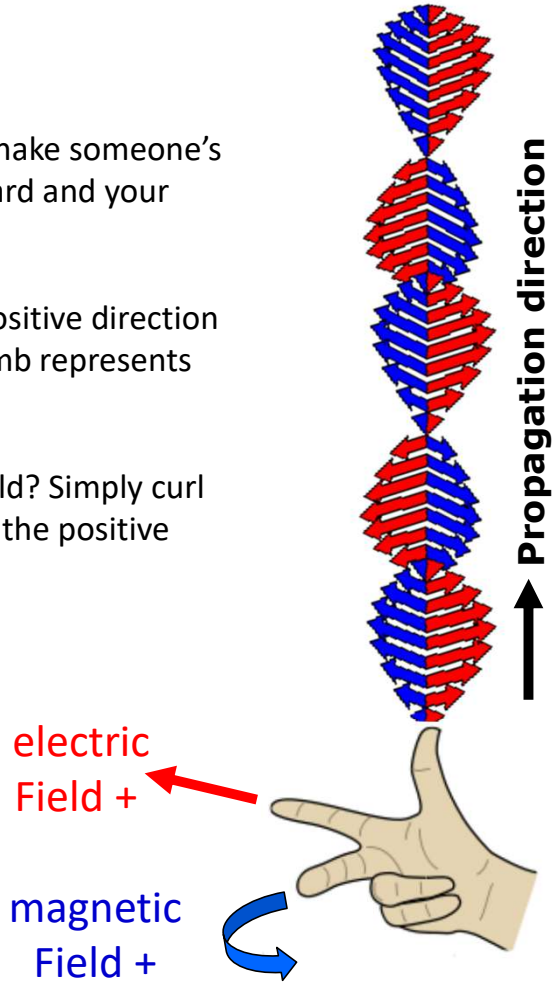
Electronic devices dominate modern combat. Warfighters depend on access to the electromagnetic spectrum to communicate with friendly forces, track enemy movements, navigate in the fog of war, collect intelligence, and perform many other vital functions. Electronic warfare is the military specialty concerned with denying enemy forces use of the spectrum while assuring that friendly forces have unfettered access.

Propagation Direction: The “Right Hand Rule”

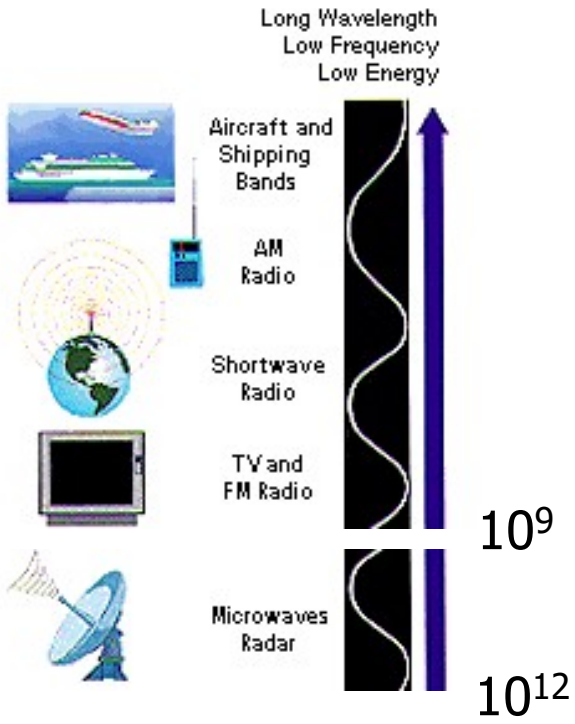
Put your right hand out like you are going to shake someone’s hand, with your fingers pointing directly forward and your thumb pointing straight up.

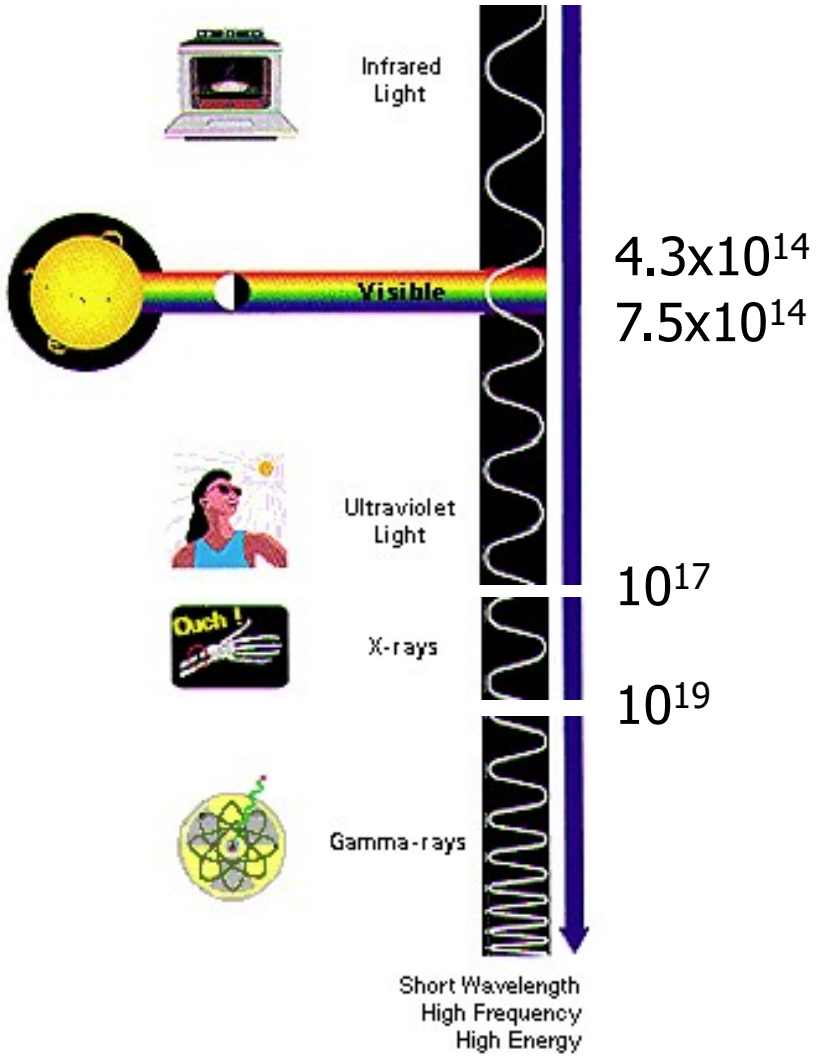
The direction of your fingers represents the positive direction of the electric field. The direction of your thumb represents the direction of travel of the radiated fields.

Which way is the direction of the magnetic field? Simply curl your fingers 90 degrees to the left, and that is the positive direction of the magnetic field.

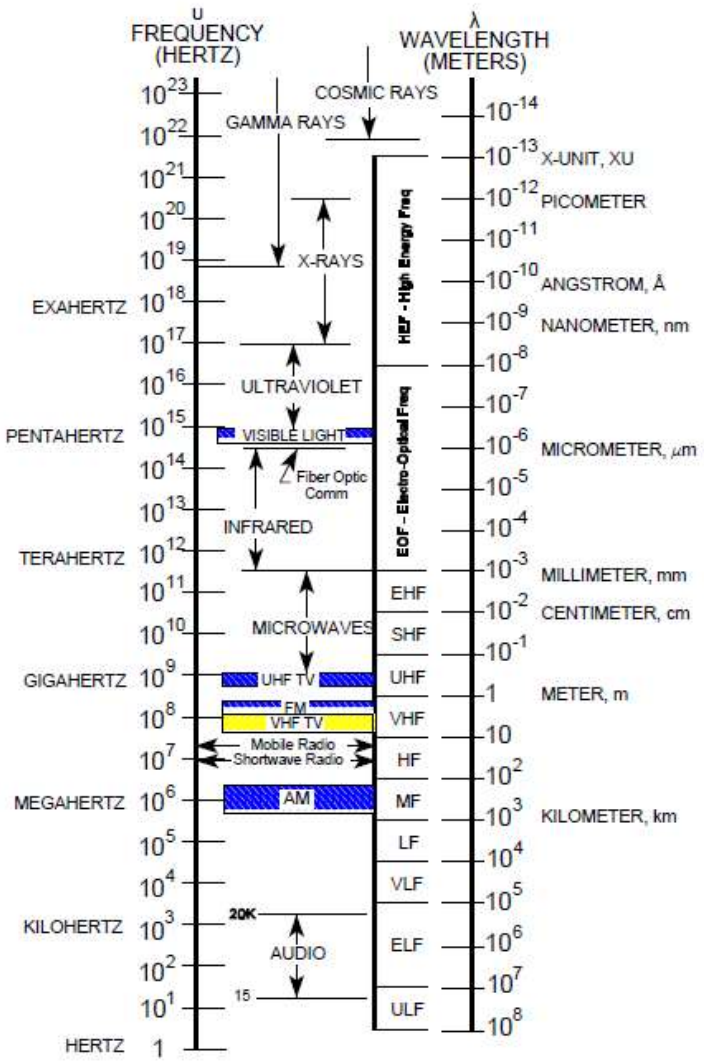


EM Spectrum


Long Wavelength
Low Frequency
Low Energy
Aircraft and Shipping Bands
AM Radio
Shortwave Radio
TV and FM Radio
Microwaves Radar
10^9
10^{12}

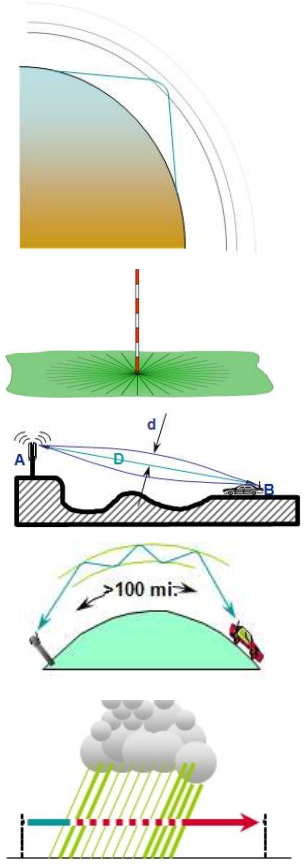

Infrared Light
Visible
4.3×10^{14}
7.5×10^{14}
Ultraviolet Light
10^{17}
Ouch !
X-rays
10^{19}
Gamma-rays
Short Wavelength
High Frequency
High Energy

Electro Magnetic Spectrum (EMS)



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



Radio Frequencies and How they Propagate: Issues with Rain

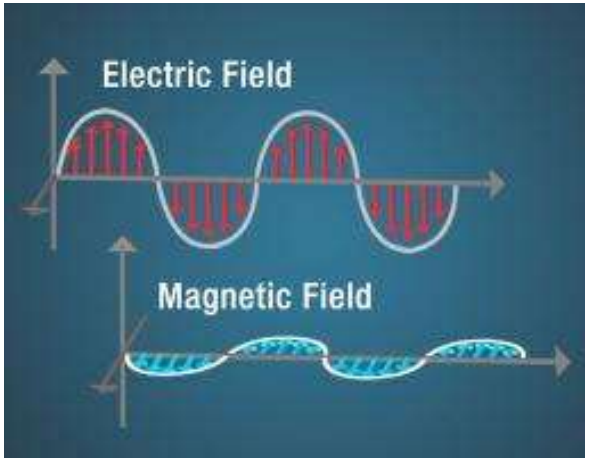
Good for rain

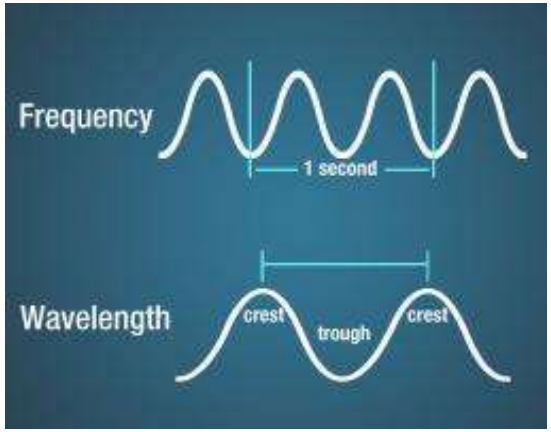
- Bigger antenna
- Less bandwidth
- L-band (1 - 2 GHz)
- S-band (2 - 4 GHz)
- C-band (4 - 8 GHz)

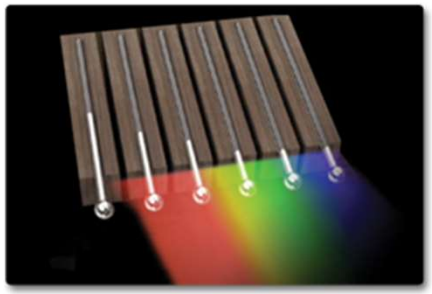
- Not good for rain
  - Smaller antenna
  - Higher bandwidth
  - X-band (8 - 12.5 GHz)
  - Ku-band (12.5 - 18 GHz)
  - K-band (18 - 26.5 GHz)
  - Ka-band (26.5 - 40 GHz)

ELECTROMAGNETIC WAVES

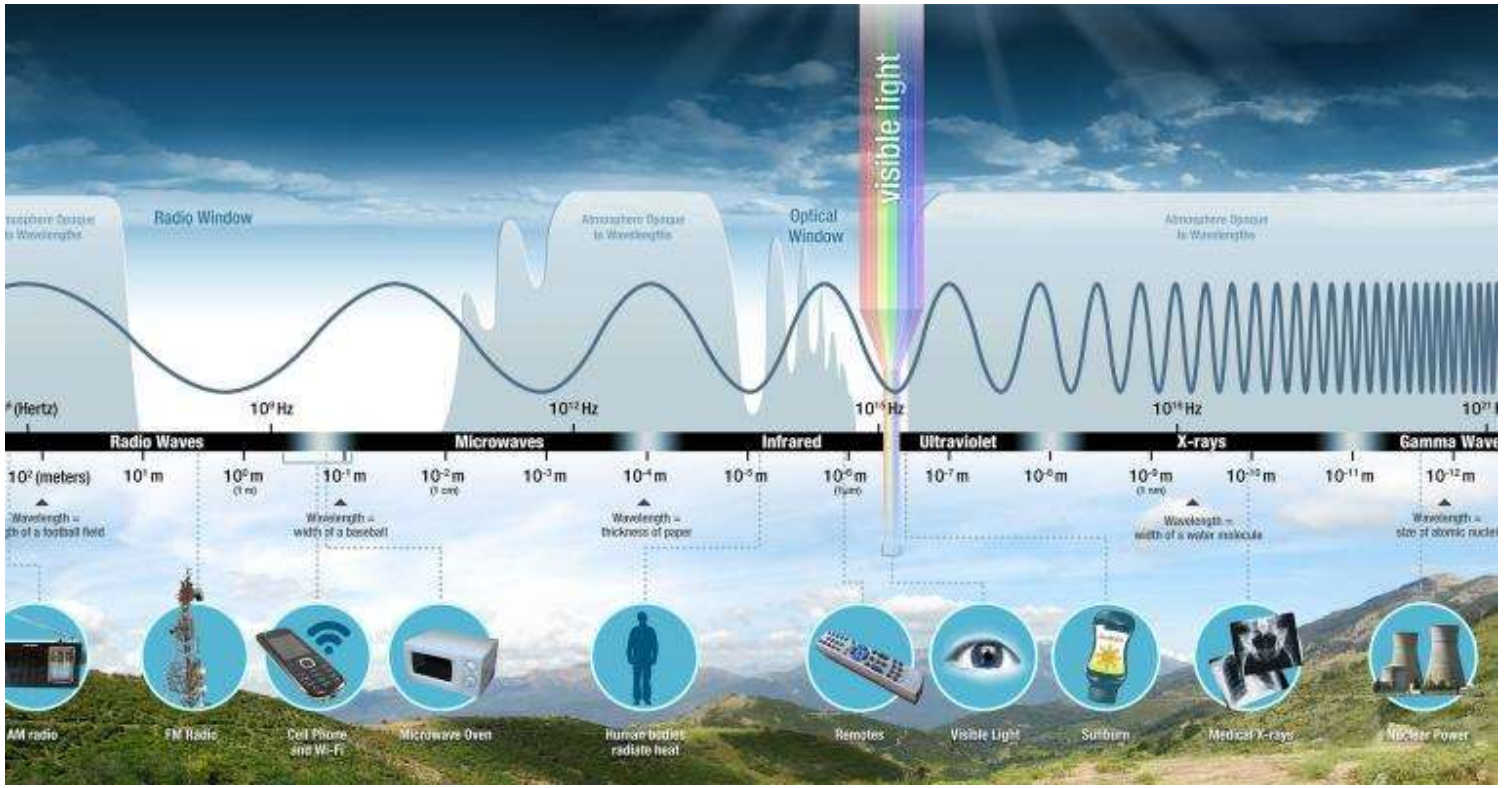
- WAVES OR PARTICLES? YES!
- POLARIZATION
- ELECTROMAGNETIC ENERGY
- FREQUENCY
- WAVELENGTH
- ENERGY







Radio Frequencies and How they Propagate

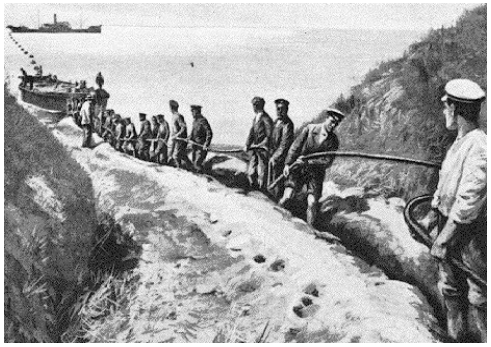


Telegraphy

- Samuel F.B. Morse conceived the telegraph on a sea cruise in the 1833. In 1837 he patented a working prototype.
- The US Congress funded a demonstration line from Washington to Baltimore, completed in 1844.
- 1857: first trans-Atlantic submarine telegraph cable was installed

Samuel F. B. Morse
at peak of his career

MORSE CODE			
A	•–	U	••–
B	– •••	V	•••–
C	– • – •	W	•– –
D	–••	X	–••–
E	•	Y	–•– –
F	••–•	Z	– –••
G	– –•	1	•– – – –
H	••••	2	••– – –
I	••	3	•••– –
J	•– – –	4	••••–
K	– •–	5	•••••
L	•–••	6	–••••
M	– –	7	– –•••
N	–•	8	– – –••
O	– – –	9	– – – –•
P	•– –•	0	– – – – –
Q	– –•–	.	•–•–•–
R	•–•	,	– –••– –
S	•••	?	••—••
T	–	ERR	•••••••



Submarine Cable Installation
news sketch from the 1850's

Field Telegraphy
during the US Civil War, 1860's

Pioneers of Electromagnetics and Radio

Andre-Marie Ampere
1775-1836

Michael Faraday
1791-1867

James Clerk Maxwell
1831-1879

Carl Friedrich Gauss
1777-1855

Georg Simon Ohm
1789-1854

Guglielmo Marconi
1874-1937

We owe much to the gentlemen at left. In honor of their contributions, many of the familiar electromagnetic units bear their names:

Ampere, the unit of current.

Faraday, the unit of capacitance (Farad).

Gauss, the unit of magnetic flux density, “magnetic induction”.

Ohm, the unit of resistance.

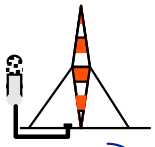
Maxwell whose four equations embody the key principles discovered by the earlier pioneers. They describe and predict every electromagnetic phenomenon known to date.

Marconi was a promoter who led some of the first successful radio experiments aimed at commercial use.

Radio Milestones

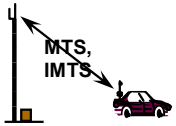
- 1888: Heinrich Hertz, German physicist, gives lab demo of existance of electromagnetic waves at radio frequencies
- 1895: Guglielmo Marconi demonstrates a wireless radio telegraph over a 3-km path near his home it Italy
- 1897: the British fund Marconi's development of reliable radio telegraphy over ranges of 100 kM
- 1902: Marconi's successful trans-Atlantic demonstration

- 1902: Nathan Stubblefield demonstrates voice over radio
- 1906: Lee De Forest invents "audion", triode vacuum tube
  - feasible now to make steady carriers, and to amplify signals



- 1914: Radio became valuable military tool in World War I
- 1920s: Radio used for commercial broadcasting

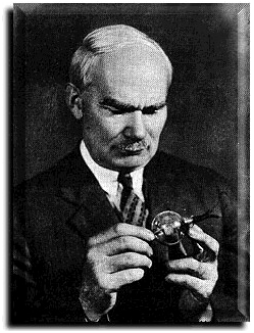
- 1940s: first application of RADAR - English detection of incoming German planes during WW II
- 1950s: first public marriage of radio and telephony - MTS, Mobile Telephone System



- 1961: transistor developed: portable radio now practical
- 1961: IMTS - Improved Mobile Telephone Service
- 1970s: Integrated circuit progress: MSI, LSI, VLSI, ASICs
- 1979, 1983: 1G: AMPS cellular demo, commercial deployment

- 2021: 5G moving towards 6G

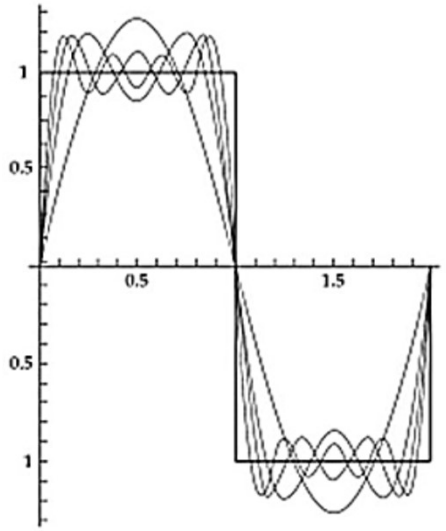
Guglielmo Marconi
radio pioneer, 1895



Lee De Forest
vacuum tube inventor

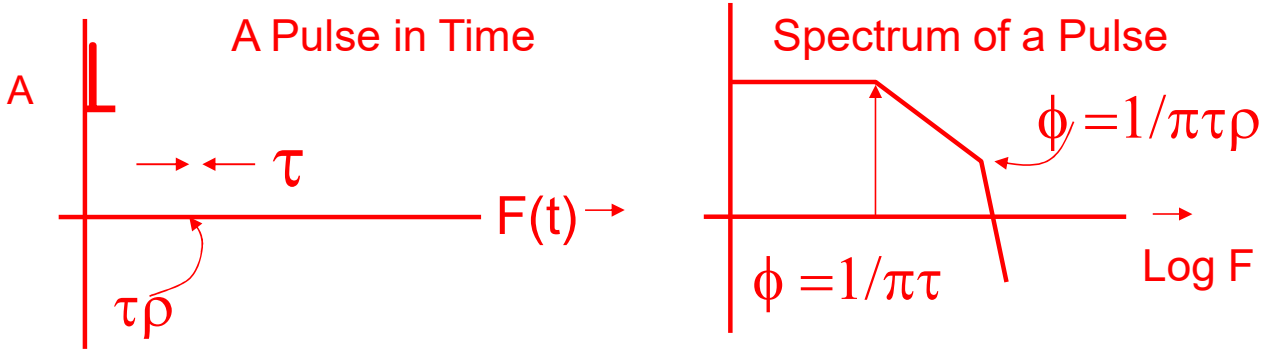
Fourier Analysis:

Understanding the relationship between a waveform and its spectrum

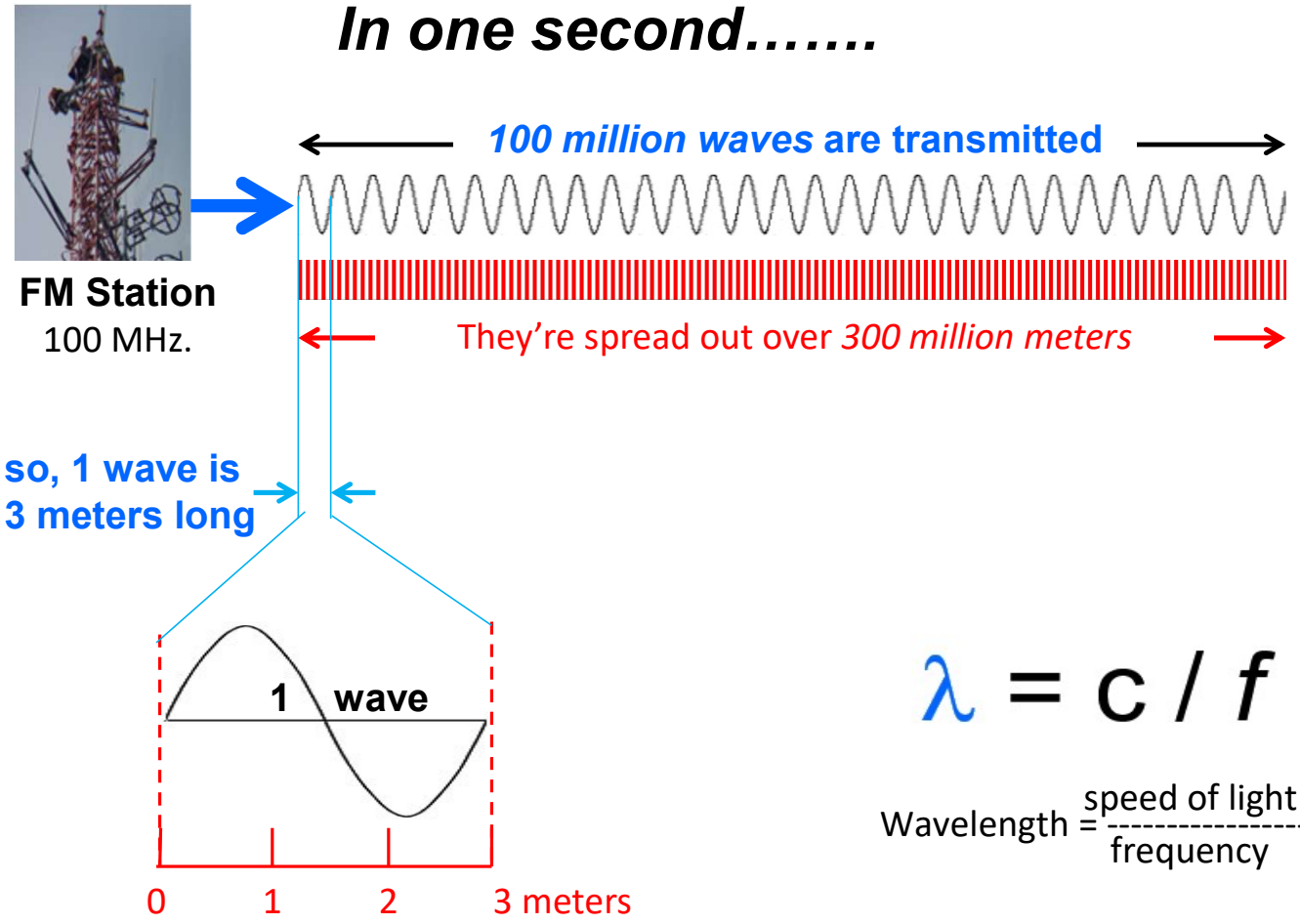


Multiple analog waveforms can be added to produce a square wave.
But notice the higher frequencies involved.
Sharp transitions in a waveform make the signal have a higher bandwidth.

Charles Fourier



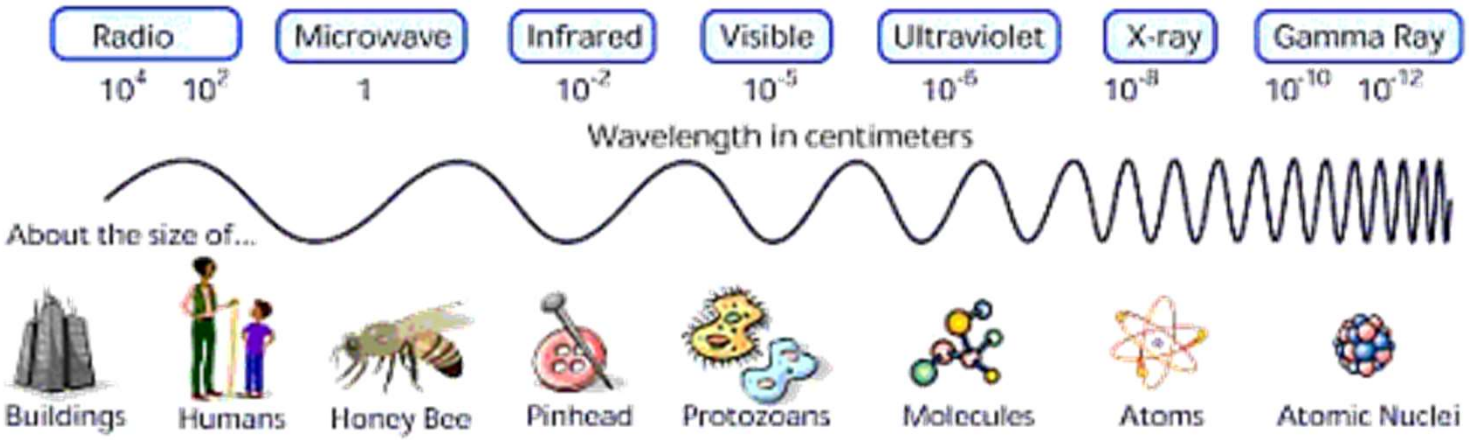
Frequency vs. Wavelength



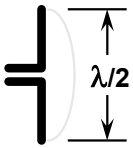
$$\lambda = c / f$$

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

The Size of λ (wavelength, 'lambda')



Why does Wavelength Matter?

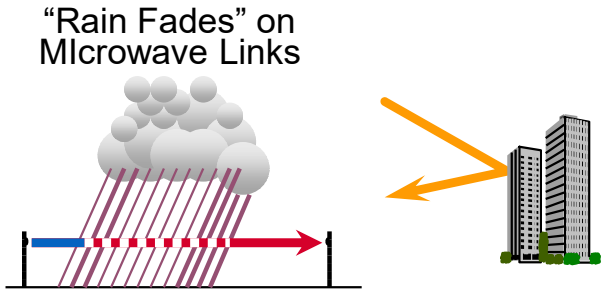


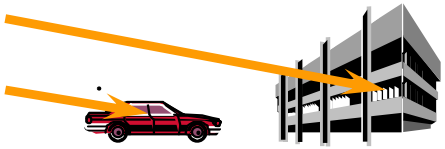
Why do we care about wavelength?

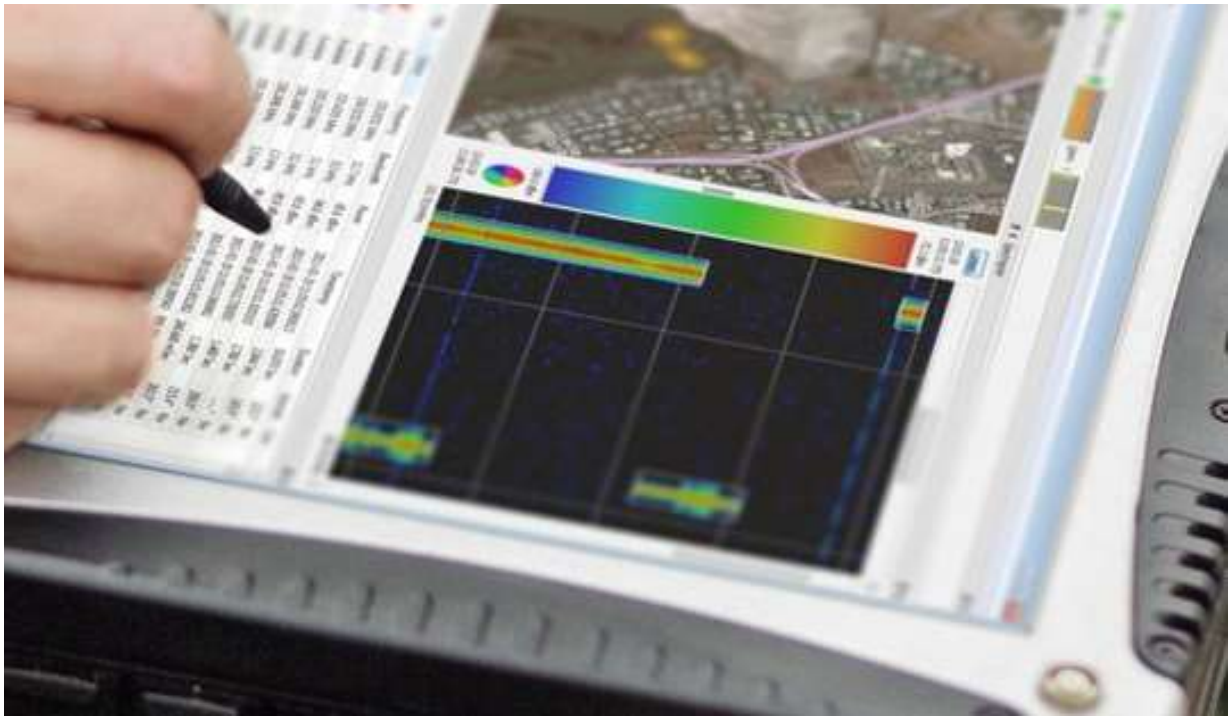
- Transmitting antennas must be at least ¼ wavelength long to be efficient

- Objects much smaller than a wavelength ***do not*** block or absorb radio waves; objects larger than a wavelength ***do***

- In order for radio waves to enter an enclosed space, it must have holes at least ¼ wave diameter. The larger, the better







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.

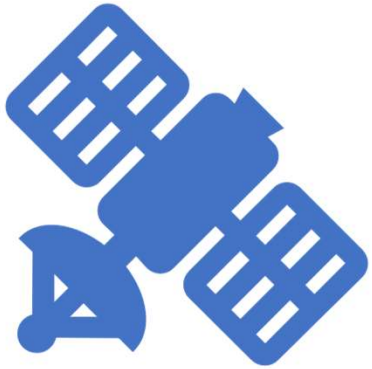
- SIGINT system combines precision RF, SDR and Direction Finding (DF) hardware with the next generation of the software.

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

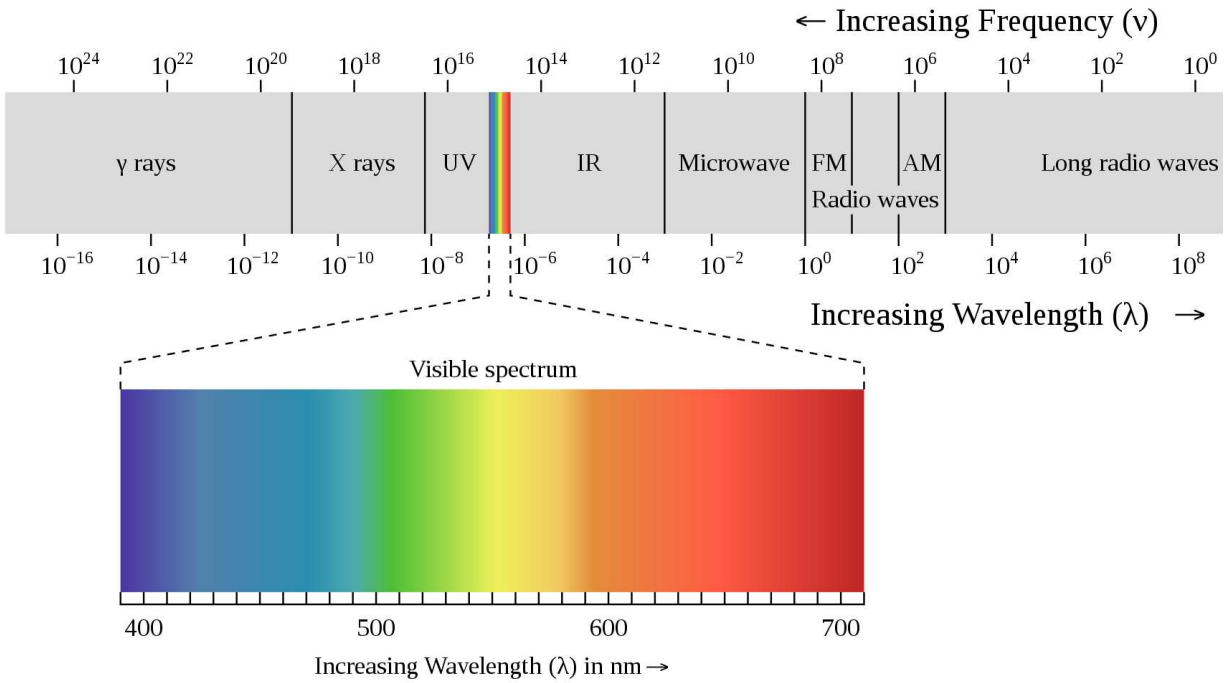
Communication Technologies



- Wireline
  - Cable: twisted pair and coax cable
  - Fiber Optics

- Wireless
  - RF
  - Microwave
  - mmWave
  - Infrared
  - Visible Light

Visible Light Communication (VLC)

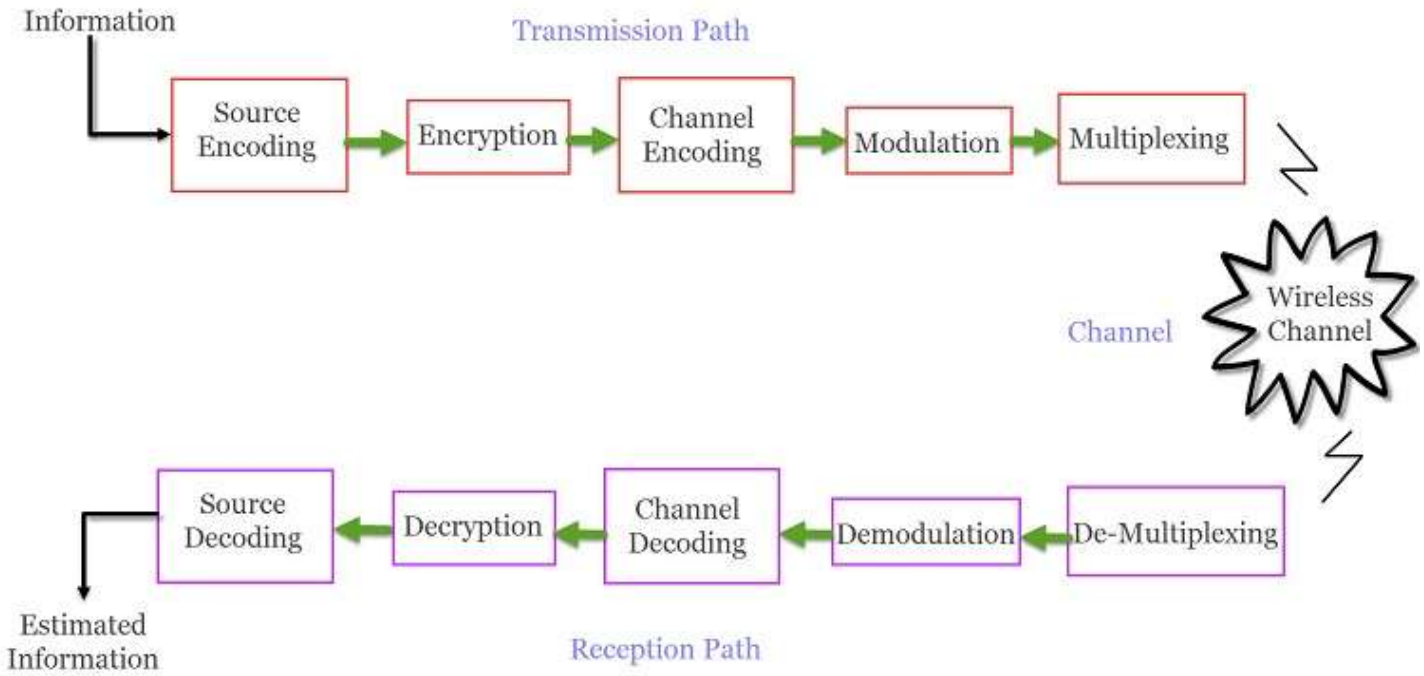


- Visible light communication (VLC) is a data communications variant which uses visible light between 400 and 800 THz (780–375 nm).
- VLC is a subset of optical wireless communications technologies.

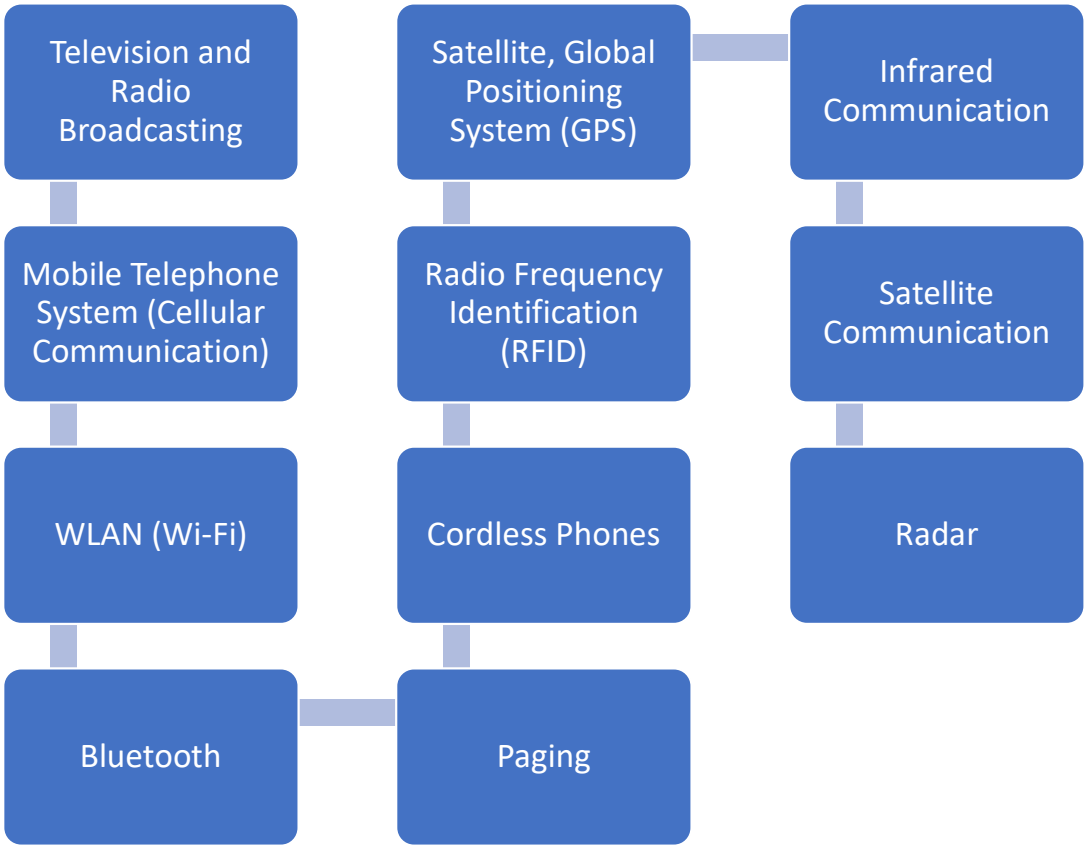
Free-Space Optical Communication (FSO)


MRV
Free Space Optics Laser

Basic Elements of a Wireless Communication System



Types of Wireless Communication Systems



Wireless Communication

- If there is no physical medium, then how does wireless communication transmit signals? Even though there are no cables used in wireless communication, the transmission and reception of signals is accomplished with Antennas.

- Antennas are electrical devices that transform the electrical signals to radio signals in the form of Electromagnetic (EM) Waves and vice versa.

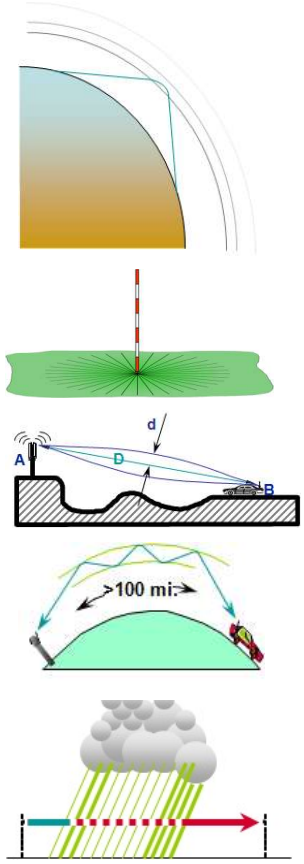
- These Electromagnetic Waves propagates through space. Hence, both transmitter and receiver consists of an antenna.

- Electromagnetic Waves carry the electromagnetic energy of electromagnetic field through space. Electromagnetic Waves include Gamma Rays (γ – Rays), X – Rays, Ultraviolet Rays, Visible Light, Infrared Rays, Microwave Rays and Radio Waves.

- Electromagnetic Waves (usually Radio Waves) are used in wireless communication to carry the signals.

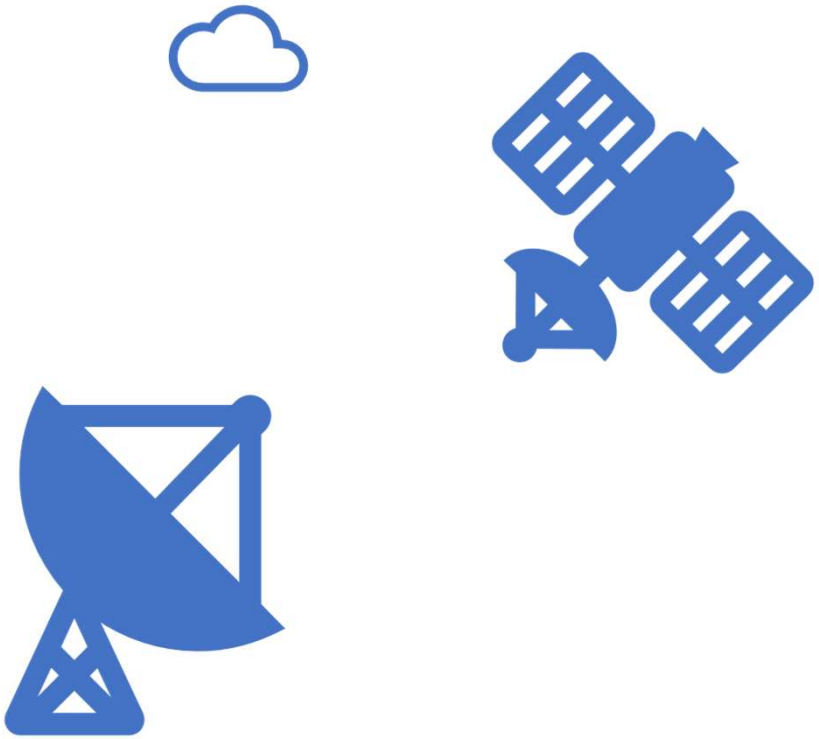
COMINT and ELINT RF, Microwave and mmWave Frequencies

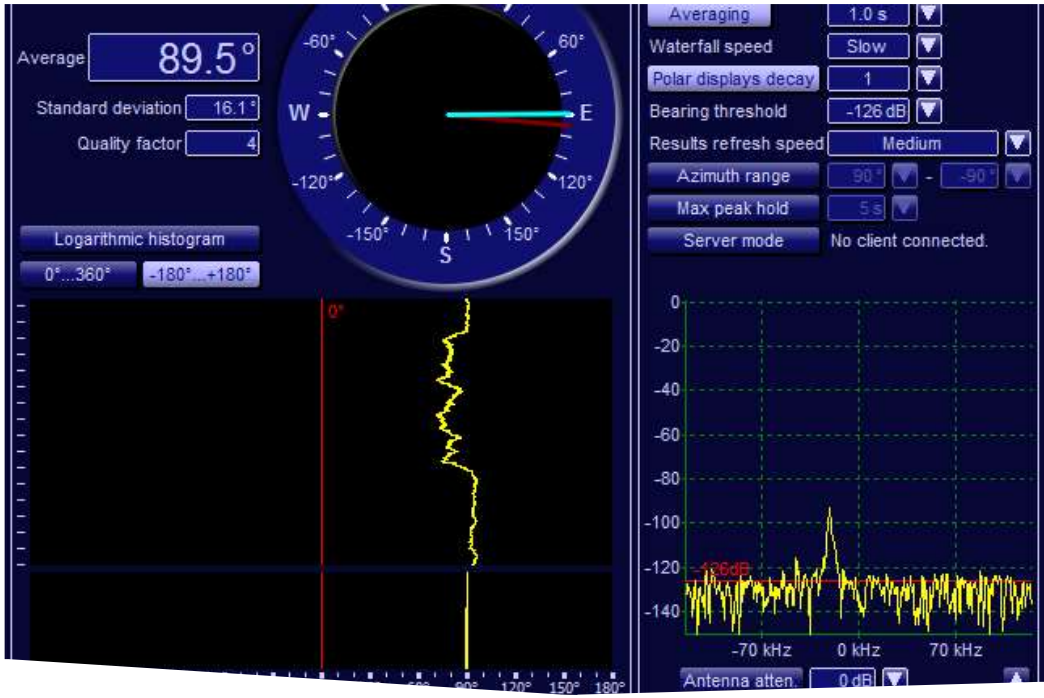
Band Name		Freq.	Length	Example Uses	How Signal Propagates
ELF	Extremely Low Frequency	3 – 300 Hz.	100,000 – 1,000 KM.	Inductive coupling to trace wiring in walls, etc.; AC mains power to users	No practical propagation outside the conducting wires
VLF	Very Low Frequency	3 – 30 KHz.	100 – 10 KM.	100+ 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



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.





SIGINT ISR Capability

- Full-band Signals Intelligence (SIGINT)

COMINT Signals of Interest (SOIs)

- VHF/UHF SIGINT signal survey, search, detection, visualization, collection, wideband recording, DF/geolocation, analysis and reporting.
- Scanning the RF spectrum, detecting and cataloging all signal activity.
- Spectrogram and map views

COMINT Signals of Interest (SOIs)

- Voice communications
- Data
- Text
- Video

- Cellular Networks
  - 2G, 3G, 4G and 5G
- Land mobile radio system (LMRS)
  - A person-to-person voice communication system consisting of two-way radio transceivers (an audio transmitter and receiver in one unit) which can be stationary (base station units), mobile (installed in vehicles), or portable (handheld walkie-talkies).
- High Power Cordless Phones

VHF/UHF/SHF COMINT

- Integrated Signal Search
- VHF/UHF/SHF Signal Search, Collection
- Direction finding (DF)/Geolocation & Analysis System
- Hybrid AOA/TDOA geolocation systems

Radio Direction Finding (RDF or DF)

- Humans do audio direction finding to a remarkable precision of less than two degrees.

- Shortly after the development of radio transmitters and receivers, radio direction finding (RDF or just DF) evolved for much the same reasons as human audio direction finding: firstly, for the location of possible threats and secondly for spatial awareness.

Electronic warfare Soldiers train with radio direction finding system

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

Source:

https://www.army.mil/article/203723/electronic_warfare_soldiers_train_with_radio_direction_finding_system

VHF/UHF/SHF DF and Spectrum Monitoring Antenna

VHF/UHF DF and Spectrum Monitoring Antenna: 20 to 3,000 MHz

Monopole HF DF and Spectrum Monitoring Antenna

- HF DF Spectrum Monitoring Antenna, which features a 5-meter (16-ft) monopole, provides high signal sensitivity over the entire HF range.

SHF Vertically-Polarized Monitoring Antenna

Spectrum monitoring systems vertical polarization coverage from 3 GHz to 8.5 GHz.

Spectrum Monitoring and COMINT DF

- ITU-compliant spectrum monitoring system interface
- RECOMMENDATION ITU-R SM.1537

- https://www.itu.int/dms_pubrec/itu-r/rec/sm/R-REC-SM.1537-0-200107-S!!PDF-E.pdf

COMINT/DF for Unmanned Aircraft System (UAS)

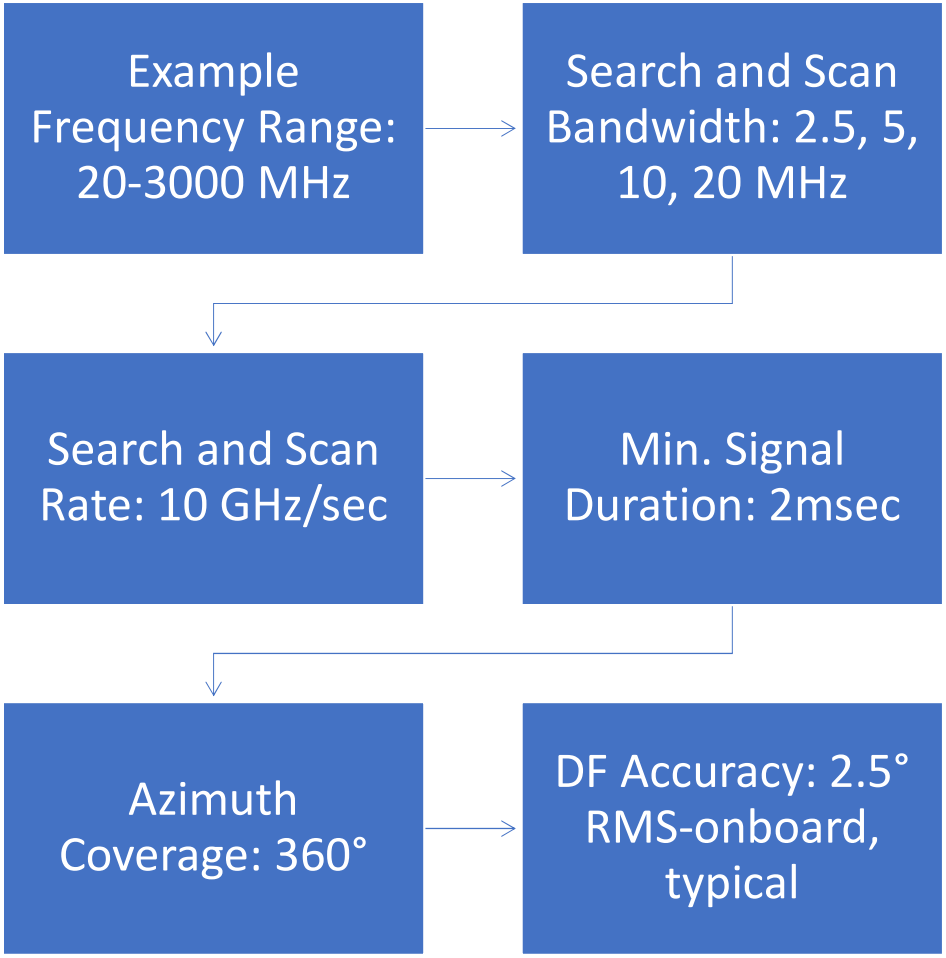
- Frequency Band: 30-1200MHz (option 30 to 3000MHz)
- Types of Detected Signals: FM, WFM, NFM, AM, CW, SSB

Man-Pack COMINT/DF

- Frequency Band: 25-3000MHz
- Shock and Vibration: MIL-STD-810G/H
- Antenna Type: 90° front sector (homing)
- Bandwidth Resolution: 25 kHz typical
- Max. Signal at Input (no damage) +20dBm
- Power Consumption: 40W (excluding PDA)
- Weight: 14 kg excluding vest

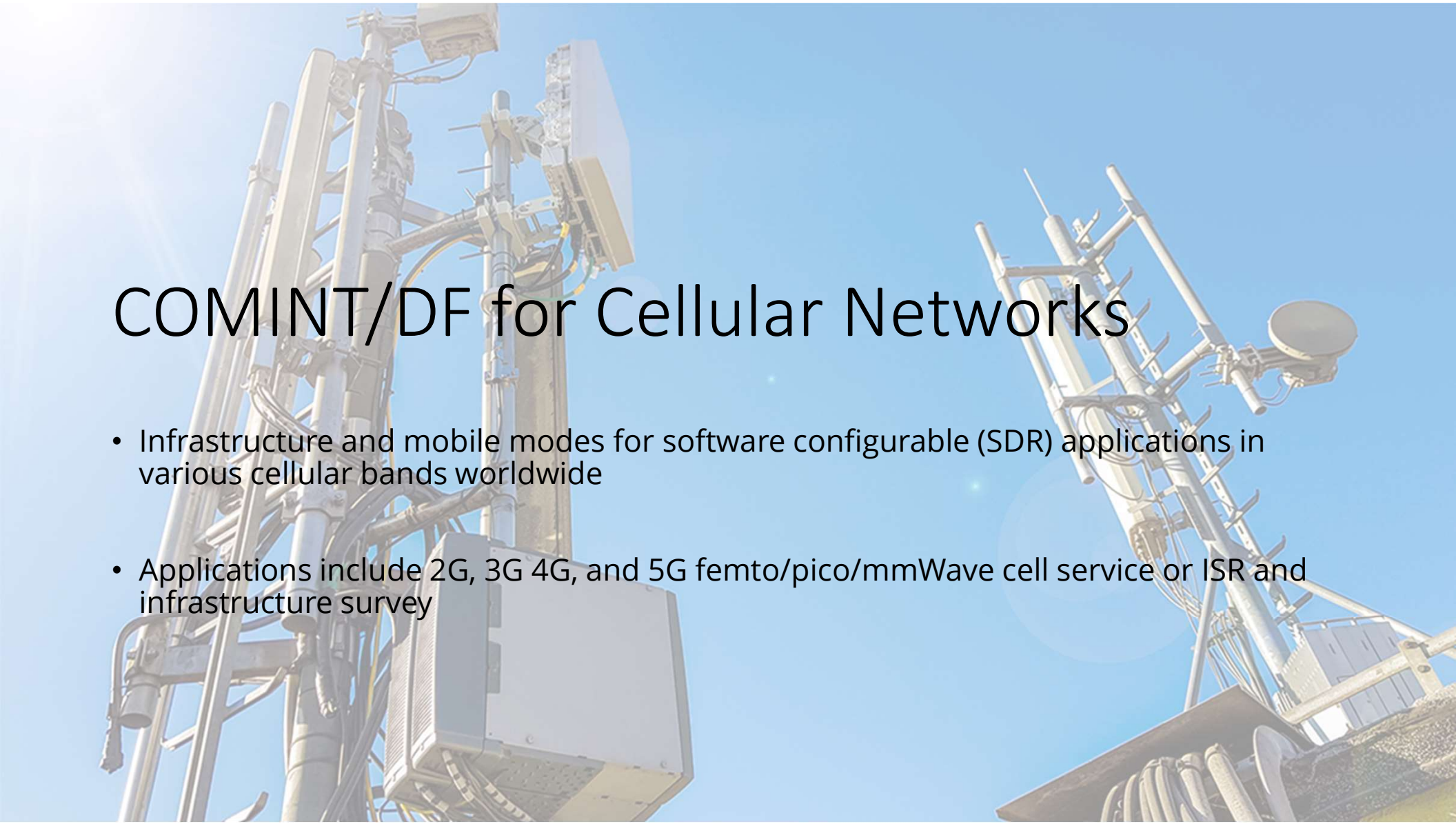
Man-Pack COMINT/DF

Example of COMINT/DF for Transport and Mission Aircraft



Example of Vehicular, Stationary & Portable COMINT/DF

- Frequency Range: 30 MHz-3 GHz (6 GHz optional)
- Azimuth Coverage: 360°
- Accuracy in Azimuth: 2° - 3.5° RMS typical
- Scanning Speed: 2000 channel/sec



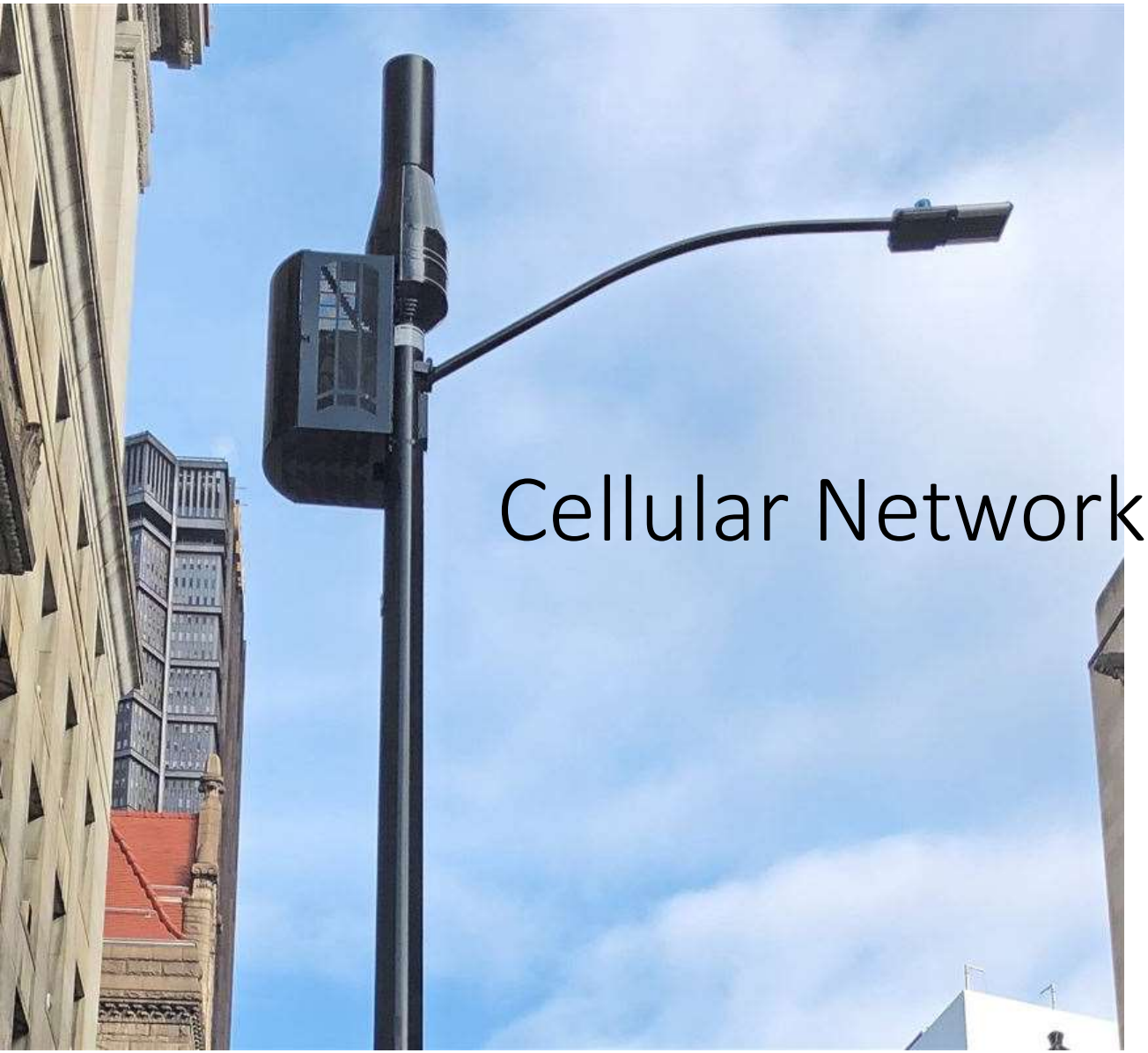
COMINT/DF for Cellular Networks

- Infrastructure and mobile modes for software configurable (SDR) applications in various cellular bands worldwide
- Applications include 2G, 3G 4G, and 5G femto/pico/mmWave cell service or ISR and infrastructure survey

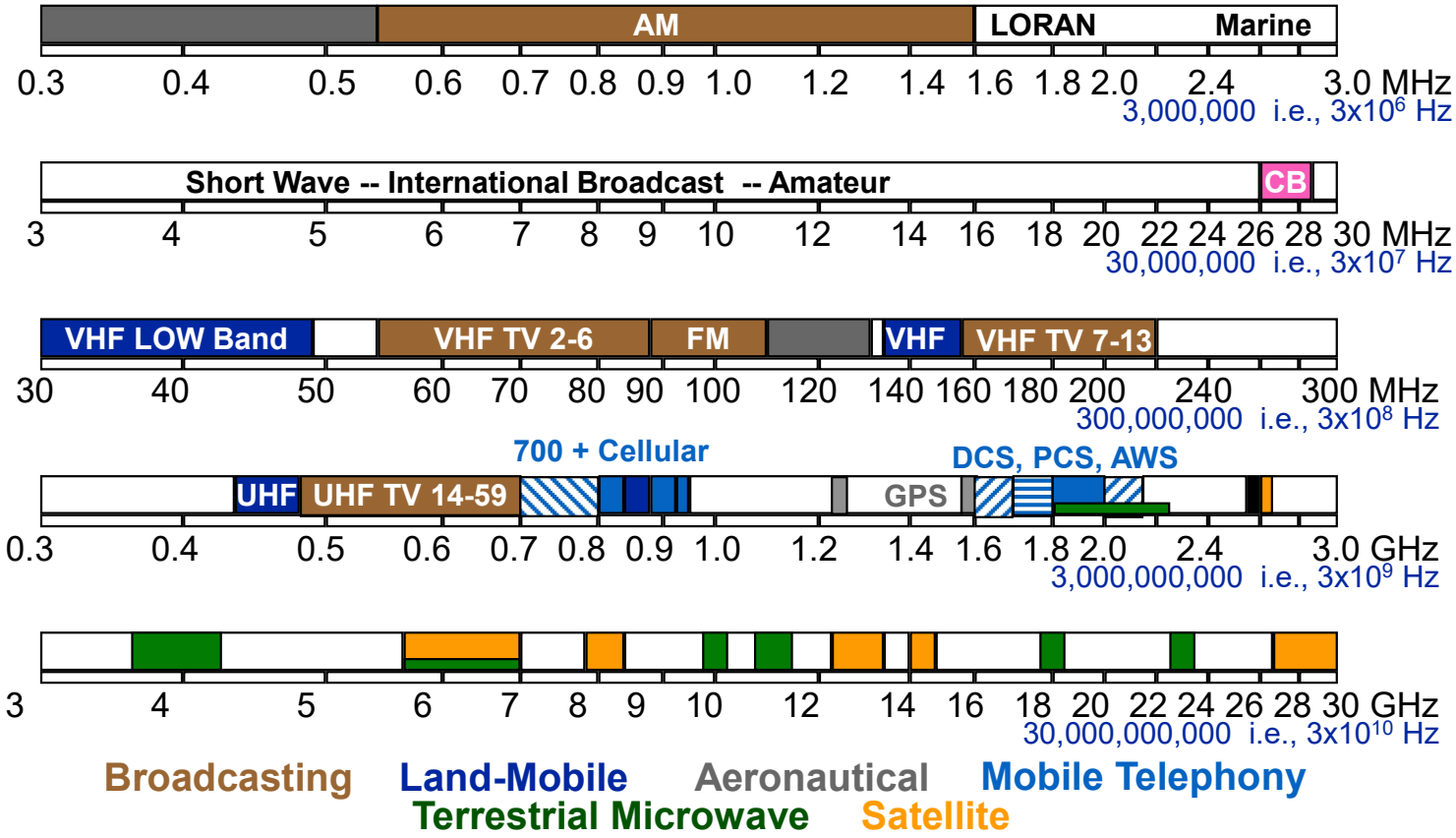
Example of COMINT/DF for Cellular Networks

- Full coverage from HF to V/UHF to deal with all targets
- Wideband capacity and fast scanning speed providing high probability of interception able to cope with most agile signals
- High DF accuracy
- Wide range of DF antennas for fixed and tactical applications
- High Performance V/UHF Interceptor and Direction Finder
- Frequency band: 20-3800 MHz

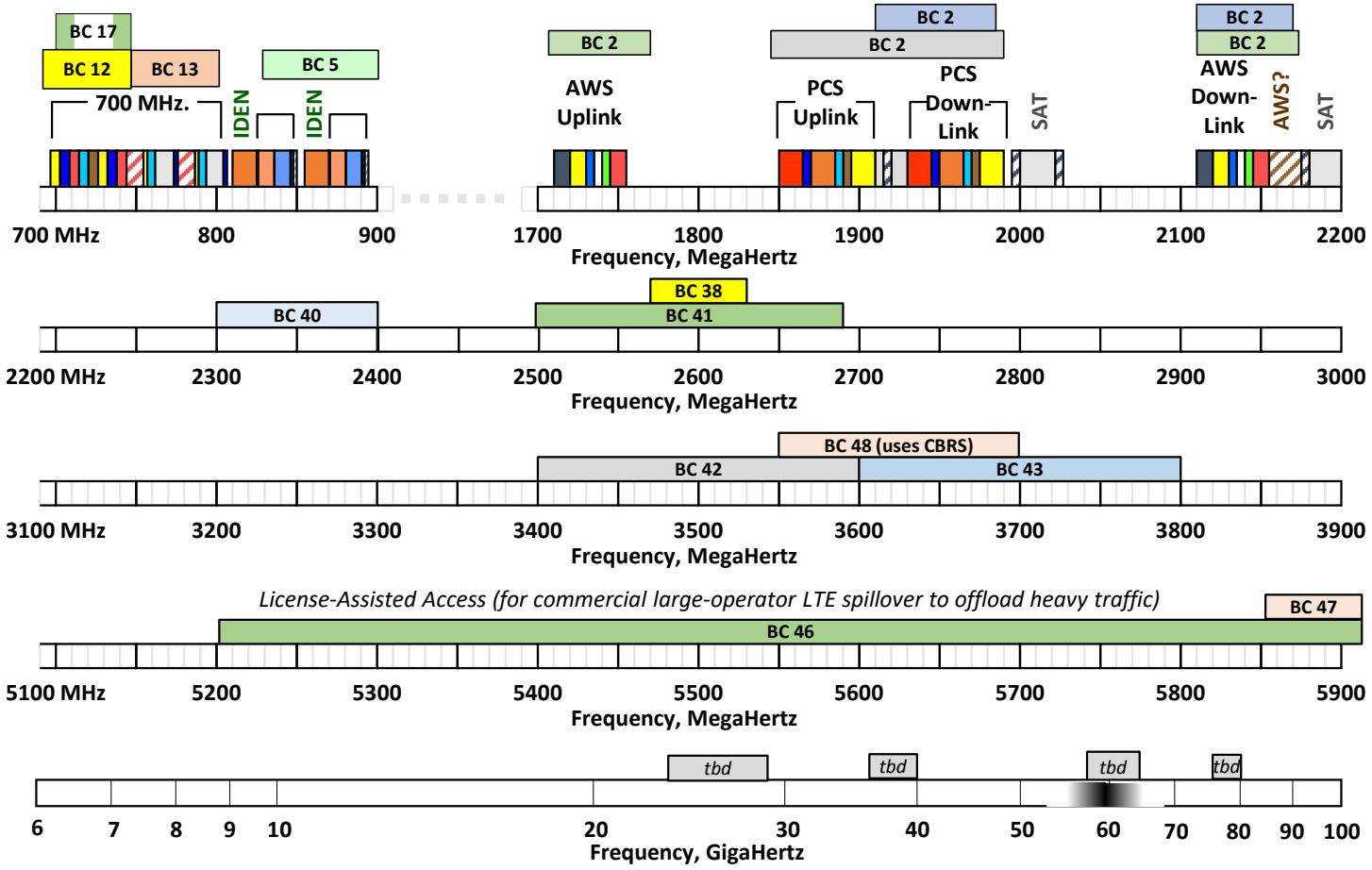
Cellular Networks



Frequencies Used by Wireless Systems: Overview of the Cellular Spectrum



Frequencies of Public Wireless/Cellular 1G-5G Networks



Band Classes from 3GPP Standards (1 of 2)

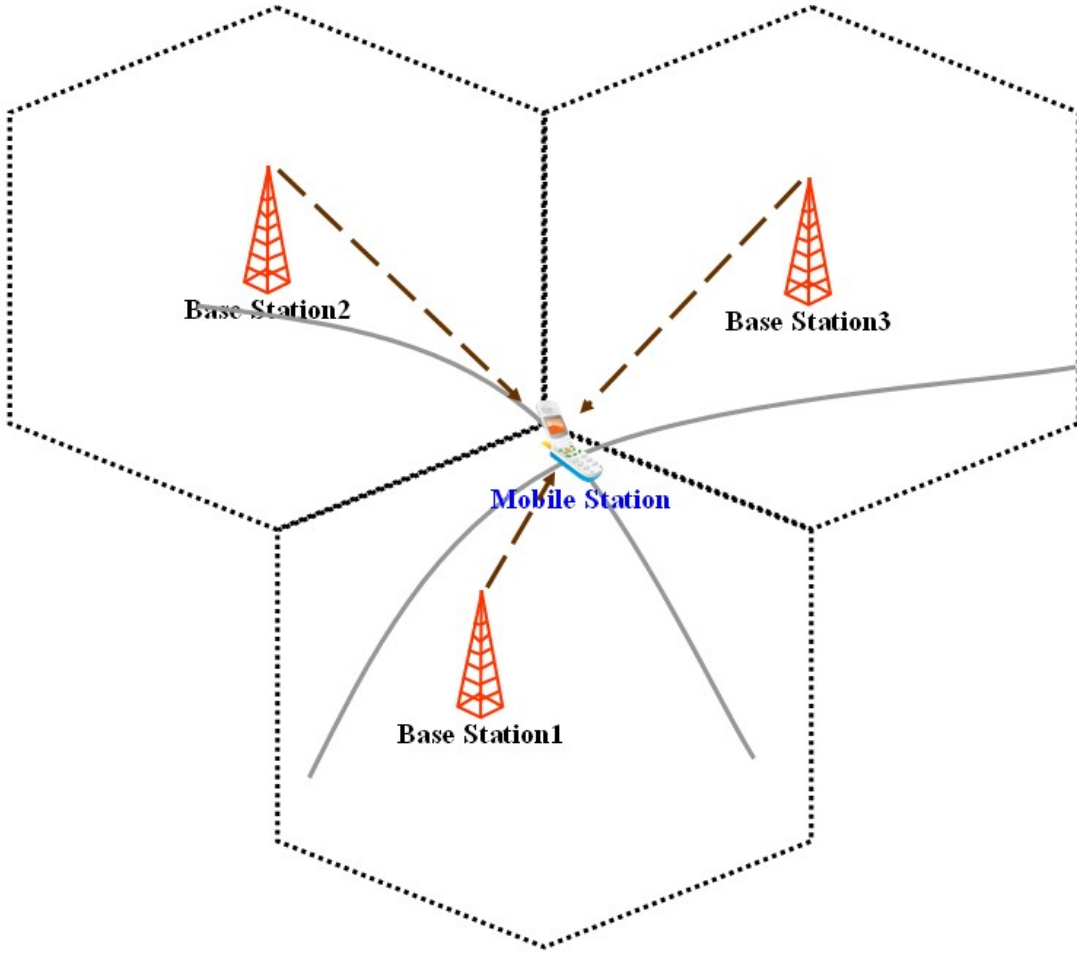
Band Class	Duplex Mode	Freq Band	Common Name	Includes Bandclass	Uplink	Downlink	Duplex Spacing	Channel Bandwidths
1	FDD	2100	IMT	*65*	1920 – 1980	2110 – 2170	190	5, 10, 15, 20
2	FDD	1900	PCS blocks A-F	*25*	1850 – 1910	1930 – 1990	80	1.4, 3, 5, 10, 15, 20
3	FDD	1800	DCS		1710 – 1785	1805 – 1880	95	1.4, 3, 5, 10, 15, 20
4	FDD	1700	AWS blocks A-F (AWS-1)	*66*	1710 – 1755	2110 – 2155	400	1.4, 3, 5, 10, 15, 20
5	FDD	850	CLR	*26*	824 – 849	869 – 894	45	1.4, 3, 5, 10
7	FDD	2600	IMT-E		2500 – 2570	2620 – 2690	120	5, 10, 15, 20
8	FDD	900	E-GSM		880 – 915	925 – 960	45	1.4, 3, 5, 10
10	FDD	1700	Extended AWS blocks A-I	*66*	1710 – 1770	2110 – 2170	400	5, 10, 15, 20
11	FDD	1500	Lower PDC		1427.9 – 1447.9	1475.9 – 1495.9	48	5, 10
12	FDD	700	Lower SMH blocks A/B/C		699 – 716	729 – 746	30	1.4, 3, 5, 10
13	FDD	700	Upper SMH block C		777 – 787	746 – 756	−31	5, 10
14	FDD	700	Upper SMH block D		788 – 798	758 – 768	−30	5, 10
17	FDD	700	Lower SMH blocks B/C	*12*	704 – 716	734 – 746	30	5, 10
18	FDD	850	Japan lower 800	*26*	815 – 830	860 – 875	45	5, 10, 15
19	FDD	850	Japan upper 800	*26*	830 – 845	875 – 890	45	5, 10, 15
20	FDD	800	EU Digital Dividend		832 – 862	791 – 821	−41	5, 10, 15, 20
21	FDD	1500	Upper PDC		1447.9 – 1462.9	1495.9 – 1510.9	48	5, 10, 15
22	FDD	3500			3410 – 3490	3510 – 3590	100	5, 10, 15, 20
24	FDD	1600	L-Band (US)		1626.5 – 1660.5	1525 – 1559	−101.5	5, 10
25	FDD	1900	Extended PCS blocks A-G		1850 – 1915	1930 – 1995	80	1.4, 3, 5, 10, 15, 20
26	FDD	850	Extended CLR		814 – 849	859 – 894	45	1.4, 3, 5, 10, 15
27	FDD	800	SMR (adjacent to band 5)		807 – 824	852 – 869	45	1.4, 3, 5, 10
28	FDD	700	APT		703 – 748	758 – 803	55	3, 5, 10, 15, 20
29	FDD	700	Lower SMH blocks D/E		*N/A*	717 – 728	*N/A*	3, 5, 10
30	FDD	2300	WCS blocks A/B		2305 – 2315	2350 – 2360	45	5, 10
31	FDD	450			452.5 – 457.5	462.5 – 467.5	10	1.4, 3, 5

Band Classes from 3GPP Standards (2 of 2)

Band Class	Duplex Mode	Freq Band	Common Name	Includes Bandclass	Uplink	Downlink	Duplex Spacing	Channel Bandwidths
32	FDD	1500	L-Band (EU)		*N/A*	1452 – 1496	*N/A*	5, 10, 15, 20
33	TDD	2100	IMT	*39*	1900 – 1920	(TDD)	*N/A*	5, 10, 15, 20
34	TDD	2100	IMT		2010 – 2025	(TDD)	*N/A*	5, 10, 15
35	TDD	1900	PCS (Uplink)		1850 – 1910	(TDD)	*N/A*	1.4, 3, 5, 10, 15, 20
36	TDD	1900	PCS (Downlink)		1930 – 1990	(TDD)	*N/A*	1.4, 3, 5, 10, 15, 20
37	TDD	1900	PCS (Duplex spacing)		1910 – 1930	(TDD)	*N/A*	5, 10, 15, 20
38	TDD	2600	IMT-E (Duplex Spacing)	*41*	2570 – 2620	(TDD)	*N/A*	5, 10, 15, 20
39	TDD	1900	DCS-IMT gap		1880 – 1920	(TDD)	*N/A*	5, 10, 15, 20
40	TDD	2300			2300 – 2400	(TDD)	*N/A*	5, 10, 15, 20
41	TDD	2500	BRS / EBS		2496 – 2690	(TDD)	*N/A*	5, 10, 15, 20
42	TDD	3500			3400 – 3600	(TDD)	*N/A*	5, 10, 15, 20
43	TDD	3700			3600 – 3800	(TDD)	*N/A*	5, 10, 15, 20
44	TDD	700	APT		703 – 803	(TDD)	*N/A*	3, 5, 10, 15, 20
45	TDD	1500	L-Band (China)		1447 – 1467	(TDD)	*N/A*	5, 10, 15, 20
46	TDD	5200	U-NII		5150 – 5925	(TDD)	*N/A*	
47	TDD	5900	U-NII-4 (V2X)		5855 – 5925	(TDD)	*N/A*	
48	TDD	3600	CBRS		3550 – 3700	(TDD)	*N/A*	
65	FDD	2100	Extended IMT		1920 – 2010	2110 – 2200	190	5, 10, 15, 20
66	FDD	1700	Extended AWS blocks A-J		1710 – 1780	2110 – 2200	400	1.4, 3, 5, 10, 15, 20
67	FDD	700	EU 700		*N/A*	738 – 758	*N/A*	5, 10, 15, 20
68	FDD	700	ME 700		698 – 728	753 – 783	55	5, 10, 15
69	FDD	2600	IMT-E (Duplex spacing)		*N/A*	2570 – 2620	*N/A*	5
70	FDD	2000	AWS-4		1695 – 1710	1995 – 2020	295/300	5, 10, 15
71	FDD	600	US Digital Dividend		663 – 698	617 – 652	−46	5, 10, 15, 20
72	FDD	450	PMR/PAMR Europe		451 – 456	461 – 466	10	1.4, 3, 5

Time Delay of Arrival (TDOA)

- Although the phased array is an active search system requiring the user to manipulate the antenna, the TDOA system is ideal for a passive search.
- This means that the TDOA can be mounted on a tripod, tower, vehicle, boat, or aircraft and identify a line of bearing to the radio signal without user manipulation.
- As the antenna is active, it collects data from 360 degrees and uses the same mapping software as the phased array system.



TDOA (*Time Difference Of Arrival*), also known as multilateration, is a well-established technique for the geolocation of RF emitters. Using three or more receivers, TDOA algorithms locate a signal source from the different arrival times at the receivers.

The Overall Geolocation Accuracy

- TDOA can provide valuable data continuously, it does not necessarily replace the phased array.
- The main difference between the systems is the level of accuracy: TDOA is approximately five degrees; phased array is approximately two degrees.
- This is important as a rescue operation is being fine-tuned or a search is conducted at long range where the difference between two and five degrees can grow to 100 meters or more.

How Accurate is TDOA?

- Factor 1: Timing accuracy
- Factor 2: Sample rate and bandwidth
- Factor 3: Signal Periodicity
- Factor 4: Network geometry
- Factor 5: Obstacles

Timing Accuracy

- Precise synchronization between receivers is essential for achieving high-accuracy TDOA.
- In remote, distributed-receiver networks, timing is usually sourced from GPS (or another positioning network such as GLONASS or BeiDou).
- TDOA accuracy is strongly dependent on the quality of reception: very good GPS conditions allow the synchronization error between receivers to be less than 30 ns RMS, which corresponds to an accuracy of

distance=speed of light×time=3×108m/s×30 ns=9 m

but under typical conditions accuracy will often be limited to a few tens of meters.

Sample Rate and Bandwidth

- The time resolution, and consequently the spatial resolution, you can expect from your TDOA network will depend on the sample rate. For example, sampling a signal at 10 MHz gives a time resolution of

$$\text{time} = 1/\text{frequency} = 110\ \text{MHz} = 0.1\ \mu\text{s}$$

which corresponds to a spatial resolution of

$$\text{distance} = \text{speed of light} \times \text{time} = 3 \times 10^{8}\ \text{m/s} \times 0.1\ \mu\text{s} = 30\ \text{m}<$$

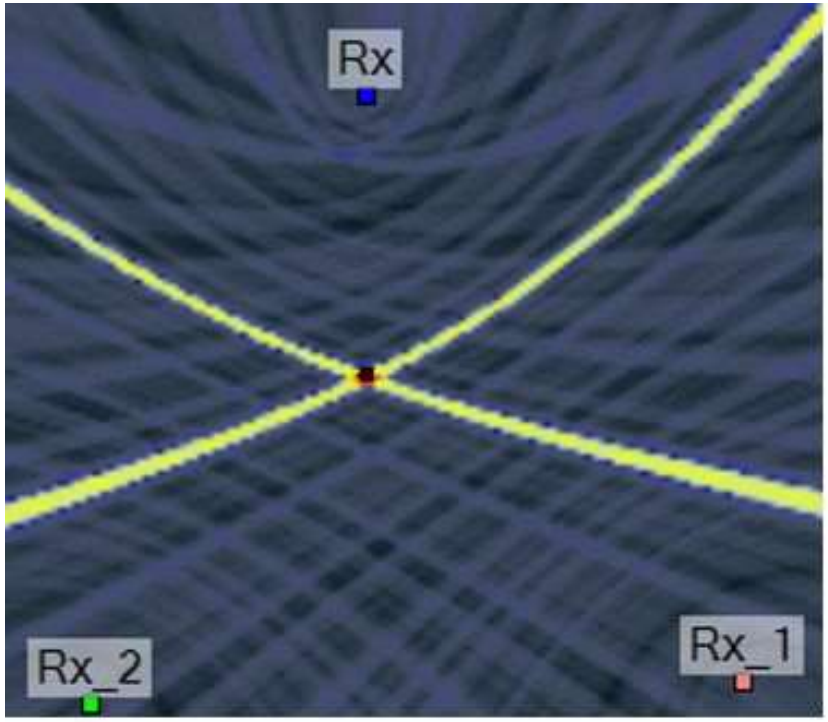
- Unfortunately, it's not just a matter of increasing the sample rate to improve TDOA accuracy.
- If we increase the sample rate much beyond the modulation rate or bandwidth of the signal, we get a law of diminishing returns, as the variations between successive data samples are increasingly related to noise rather than to variations in the signal. The optimal sample rate for TDOA will be comparable with the bandwidth of the signal being geolocated, and the accuracy will be given approximately by

$$\text{accuracy} = \text{speed of light4} \times \text{bandwidth} = 3 \times 10^{8}\ \text{m/s4} \times \text{bandwidth}$$

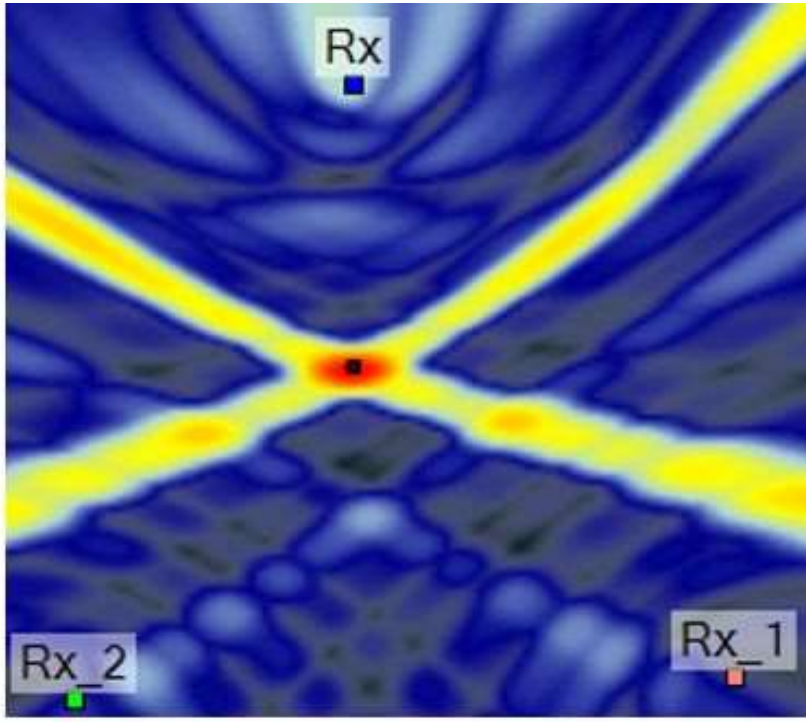
- which is consistent with an accuracy of 10 m at bandwidth 10 MHz, worsening to 100 m at 1 MHz, and 1 km for a bandwidth of 100 kHz.
- The graph below shows how the uncertainty in position decreases as we increase the sample rate, for PSK signals with modulation rates of 8 MHz and 30 MHz.

Time Delay of Arrival (TDOA)

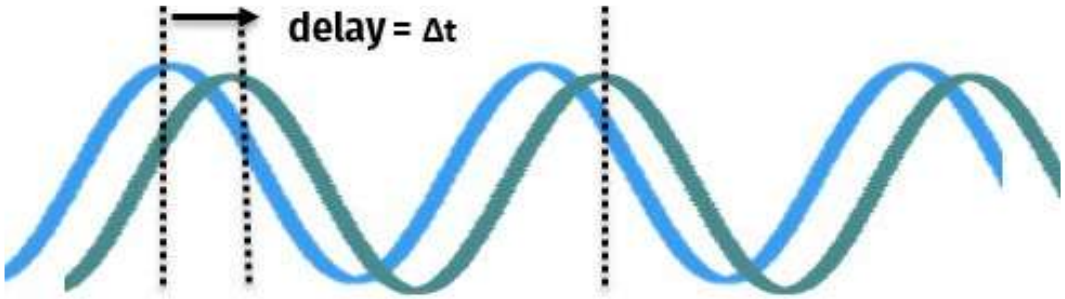
Heatmap



TDOA heatmap for 4 MHz bandwidth signal



TDOA heatmap for 1 MHz bandwidth signal



The curves of different colors represent the same periodic signal at different receivers

Signal Periodicity

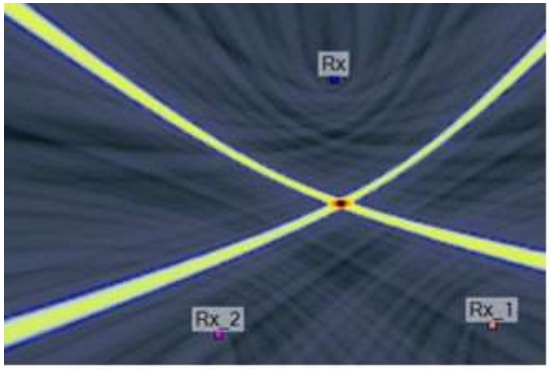
- If a signal is periodic, the cross-correlation function will have more than one peak, corresponding to more than one possible value for the time delay (and therefore the location).
- If more than one location is feasible (which is more likely if the period is short), there will be uncertainty in the geolocation.

Signal Periodicity

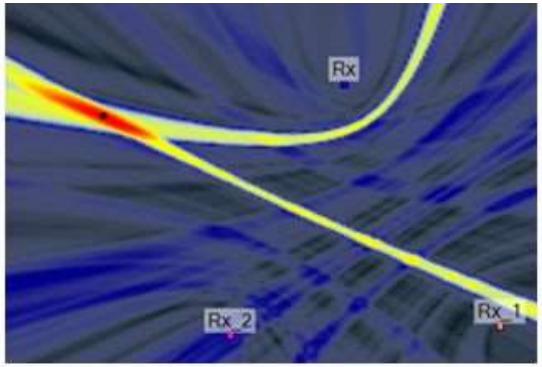
- The distance between possible locations will be of the order $3\times10^{8}\times$period
- so TDOA is likely to be successful if the period is milliseconds or greater (possible locations are hundreds of kilometers apart), and unlikely to be successful if the period is microseconds or less (locations are no more than hundreds of meters apart).

- The worst case is a CW (unmodulated continuous wave) signal, for which TDOA geolocation is unlikely to be useful, except for frequencies below 1 MHz.

- For periodic signals (as also for narrowband signals), AOA geolocation performs much better than TDOA.
- H
- hybrid system combining AOA and TDOA techniques, so that geolocation performance is optimized across all signal types and scenarios.



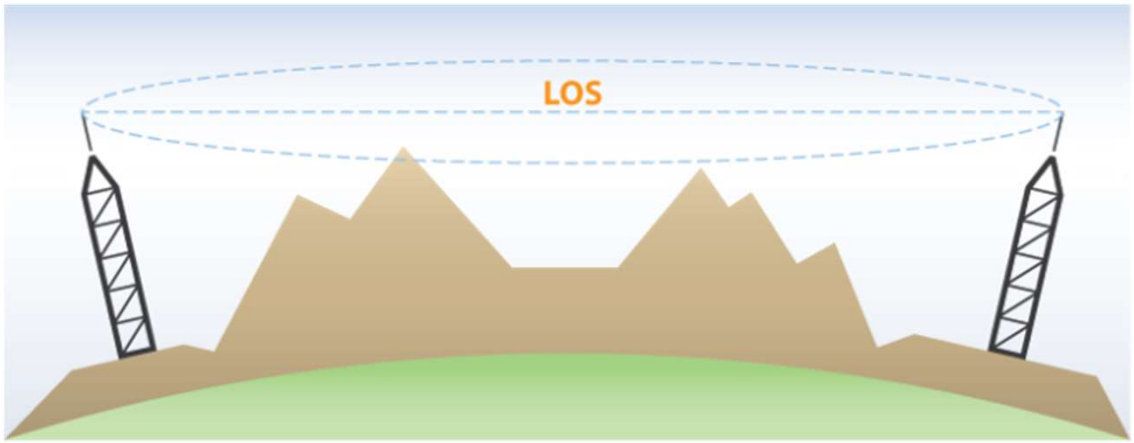
TDOA for bounded transmitter

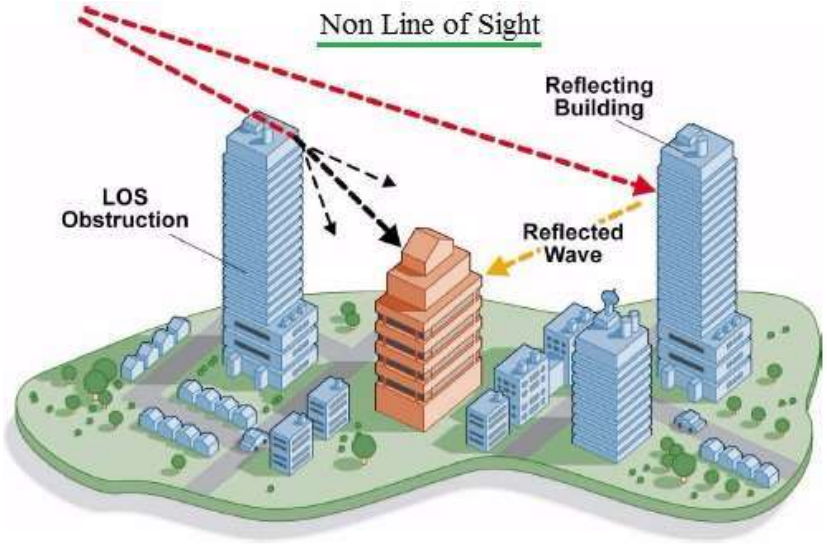


TDOA for unbounded transmitter - reduced accuracy

Network Geometry

- TDOA accuracy is affected by the transmitter location relative to the receiver network, and by the geometry of the network, because of an effect called ‘dilution of precision’.
- The geolocation will be most accurate at a location where a small change in time difference results from a small change in location, and less accurate if a larger change in location is needed to produce the same small change in time difference.
- To a first approximation, the best accuracy will be achieved when the transmitter lies within the envelope of the three (or more) receiver locations.
- Outside this envelope, inaccuracies introduced by other factors will be magnified by the geometry. The two images below show location probability heat maps for transmitters within, and outside, the envelopes.
- The larger, red area for the latter transmitter indicates a greater uncertainty in location. The receivers are near the corners of an equilateral triangle with sides 9 km long.

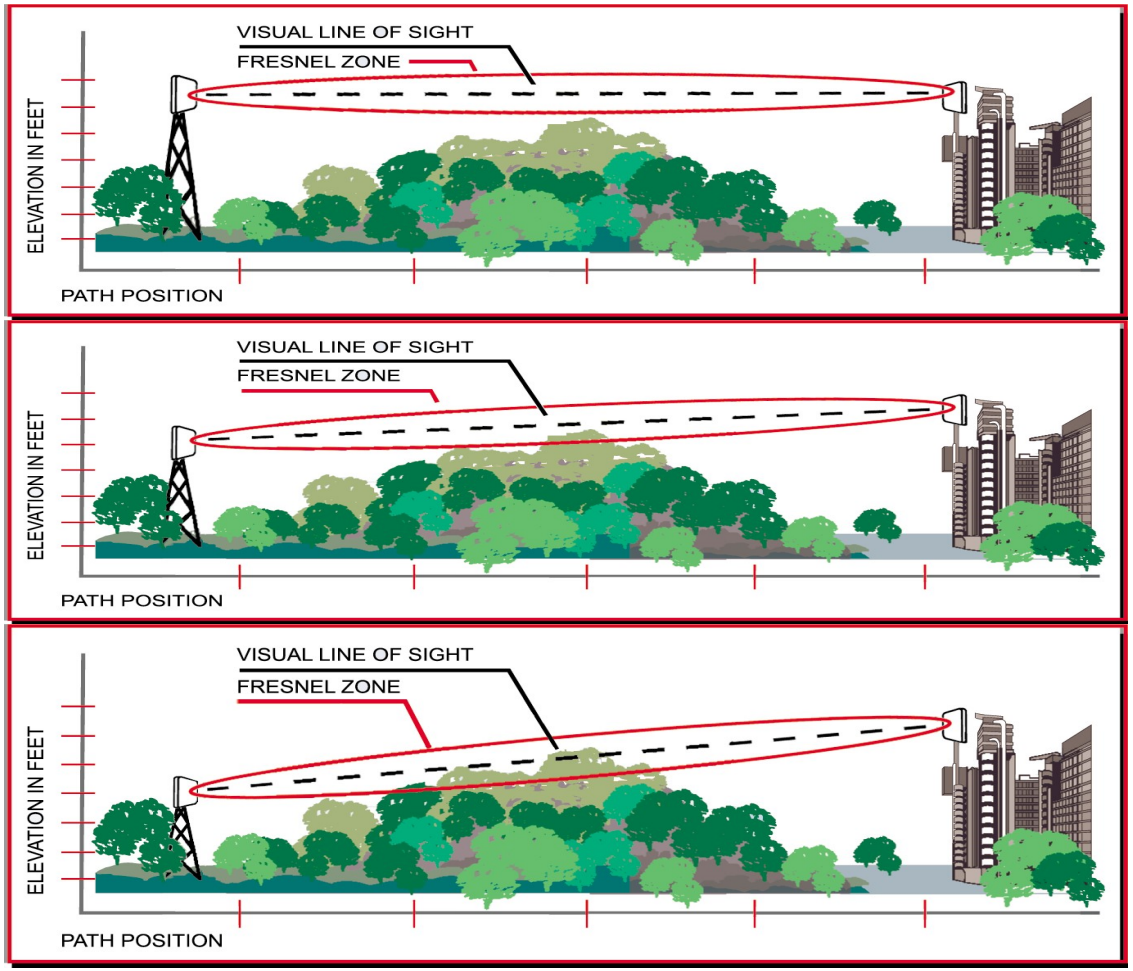




Obstacles

- As with any monitoring or geolocation task, the receivers need to be able to “see” the signal: *obstacle shadowing will prevent successful TDOA geolocation.*
- Multipath effects from reflected and diffracted signals can also complicate geolocation, although TDOA is relatively robust against multipath in comparison with AOA geolocation techniques.
- The biggest obstacle of all, the earth’s curvature, can also limit TDOA over long ranges.
- The presence of obstacles is an important factor for network optimization.
- The greater the receiver heights, the easier it will be to see around obstacles such as mountains, buildings and the earth itself. F
- or any given height above ground level, optimum positioning can also improve geolocation performance, e.g., by placing receivers on the tops of hills rather than behind them.

LoS, nLoS, and NLoS Definitions



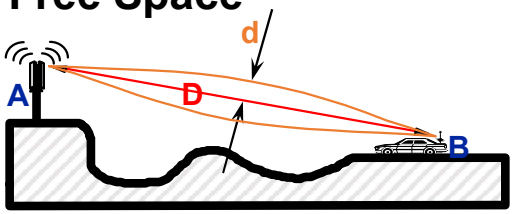
Line of Sight (LoS)

Near Line of Sight (nLoS)

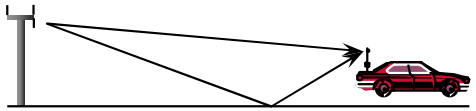
Non-Line of Sight (NLoS)

The Dominant Mechanisms of Mobile Propagation for COMINT

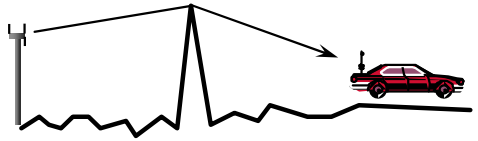
Free Space



Reflection
with partial cancellation



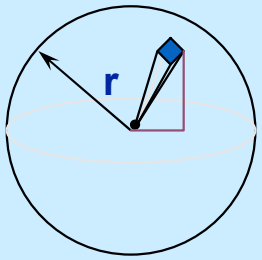
Knife-edge Diffraction



Most propagation in the mobile environment is dominated by these three mechanisms:

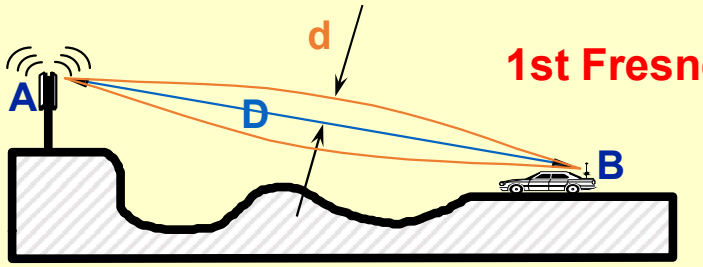
- **Free space**
  - No reflections, no obstructions
    - first Fresnel Zone clear
  - Signal spreading is only mechanism
  - Signal decays 20 dB/decade
- **Reflection**
  - Reflected wave 180°out of phase
  - Reflected wave not attenuated much
  - Signal decays 30-40 dB/decade
- **Knife-edge diffraction**
  - Direct path is blocked by obstruction
  - Additional loss is introduced
  - Formulae available for simple cases

Free-Space Propagation Technical Details



Free Space "Spreading" Loss
energy intercepted by receiving antenna is proportional to **$1/r^2$**

- **The simplest propagation mode**
  - Antenna radiates energy which spreads in space
  - Path Loss, db (between two *isotropic antennas*) = **$36.58 + 20*\text{Log}_{10}(F_{MHZ}) + 20\text{Log}_{10}(\text{Dist}_{MILES})$**
  - Path Loss, db (between two *dipole antennas*) **$= 32.26 + 20*\text{Log}_{10}(F_{MHZ}) + 20\text{Log}_{10}(\text{Dist}_{MILES})$**
  - Notice the rate of signal decay:
  - **6 db per octave** of distance change, which is **20 db per decade** of distance change
- **Free-Space propagation is applicable if:**
  - there is only one signal path (no reflections)
  - the path is unobstructed (i.e., first Fresnel zone is not penetrated by obstacles)

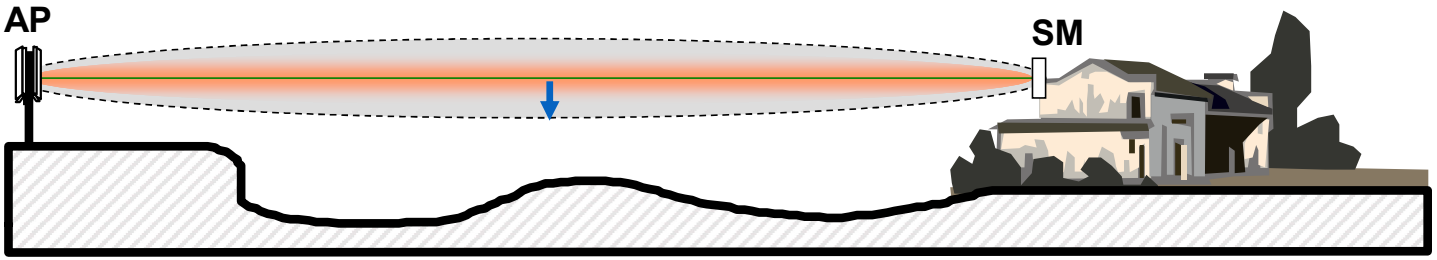


1st Fresnel Zone

First Fresnel Zone =
{Points P where AP + PB - AB $< \lambda/2$ }
Fresnel Zone radius d = 1/2 $(\lambda D)^{\wedge(1/2)}$

The First Fresnel Zone and Free-Space Propagation

Frequency, GHz.	Path, Miles	Mid-Pt Fresnel R, ft
0.92	10	119
2.4	10	74
5.8	10	47

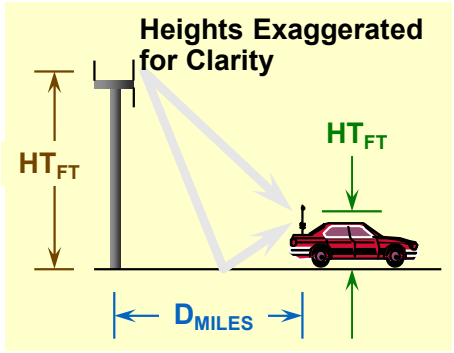


- Most of the signal power sent from one antenna to another travels in an elliptical, “football” shape called the First Fresnel zone.
  - the thickness of the zone depends on the signal frequency
- If the First Fresnel zone is free of penetration or obstruction by any objects, we say “free-space” conditions apply
  - this is the desirable condition providing highest received signal strength
- Sometimes obstructions are unavoidable, and penetrate the first fresnel zone
  - this attenuates the signal and reduces the signal strength received at the other end of the link
  - the amount of attenuation depends on the degree of penetration by the obstruction, and its absorbing characteristics

Terrain Profile: 800 MHz. 1st Fresnel Zone Boggs Mountain to Woodland, CA

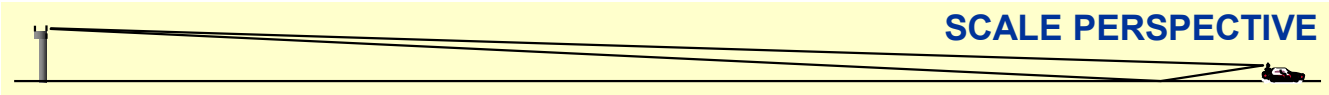
This path isn't clear. How much extra attenuation will this cause?

Reflection With Partial Cancellation



- Mobile environment characteristics:
  - Small angles of incidence and reflection
  - Reflection is unattenuated (reflection coefficient =1)
  - Reflection causes phase shift of 180 degrees
- Analysis
  - Physics of the reflection cancellation predicts signal decay of **40 dB** per decade of distance

Path Loss [dB]= 172 + 34 x Log (D_{Miles})
- 20 x Log (Base Ant. Ht_{Feet})
- 10 x Log (Mobile Ant. Ht_{Feet})

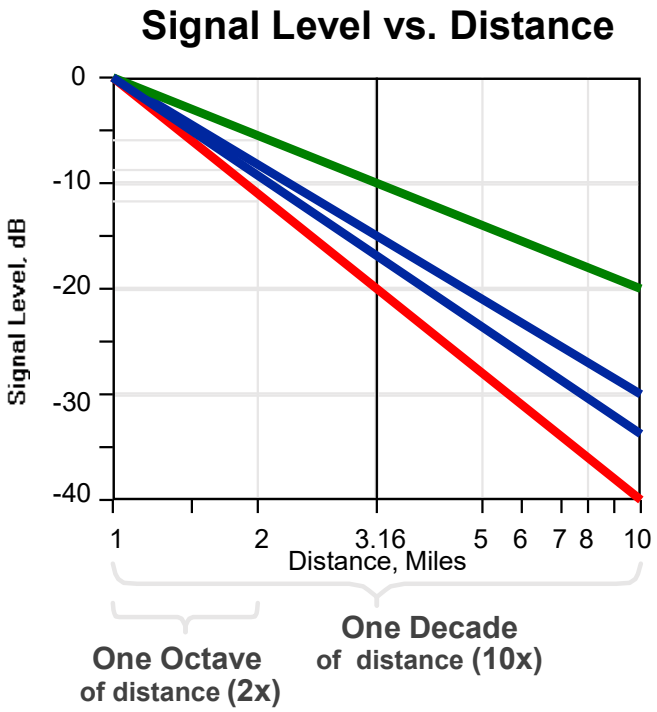


Comparison of Free-Space and Reflection Propagation Modes

Assumptions: Flat earth, TX ERP = 50 dBm, @ 1950 MHz. Base Ht = 200 ft, Mobile Ht = 5 ft.

$Distance_{MILES}$	1	2	4	6	8	10	15	20
Received Signal in Free Space, DBM	-52.4	-58.4	-64.4	-67.9	-70.4	-72.4	-75.9	-78.4
Received Signal in Reflection Mode	-69.0	-79.2	-89.5	-95.4	-99.7	-103.0	-109.0	-113.2

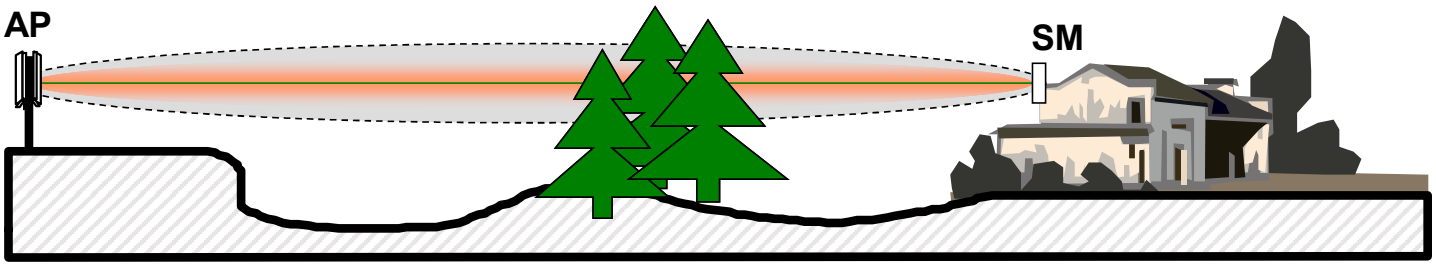
How Distance affects Signal Strength in different environments



We've seen how the signal decays with distance in two basic modes of propagation:

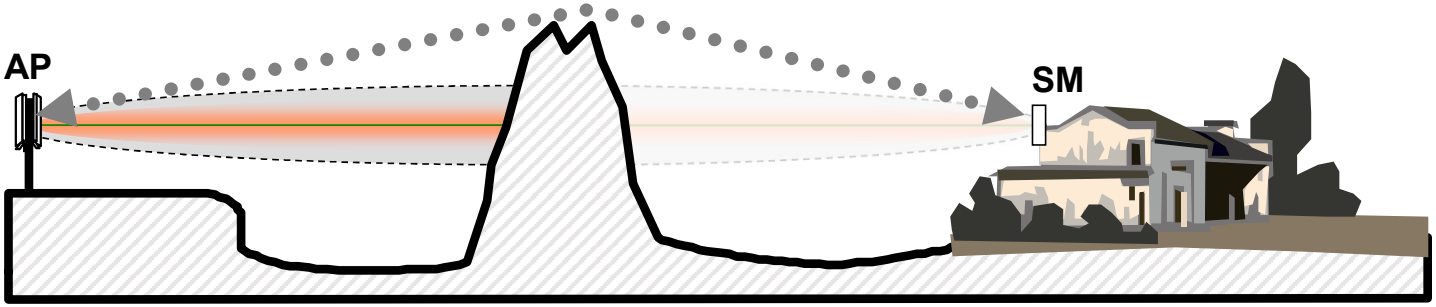
- **Free-Space**
  - 20 dB per decade of distance
  - 6 db per octave of distance
- **Reflection Cancellation**
  - 40 dB per decade of distance
  - 12 db per octave of distance
- Real-life wireless propagation decay rates are typically somewhere between 30 and 40 dB per decade of distance

Obstructions and their Effects



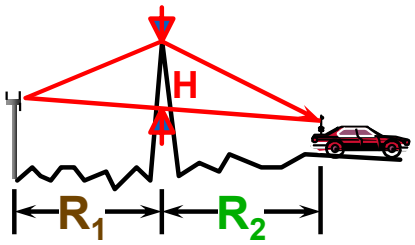
- When an obstruction penetrates the first fresnel zone, the signal is attenuated. The degree of attenuation depends on
  - how much of the first fresnel zone is obstructed
  - the absorptive characteristics of the obstructing object(s)
  - whether the signal is also reflecting off of other nearby objects, possibly providing a degree of "fill-in"
- Depending on the length of the path, the transmitter power, and the receiver sensitivity, the link may still work despite the obstruction

Severe Obstructions

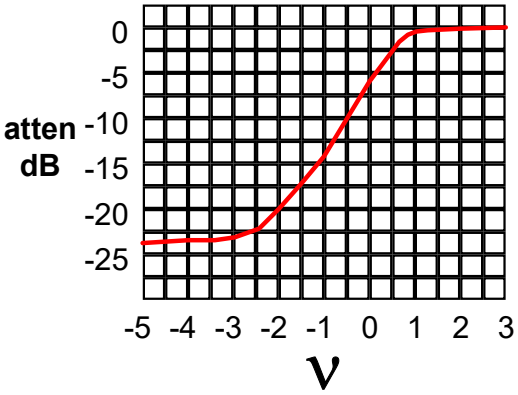


- When the path is blocked by a major obstruction (large hill, downtown building, etc.) there will be substantial signal attenuation
- Even under this undesirable condition, if the distance is small there may be enough signal to make the link usable
  - A very small amount of the signal will actually diffract (“bend”) over the obstruction
  - the extra attenuation caused by the obstruction can be calculated by the “knife edge diffraction” model
  - this “diffraction loss” can be considered in the link budget to see if the link is likely to be usable anyway

Knife-Edge Diffraction

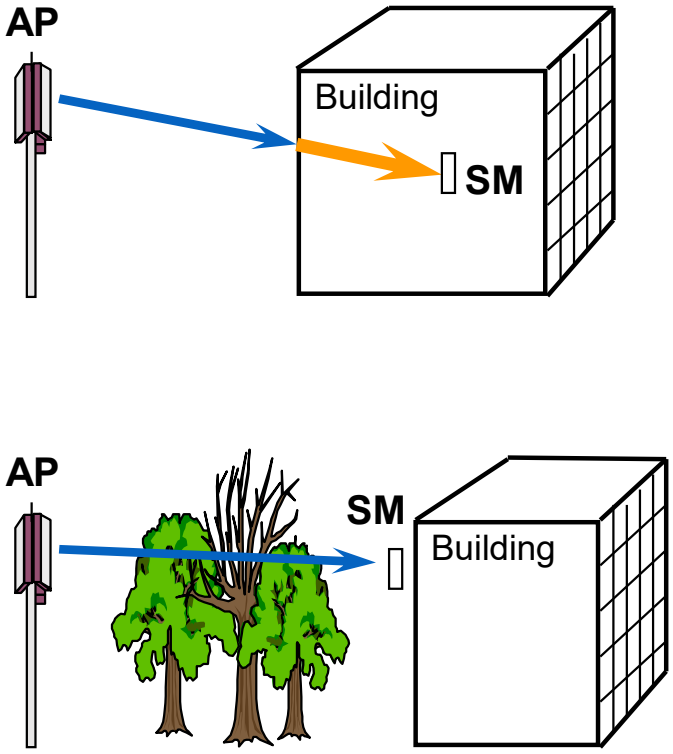


$$\nu = -H\sqrt{\frac{2\,(R1 + R2)}{\lambda\, R1\, R2}}$$



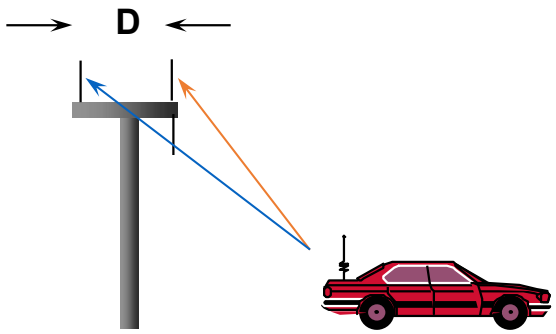
- Sometimes a single well-defined obstruction blocks the path, introducing additional loss. This calculation is fairly easy and can be used as a manual tool to estimate the effects of individual obstructions.
- First calculate the diffraction parameter ν from the geometry of the path
- Next consult the table to obtain the obstruction loss in db
- Add this loss to the otherwise-determined path loss to obtain the total path loss.
- Other losses such as free space and reflection cancellation still apply, but computed independently for the path as if the obstruction did not exist

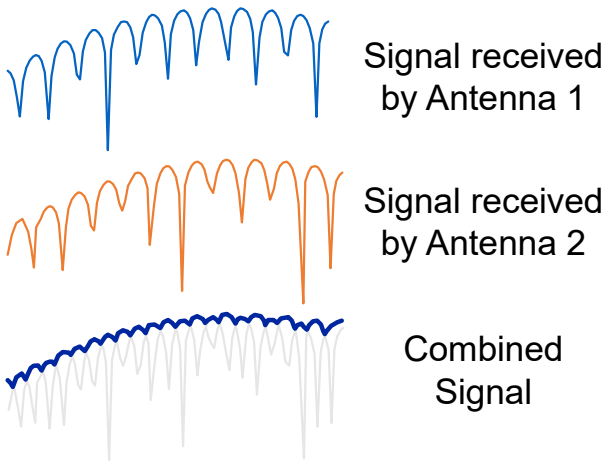
Foliage and Building Penetration Considerations



- At broadband wireless frequencies, the penetration loss entering a building often exceeds 35 db.
  - this restricts range so greatly that antennas are almost never located inside a building
- At broadband wireless frequencies, trees and other vegetation effectively block and absorb the signal
  - typical attenuation for just one mature tree can be 20 db or more
- Unfortunately, neither building nor vegetation loss can be predicted accurately. Measurement is the only way to know accurately what is happening.

Combating Rayleigh Fading: Receiving using Space Diversity





- Fortunately, Rayleigh fades are very short and last a small percentage of the time
- Two antennas separated by several wavelengths will not generally experience fades at the same time
- "Space Diversity" can be obtained by using two receiving antennas and switching instant-by-instant to whichever is best
- Required separation **D** for good decorrelation is 10-20λ
  - 12-24 ft. @ 800 MHz.
  - 5-10 ft. @ 1900 MHz.

Types of Fading

- Fast fading
  - Caused by multipath cancellation
- Slow fading
  - Caused when driving past physical obstructions
- Flat fading
  - Fading which affects all frequencies on a path
- Selective fading
  - Fading which affects only certain specific frequencies on a path
- Rayleigh fading
  - Fading when the line-of-sight signal is blocked and the many reflections are the only signals present. Deep and frequent fading occurs.
- Rician fading
  - Fading which occurs when the line-of-sight signal is strong and fades only occur when the multipath reflections are in opposing phases. Deep fades are not as prevalent as in Rayleigh fading.

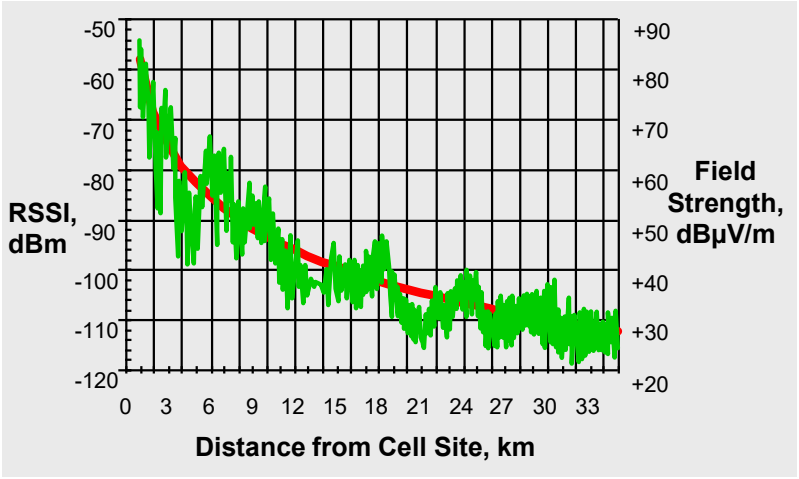
Types Of Propagation Models And Their Uses

- Simple ***Analytical*** models
  - Used for understanding and predicting individual paths and specific obstruction cases
- General ***Area*** models
  - Primary drivers: statistical
  - Used for early system dimensioning (cell counts, etc.)
- ***Point-to-Point*** models
  - Primary drivers: analytical
  - Used for detailed coverage analysis and cell planning
- ***Local Variability*** models
  - Primary drivers: statistical
  - Characterizes microscopic level fluctuations in a given locale, confidence-of-service probability

- **Examples of various model types**

- **Simple Analytical**
  - Free space (Friis formula)
  - Reflection cancellation
  - Knife-edge diffraction
- **Area**
  - Okumura-Hata
  - Euro/Cost-231
  - Walfisch-Betroni/Ikegami
- **Point-to-Point**
  - Ray Tracing
    - Lee's Method, others
  - Tech-Note 101
  - Longley-Rice, Biby-C
- **Local Variability**
  - Rayleigh Distribution
  - Normal Distribution
  - Joint Probability Techniques

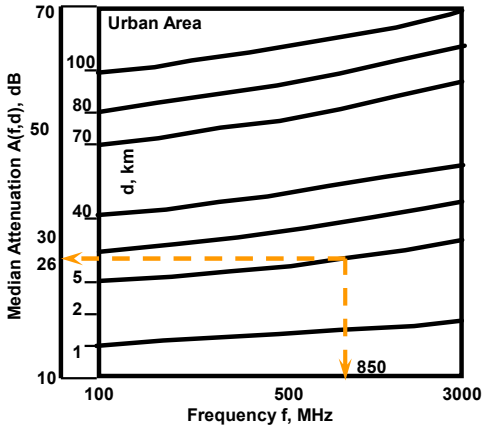
General Principles Of Area Models

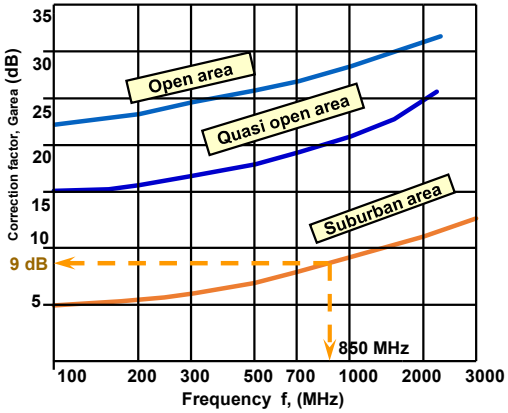


- **Green Trace** shows actual measured signal strengths on a drive test radial, as determined by real-world physics.
- **Red Trace** shows the Okumura-Hata prediction for the same radial. The smooth curve is a good "fit" for real data. However, the signal strength at a specific location on the radial may be much higher or much lower than the simple prediction.

- Area models mimic an *average path* in a defined area
- They're based on measured data alone, with no consideration of individual path features or physical mechanisms
- Typical inputs used by model:
  - Frequency
  - Distance from transmitter to receiver
  - Actual or effective base station & mobile heights
  - Average terrain elevation
  - Morphology correction loss (Urban, Suburban, Rural, etc.)
- Results may be quite different than observed on individual paths in the area

The Okumura Model: General Concept





The Okumura model is based on detailed analysis of exhaustive drive-test measurements made in Tokyo and its suburbs during the late 1960's and early 1970's. The collected date included measurements on numerous VHF, UHF, and microwave signal sources, both horizontally and vertically polarized, at a wide range of heights.

The measurements were statistically processed and analyzed with respect to almost every imaginable variable. This analysis was distilled into the curves above, showing a median attenuation relative to free space loss **Amu (f,d)** and correlation factor **Garea (f,area), for** BS antenna height **ht = 200 m** and MS antenna height **hr = 3 m.**

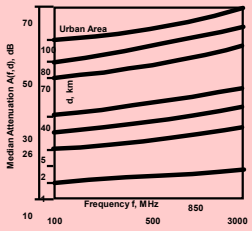
Okumura has served as the basis for high-level design of many existing wireless systems, and has spawned a number of newer models adapted from its basic concepts and numerical parameters.

Structure of the Okumura Model

Path Loss [dB] = L_{FS} + $A_{mu}(f,d)$ - $G(H_b)$ - $G(H_m)$ - G_{area}

Free-Space Path Loss

$A_{mu}(f,d)$ Additional Median Loss from Okumura's Curves

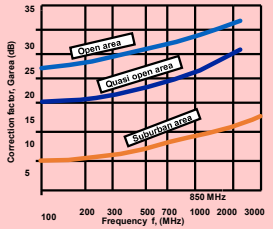


Base Station Height Gain = 20 x Log (H_b/200)

Mobile Station Height Gain = 10 x Log (H_m/3)

Morphology Gain

0 dense urban
5 urban
10 suburban
17 rural



- The Okumura Model uses a combination of terms from basic physical mechanisms and arbitrary factors to fit 1960-1970 Tokyo drive test data
- Later researchers (HATA, COST231, others) have expressed Okumura's curves as formulas and automated the computation

Typical Model Results
Including Environmental Correction

COST-231/Hata
f =1900 MHz.

	Tower Height, m	EIRP (watts)	C, dB	Range, km
Dense Urban	30	200	0	2.52
Urban	30	200	-5	3.50
Suburban	30	200	-10	4.8
Rural	50	200	-17	10.3

Okumura/Hata
f = 870 MHz.

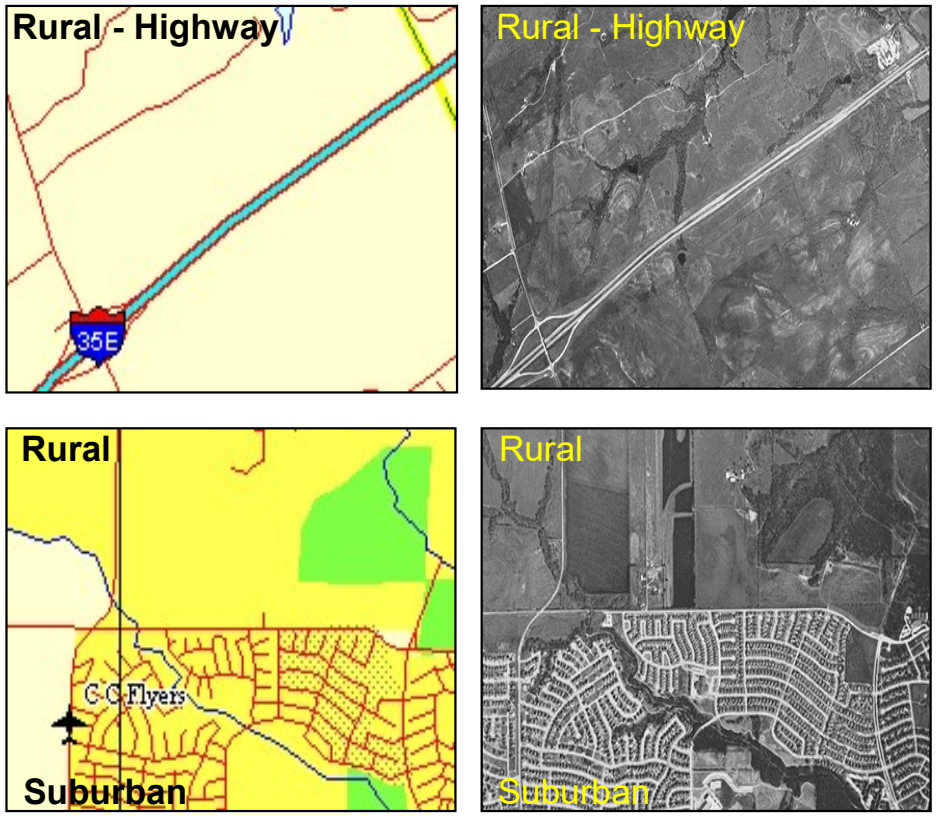
	Tower Height, m	EIRP (watts)	C, dB	Range, km
Dense Urban	30	200	-2	4.0
Urban	30	200	-5	4.9
Suburban	30	200	-10	6.7
Rural	50	200	-26	26.8

Examples of Morphological Zones

- **Suburban**: Mix of residential and business communities. Structures include 1-2 story houses 50 feet apart and 2-5 story shops and offices.
- **Urban**: Urban residential and office areas (Typical structures are 5-10 story buildings, hotels, hospitals, etc.)
- **Dense Urban**: Dense business districts with skyscrapers (10-20 stories and above) and high-rise apartments

Although zone definitions are arbitrary, the examples and definitions illustrated above are typical of practice in North American PCS designs.

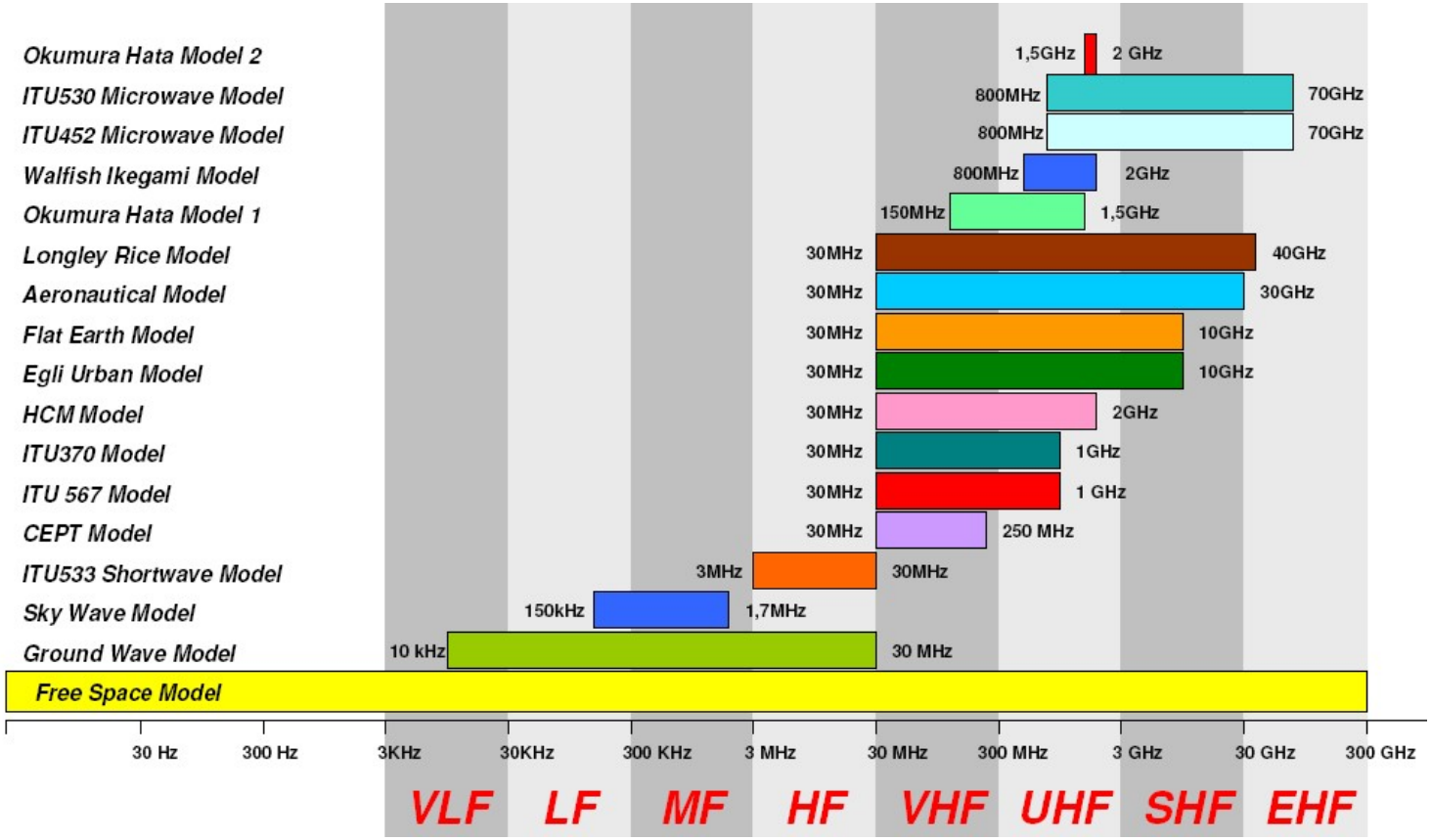
Example Morphological Zones



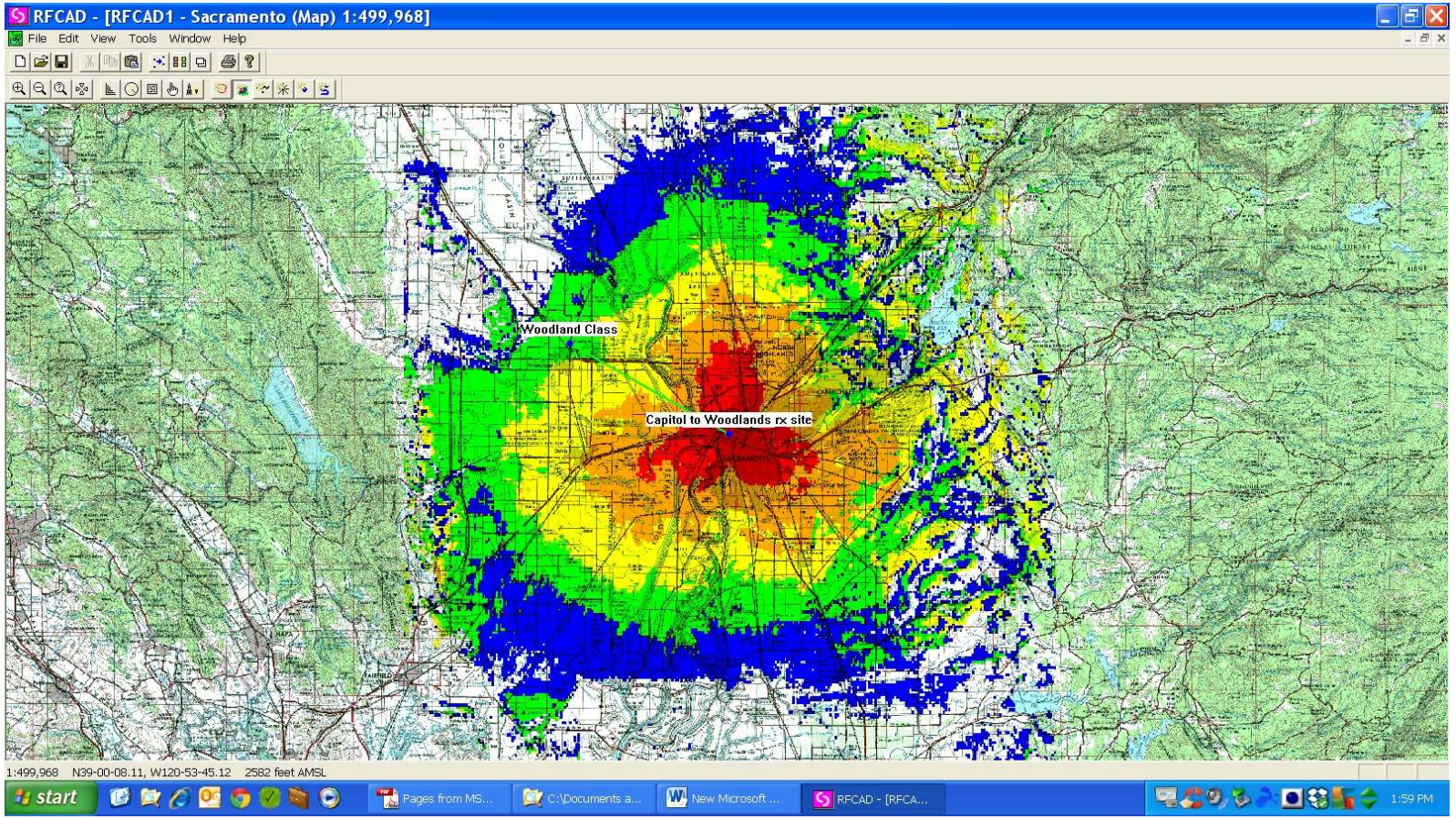
- **Rural - Highway**: Highways near open farm land, large open spaces, and sparsely populated residential areas. Typical structures are 1-2 story houses, barns, etc.
- **Rural - In-town**: Open farm land, large open spaces, and sparsely populated residential areas. Typical structures are 1-2 story houses, barns, etc.

Notice how different zones may abruptly adjoin one another. In the case immediately above, farm land (rural) adjoins built-up subdivisions (suburban) -- same terrain, but different land use, penetration requirements, and anticipated traffic densities.

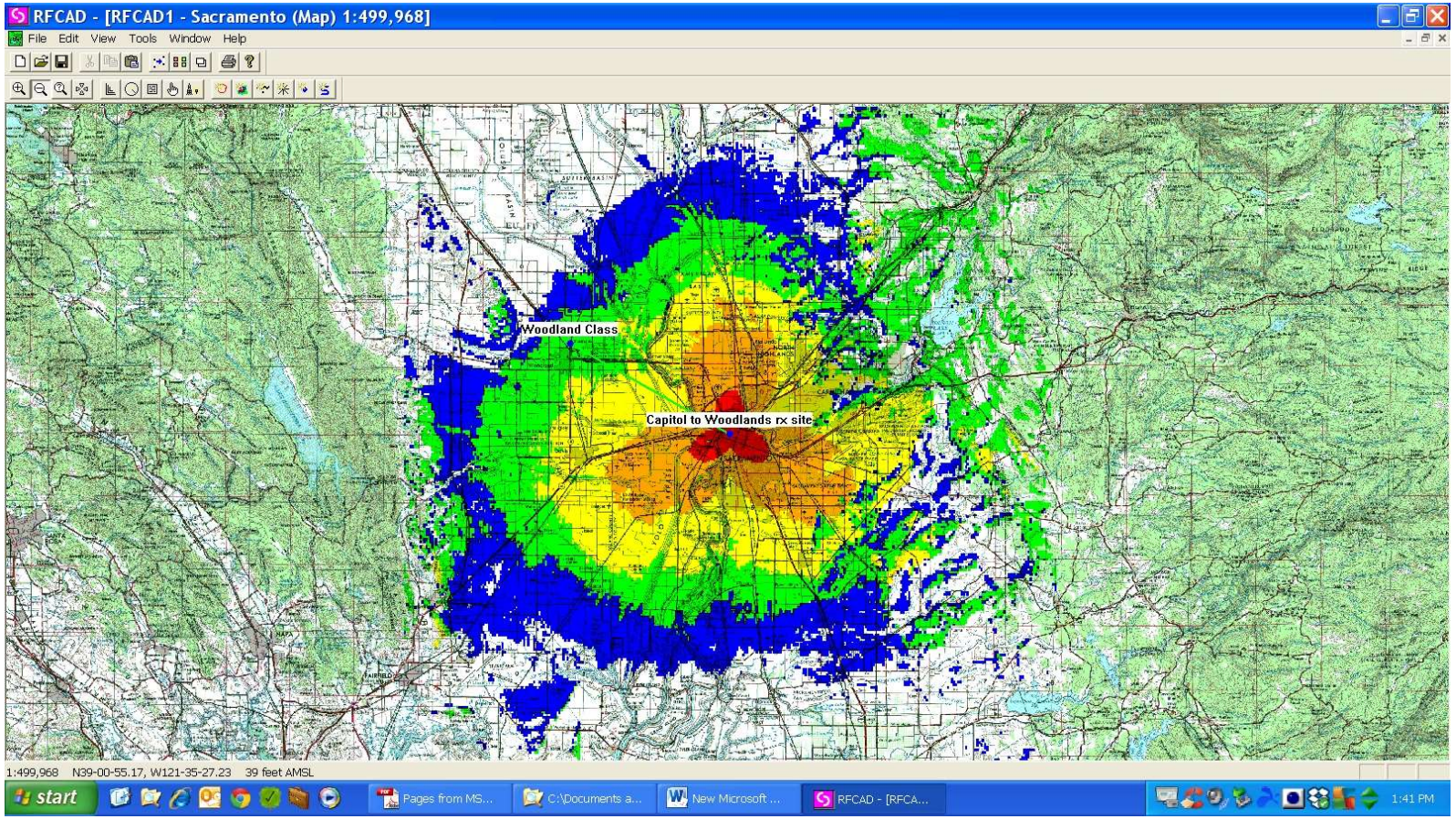
Radio Network Planning Tools - Basics



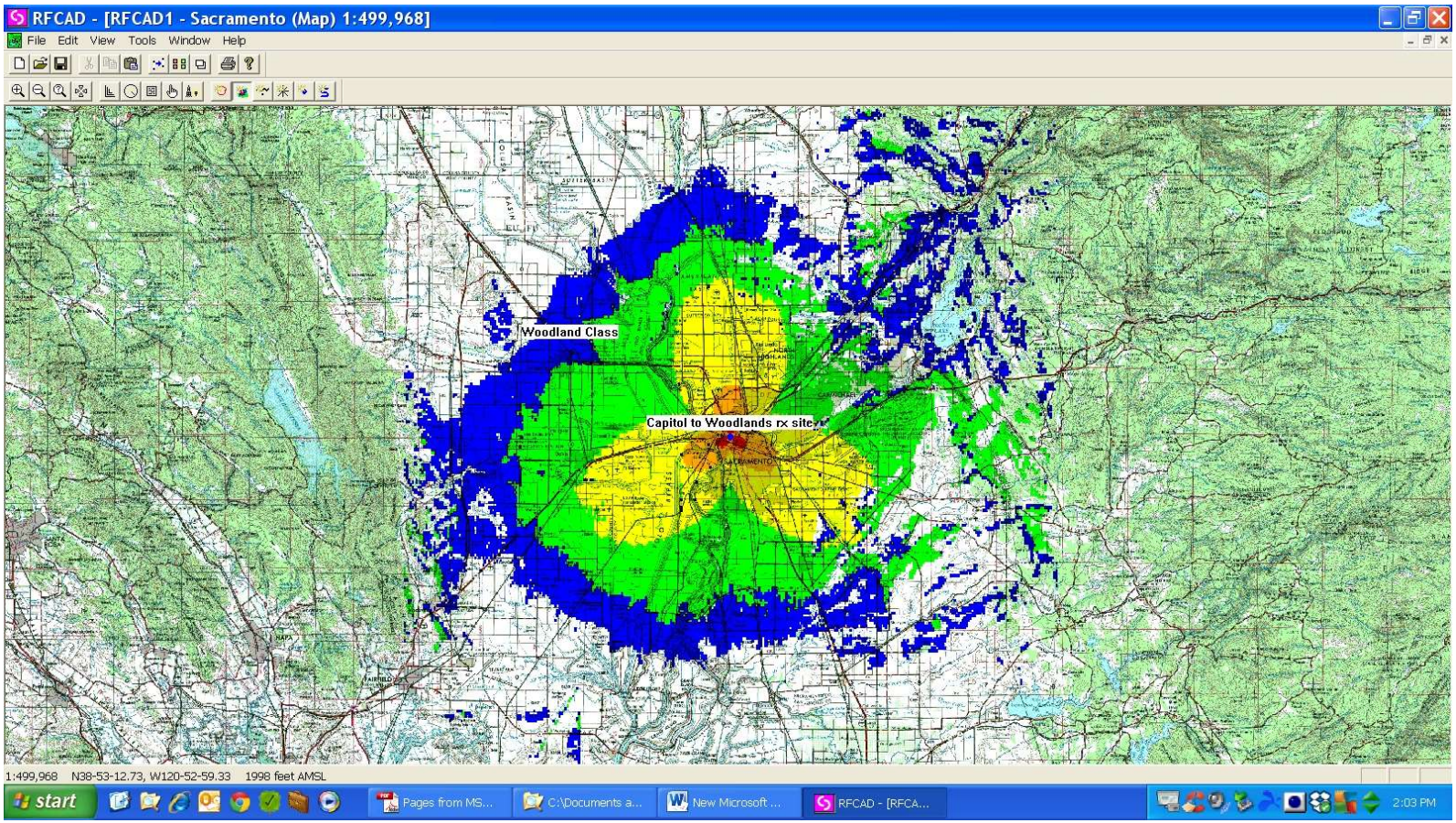
Predicted Coverage:
800 MHz. from atop State Capitol Dome



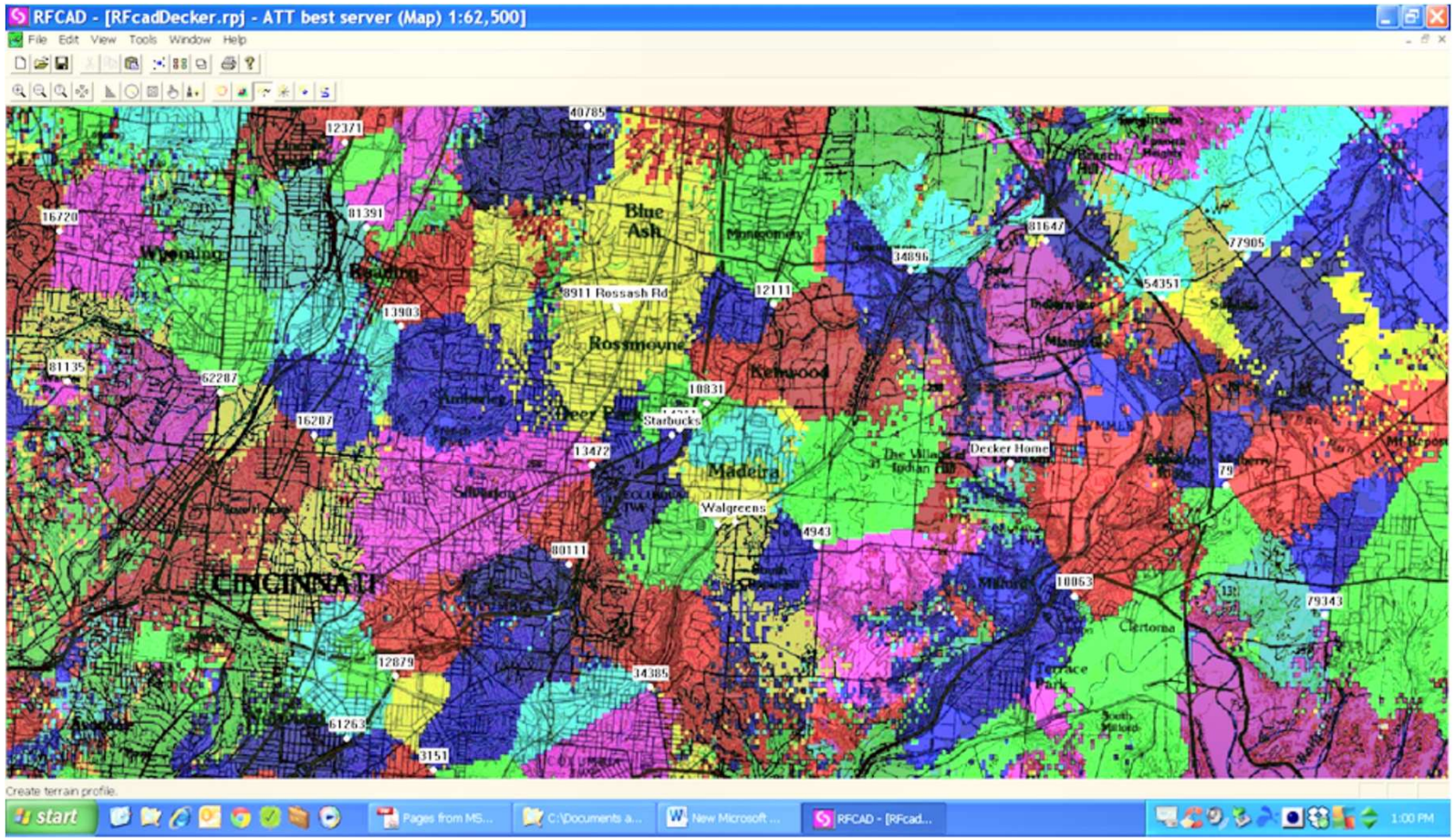
Predicted Coverage:
1900 MHz. from atop State Capitol Dome



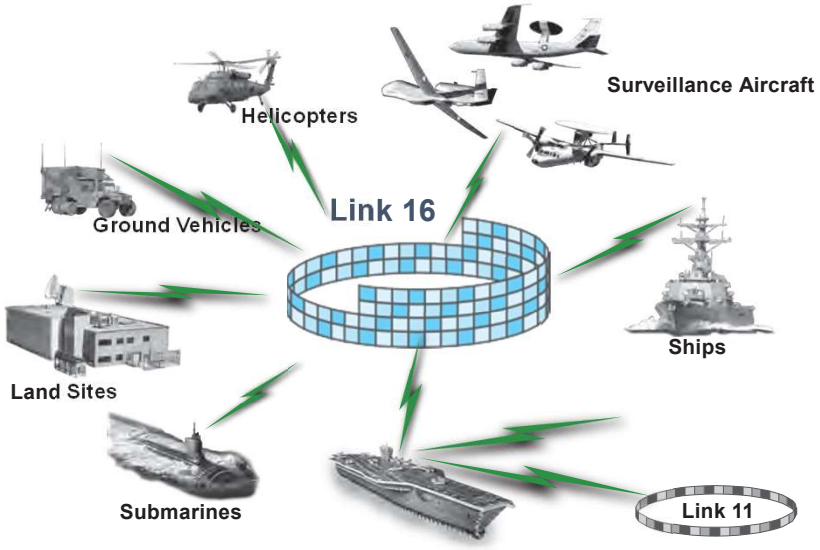
Predicted Coverage:
5000 MHz. from atop State Capitol Dome



Typical Best-Server Plot:
AT&T Wireless, Cincinnati



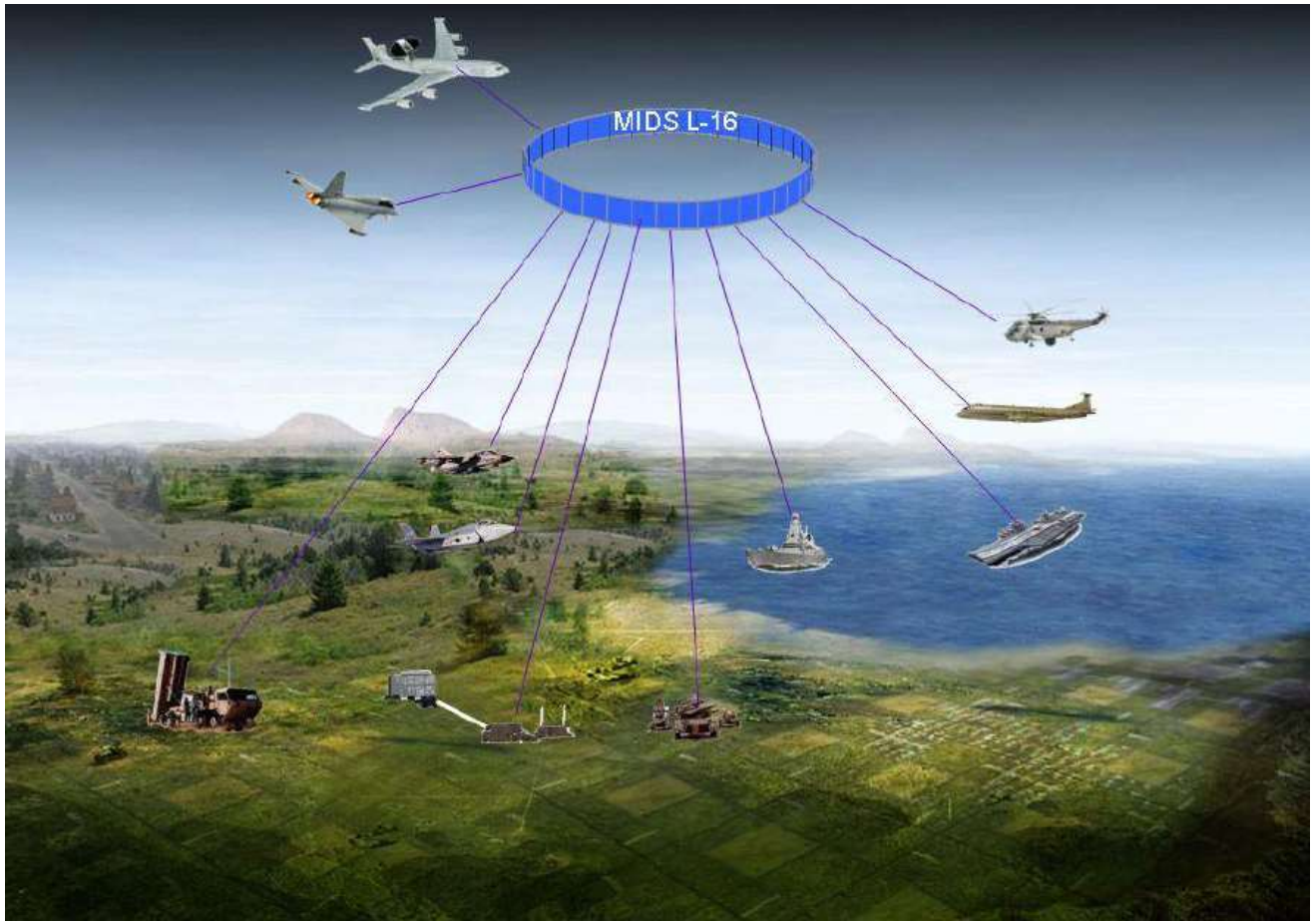
ELINT: Link 16 Platforms



Some examples of platforms currently using the Link 16 capability are:

- Aircraft
- Ships
- Ground vehicles
- Missile defense systems
- Networked Weapons
- Command and Control

ELINT: Link 16 Operation



Standard Bands (Example Use)

HF	3 – 30 MHz
VHF	30 MHz–300 MHz
UHF	300 MHz–1 GHz
L-Band	1 GHz–2 GHz
S-Band	2 GHz–4 GHz
C-Band	4 GHz–8 GHz
X-Band	8 GHz–12 GHz
Ku-Band	12 GHz–18 GHz
K-Band	18 GHz–27 GHz
Ka-Band	27 GHz–40 GHz
W-Band	40 GHz – 100+ GHz

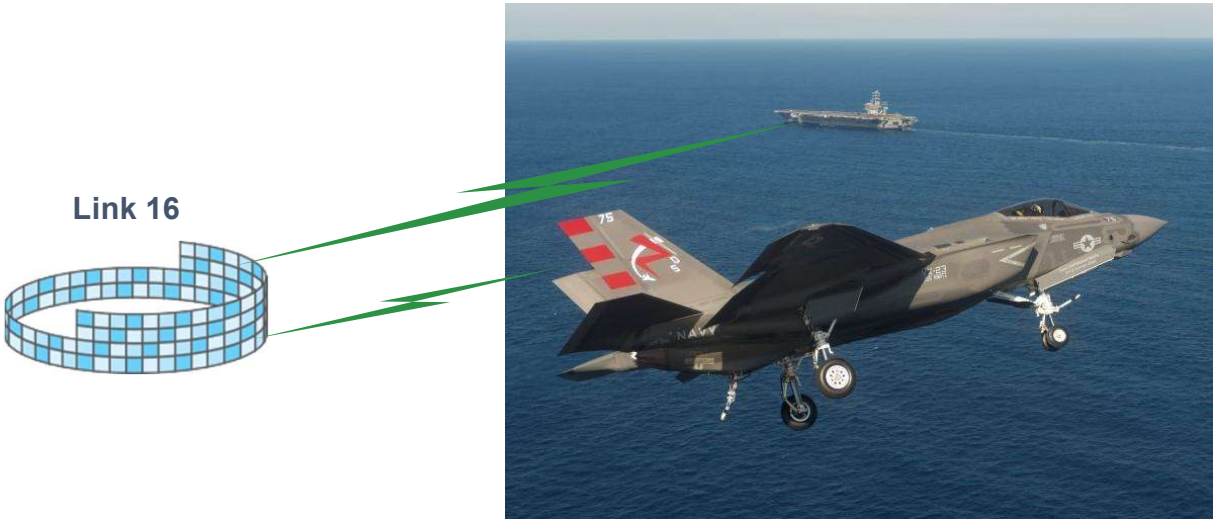
Link 16
Search Radars

Link 16
TTNT
Search &
Track Radars

Fire Control &
Imaging Radars

Missile
Seekers

Basic Operational Functionality



- JTIDS/MIDS/JTRS Link 16 is primarily used to support military functions/tasks such as:
  - Air Defense Anti-Air Warfare
  - Anti-Surface Warfare
  - Anti-Submarine Warfare
  - Reconnaissance and Intelligence gathering
  - Electronic Warfare (EW)
  - Air to Air and Air to Ground Targeting

Link 16 communications Terminals

Traditional Link 16 communications terminal types:

- Joint Tactical Information Distribution System (JTIDS)
- Multifunctional Information Distribution System (MIDS)

Modern Link 16 communications terminal

- Joint Tactical Radio System (JTRS) Waveforms

Joint Tactical Radio System (JTRS) Waveforms

- Wideband Networking Waveform (WNW)
- Soldier Radio Waveform (SRW)
- Link-16
- High Frequency (HF)
- UHF SATCOM
- Mobile User Objective System (MUOS)
- Enhanced Position Location Reporting System (EPLRS)
- Single Channel Ground and Airborne Radio System (SINCGARS)
- Joint Airborne Networking–Tactical Edge (JAN-TE)
  - TTNT

- Cost per Unit: $10,000 to $270,000

What is Link 16?

- Link 16 is the backbone tactical datalink system for exchange of related surveillance, weapons coordination, and air control information.
    - A Link 16 terminal is normally part of a platform configuration. The terminal is in the airplane, ship, or weapons control area.
- The TDLs, formerly known as Tactical Digital Information Links (TADILs)1, were developed in conjunction with digital computers to permit Joint and Coalition forces to exchange information across a digital interface.
    - Link 11 (the former TADIL A and Link 11B (the former TADIL B) were designed to enable eight-bit computers to share near-real-time surveillance and command data among functionally supporting units in the performance of their missions.
    - Link 16, formerly known as TADIL J, was developed as a modernized, replacement upgrade to these links to reflect later 16-bit requirements.
- Link 16 development began in the 1970s.
    - Link 16 initially became operational in the United States Military during the mid-to-late 1980s, with the introduction of the Class 1 JTIDS terminal. Although these platforms processed only the Interim JTIDS Message Specification (IJMS), this was the beginning of the Link 16 evolution.

Overview of Link 16

- Link 16 employs the Joint Tactical Information Distribution System (JTIDS) and Multifunctional Information Distribution System (MIDS) data link terminals.
  - Link 16 is a frequency-hopping, jam-resistant, high-capacity data link.
  - Operating on the principle of Time Division Multiple Access (TDMA), wherein 128 time slots per second are allocated among participating JTIDS Units (JUs), time slots are organized into multiple functional Network Participation Groups (NPGs).
  - Link 16 includes elements of Link 11/Link 11B and Link 4A/Link 4C, while providing many new or improved capabilities, including voice.

Link 16 Terminal

- The word “terminal” refers to a number of radio sets that are used to transmit and receive tactical data to and from a Link 16 RF network.
- The acronym “JTIDS” refers to the Joint Tactical Information Distribution System, the first-generation Link 16 terminal.
    - It encompasses the Class 1 and Class 2 terminals’ software, hardware, and RF equipment, as well as the high-capacity, secure, antijam waveform that they generate.
    - The **Multifunctional Information Distribution System (MIDS)** Low- Volume Terminal (LVT) is the second generation of Link 16 terminals. Many variants of this terminal, designated LVT 1 through LVT 11, have been produced, each unique in its interface and programming.
    - The next generation of Link 16-capable radios will be the **Joint Tactical Radio System (JTRS) and MIDS JTRS.**
- *JTIDS or MIDS is the software, hardware, RF equipment, and waveform of Link 16.*

MIDS/Link 16 Terminals

- JTIDS Class I
- IJMS only
- JTIDS Class II
- Bilingual
- IJMS
- Link 16 J-Series
- messages
- UK AN/URC 138 (also
- known as the ‘SHAR’
- terminal)
- MIDS LVT
- MIDS JTRS

Source:

NORTHROP GRUMMAN

Link 16 is a standardized communications link for the transmission and exchange of real time tactical data among network participants (also known as TADIL J).
Link 16 uses TDMA to provide multiple, simultaneous communication paths through different nets.

Ultra High Frequency TDMA/CDMA based

- JTIDS / MIDS use Lx portion of L band
  - 960 – 1215 MHz (Lx band)
  - 969 – 1206 MHz (actual)
- 51 frequencies
- 3 MHz separation

- Access method:
  - TDMA
  - CDMA
  - Synchronization: Acquisition & maintenance of system time

Frequency Number	Frequency (MHz)	Frequency Number	Frequency (MHz)	Frequency Number	Frequency (MHz)
1	969	18	1062	35	1158
2	972	19	1065	36	1161
3	975	20	1113	37	1164
4	978	21	1116	38	1167
5	981	22	1119	39	1170
6	984	23	1122	40	1173
7	087	24	1125	41	1176
8	990	25	1128	42	1179
9	993	26	1131	43	1182
10	996	27	1134	44	1185
11	999	28	1137	45	1188
12	1002	29	1140	46	1191
13	1005	30	1143	47	1194
14	1008	31	1146	48	1197
15	1053	32	1149	49	1200
16	1056	33	1152	50	1203
17	1059	34	1155	51	1206

Higher IFF Notch

Lower IFF Notch

Ultra High Frequency

Identification Friend or Foe (**IFF**)

MIDS JTRS Terminal

- The MIDS JTRS terminal from combines the network-centric communications capability of tomorrow with the real-time operating picture of today – all in one unit.
  - For example a four-channel software-programmable radio delivers Link 16 and TACAN functionality, as well as three channels for future growth, including JTRS advanced networking waveforms such as TTNT meeting Joint Aerial Network – Tactical Edge (JAN-TE) requirements.

Viasat's MIDS JTRS terminal: IP NETWORKING OVER ADVANCED WAVEFORMS TO THE COCKPIT

- With three universal channels available, Viasat's MIDS JTRS terminal is ready for legacy as well as the next generation of IP-based tactical networking.
  - The terminal's reprogrammable transceivers can support current legacy waveforms, such as SINCGARS and HAVE QUICK to provide greater interoperability between forces.
  - The MIDS JTRS architecture provides a logical upgrade path capable of future waveforms, including TTNT, IFDL, CDL, MDL, etc.

  - Source: ViaSat

MIDS-LVT vs. MIDS JTRS

(left) MIDS-LVT; Open and Modular Design; Secure Voice @ 2.4 Kbps & 16 Kbps; TACAN

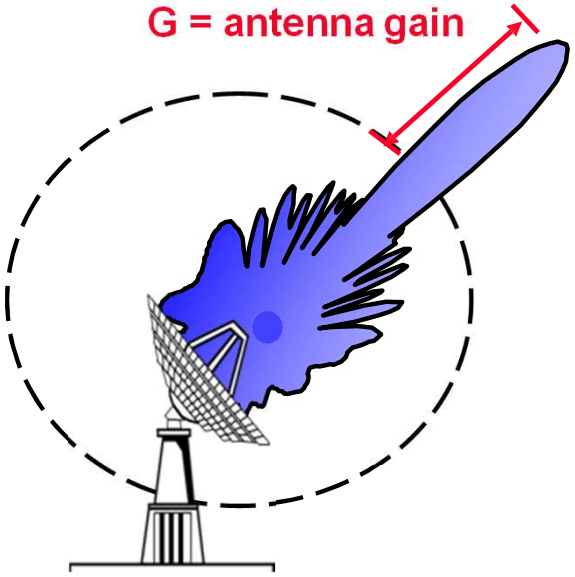
(right) MIDS JTRS; MIDS-LVT Form-Fit-Function Replacement; Programmable 4- Channel Radio (Link 16 + 3); Reserved capacity to support wide band networking waveforms (SRW, WNW, JAN-TE →TTNT)

MIDS JTRS

- MIDS JTRS has a Link 16 throughput of 1.1 MB/sec, which is ten times greater than MIDS-LVT. It is National Security Agency (NSA) certified with the Link 16 waveform and also includes frequency remapping, which allows MIDS JTRS to meet an agreement between DoD and DoT (Federal Aviation Administration) regarding frequency de-confliction.

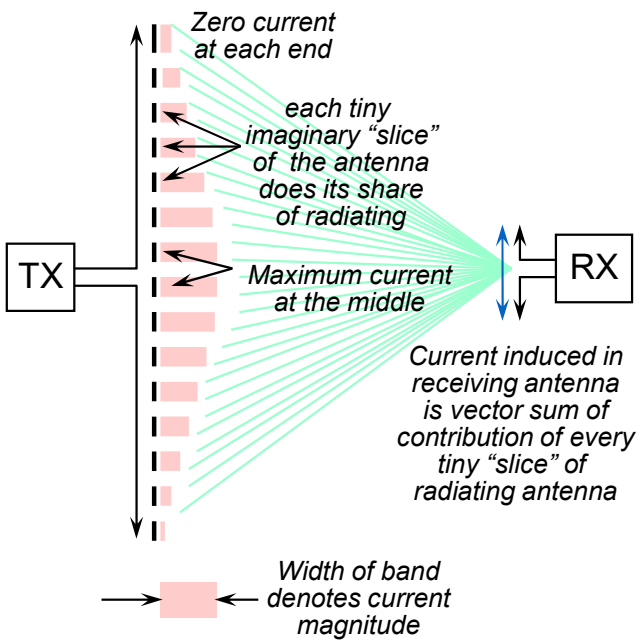
  Unlike the other JTRS programs, the MIDS program is specifically organized to include international partners, which include France, Italy, Germany and Spain.

Directional antenna



Basics of Antenna

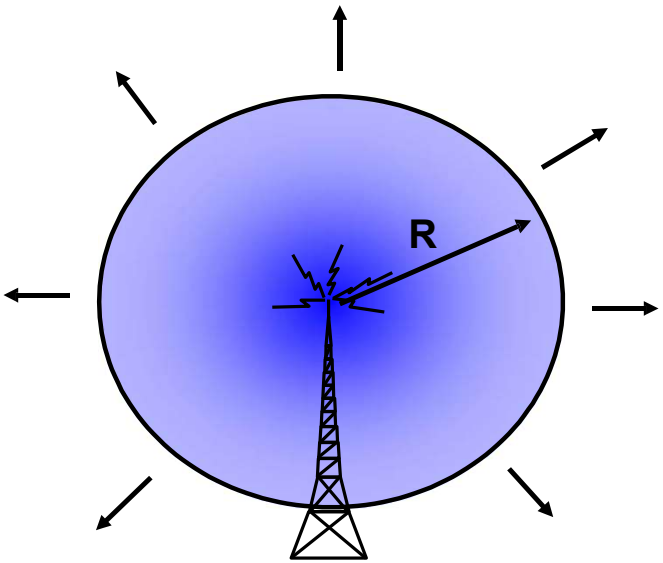
Electromagnetics: Antenna and Radiation Modeling



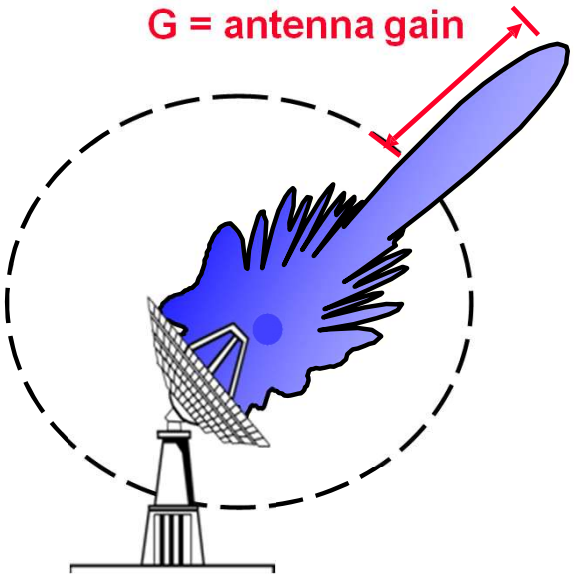
- Maxwell's equations describe how standing waves of current on antennas cause electromagnetic fields to radiate outward and have specific shapes
- Using NEC (numeric electric code) software it is possible to predict the shape of the radiation given off by a specific antenna, and to calculate how the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

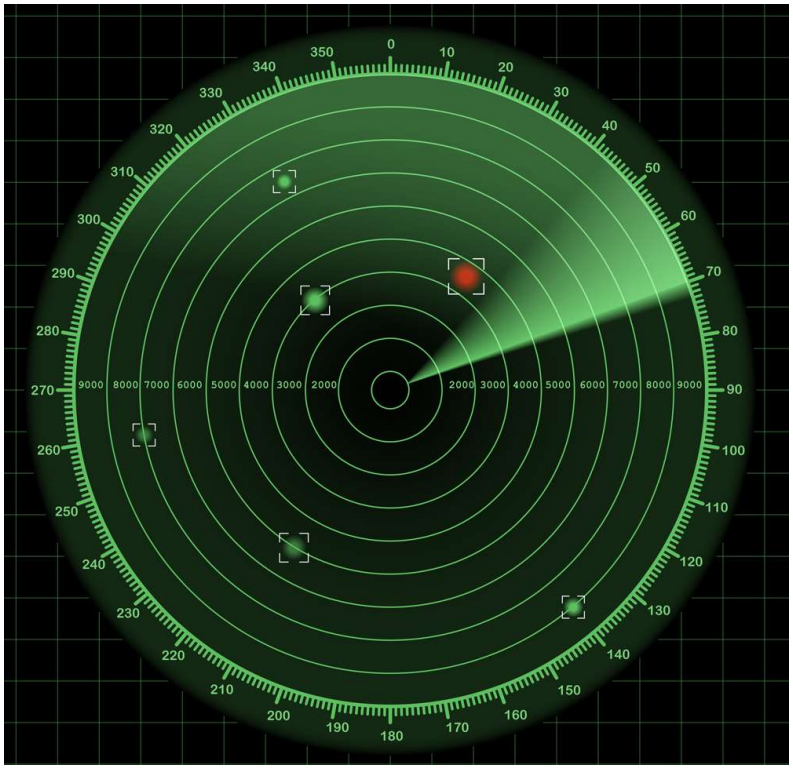
Antenna Gain

Isotropic antenna



Directional antenna





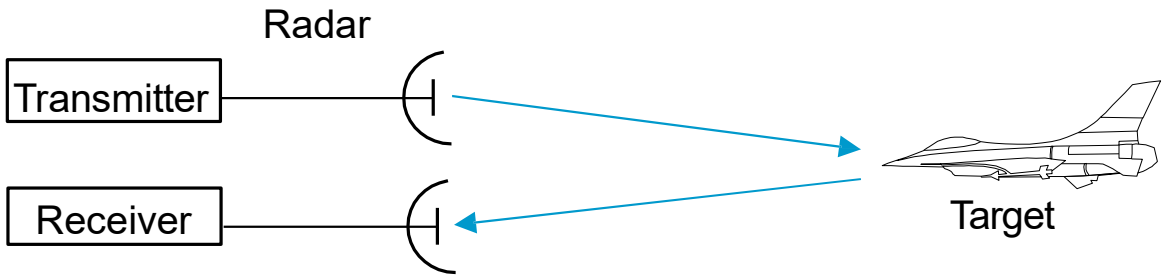
Basics of Radar

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

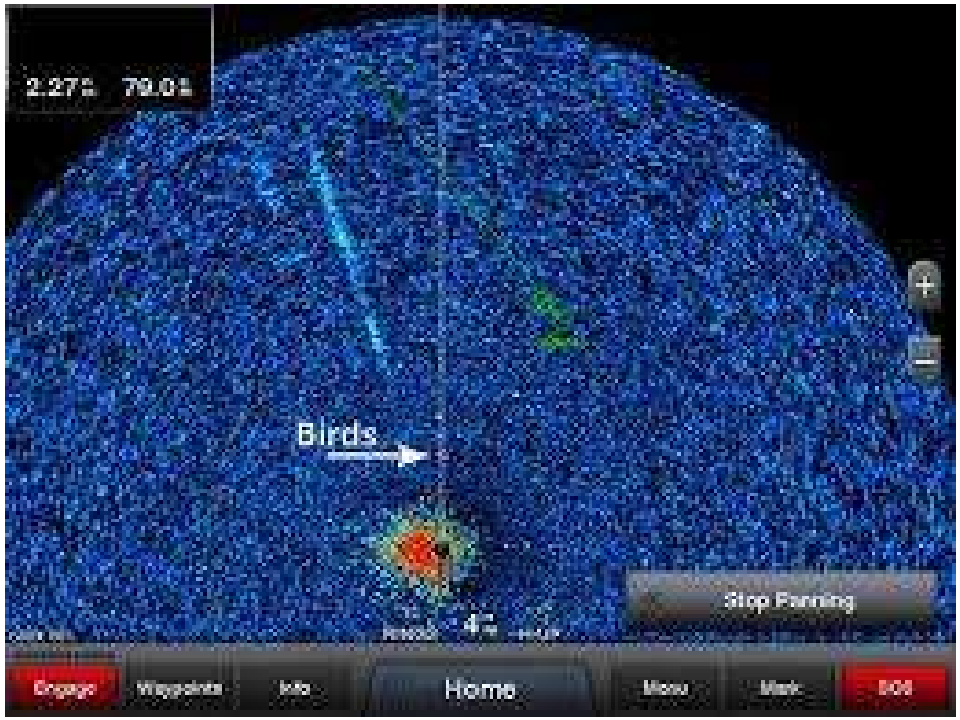
- The complexity (cost & size) of the radar increases with the extent of the functions that the radar performs.

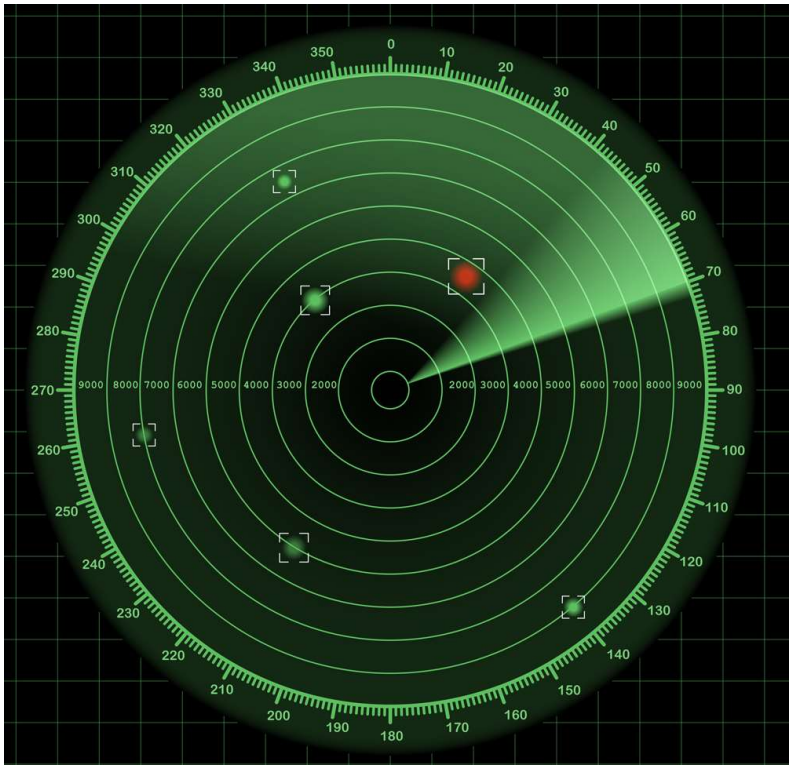
Simplified Radar



- 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.

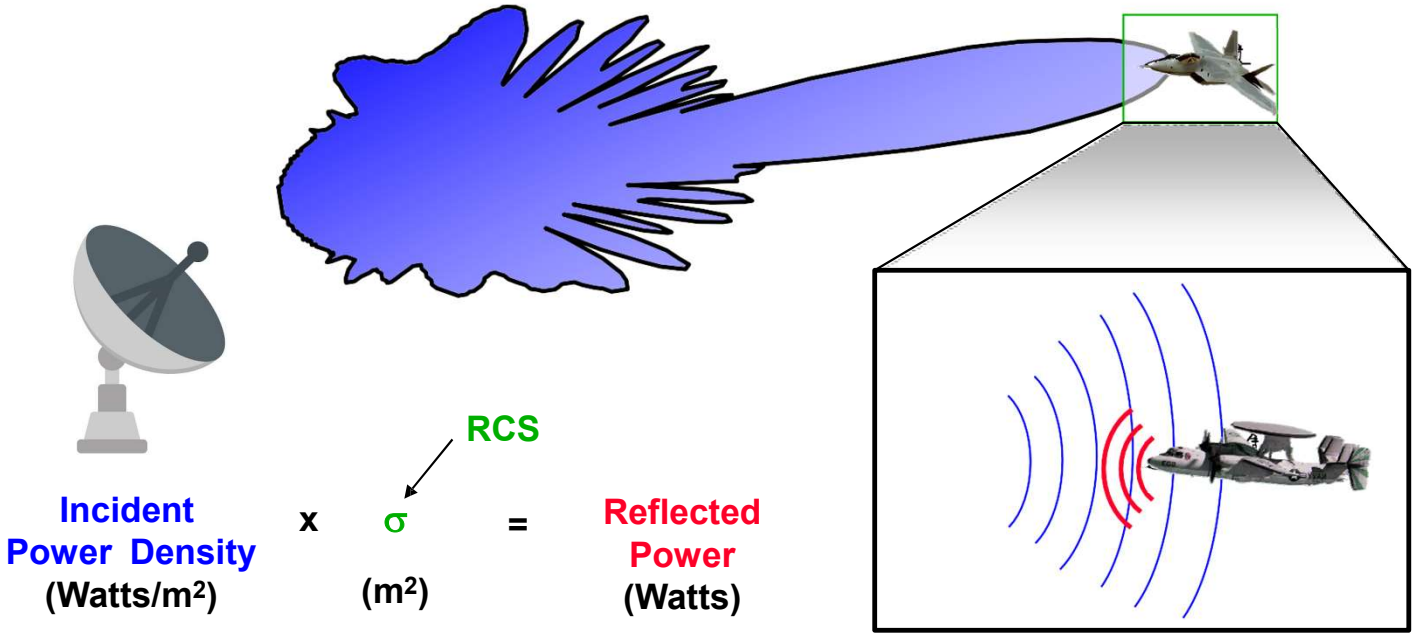
Birds as a Targets





Radar Cross Section (RCS)

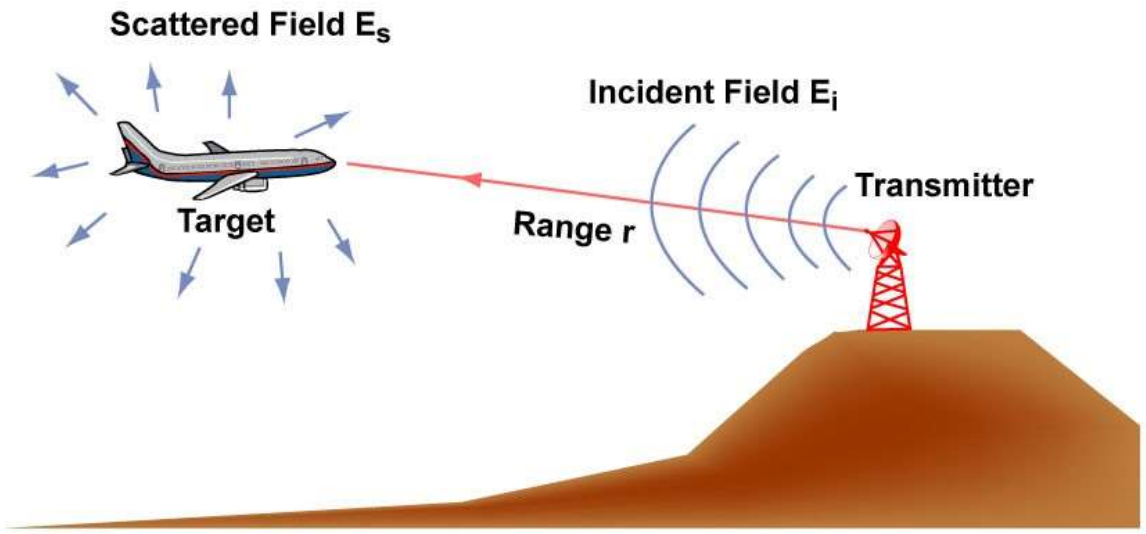
Radar Cross Section (RCS)



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)

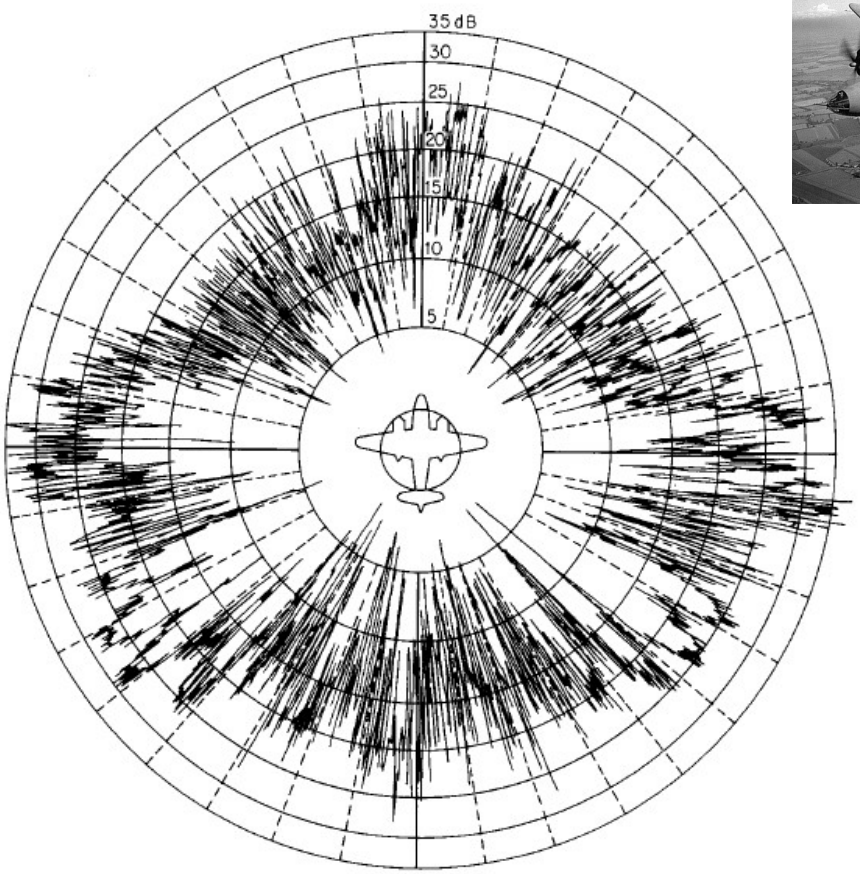


$$\text{RCS} = \lim_{r \to \infty} 4\pi r^2 \frac{|E_s|^2}{|E_i|^2} \quad \text{(Unit: Area)}$$

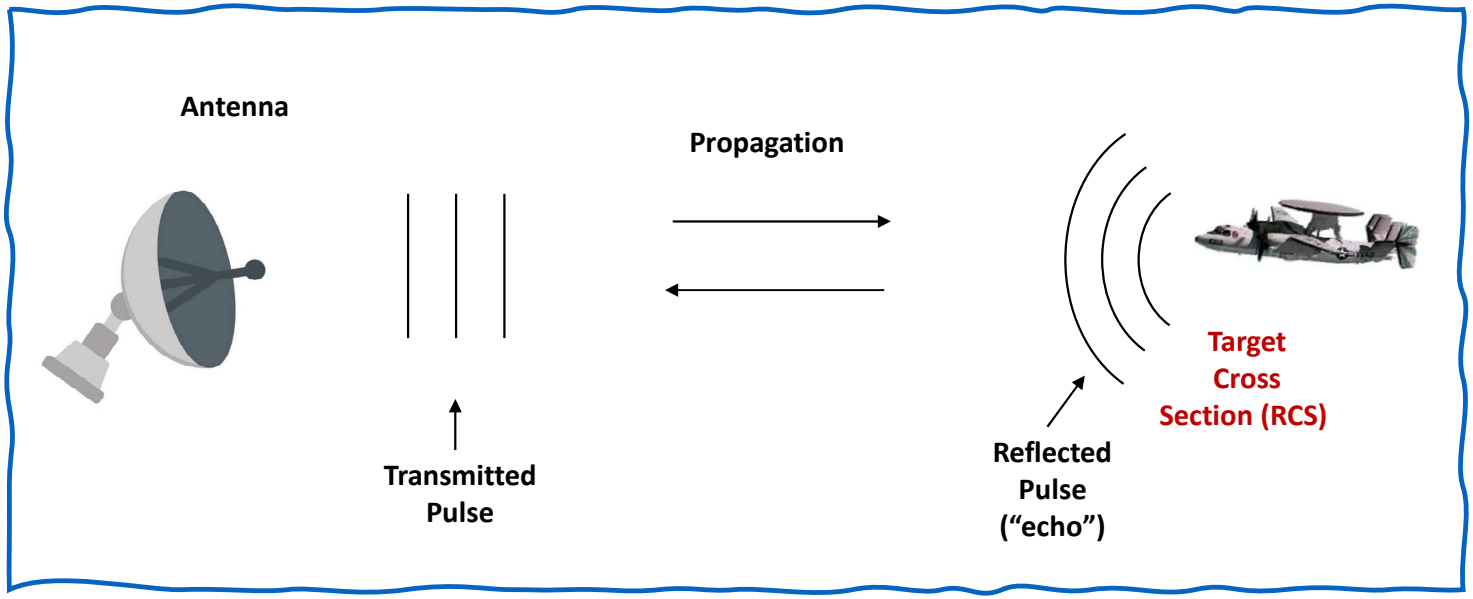
Figure by MIT OCW.

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)

Technical ELINT

Signal structure

Emission characteristics

Modes of operation

Emitter functions

Weapons systems associations of such emitters as radars, beacons, jammers, and navigational signals.

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.

Collection and Exploitation of Signals

- SIGINT, or signals intelligence, is intelligence gathered from communications, electronics, or foreign instrumentation.
- Collection and exploitation of signals transmitted from various emitters, communication systems, radars, IR/EO, and weapon systems.

RF Spectrum Mapping

- Radio frequency (RF) spectrum mapping; eavesdropping, jamming, and hijacking of communication systems
    - The least-threatening and most-prolific form of signals exploitation is eavesdropping, which also provides the one capability that is clearly SIGINT, rather than electronic warfare.

Externals vs. Signal Internals

SIGNAL EXTERNALS PROVIDE SUCH INFORMATION AS THE STRENGTH, FREQUENCY, AND MODULATION OF THE SIGNAL AND CAN BE USED TO ANALYZE TRAFFIC FLOWS, TRAFFIC PATTERNS, AND NETWORK ACTIVITY. SUCH INFORMATION CAN, FOR EXAMPLE, BE USED TO IMPROVE NETWORK MANAGEMENT.

SIGNAL INTERNALS, BY CONTRAST, REVEAL THE MESSAGE CONTENT BEING TRANSMITTED AND MAY REQUIRE DECRYPTION OR LANGUAGE TRANSLATION.

Discussions