Communications: Use

The Illiterate of the 21st century will not be those who cannot read and write, but those who cannot learn, unlearn, and relearn.

- Alvin Toffler

Radio Preparation and Rules

Preparation for use:

- Prepare to use your radio:
  - **READ** the Technical Manual (TM) of your radio. Look at the panel & connection diagrams and read the descriptions for use.
    - Damage or failure to properly communicate may result from "*just winging it*"
    - Many online resources such as YouTube or forum sources exist to sub a TM
  - Inspect the radio for damage such as missing knobs/dials
- Operating Tips:
  - Use a hand or headset if the incoming signal is weak instead of a loudspeaker
  - Manage your cables! A simple set of Velcro or Zip ties can prevent damage!
  - Check the operation of the radio before departure (is the battery charged?)

What is Forbidden?

- **Violation of a Radio Silence order**
- Transmission on a net without approved permission to do so
- Excessive testing or tuning
- Profane or obscene language
- Unauthorized use of plain language (refer to SOP for Radio Comms)
- Unofficial or casual conversation
- Non-use of Phonetic Alphabet
- Not using your call sign or the call sign of another in messages

Radio Operational Considerations

Site Selection - Location:

- **Location**: Always pick a primary and alternate site
  - Hills/Mountains between stations limit range, pick the high ground
  - Wet ground or bodies of water surrounding the radio increase range
  - Avoid foliage for the antenna, but use trees for concealment
  - Avoid buildings, overhead power lines, large metal structures (bridges)

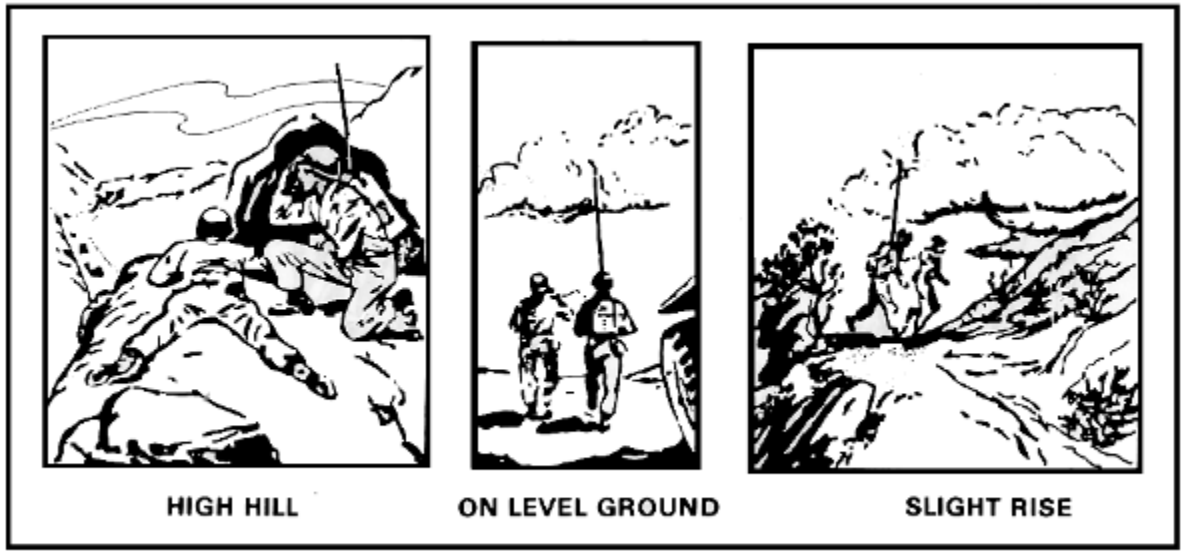


Figure 4-1. Good sites for radio communications.

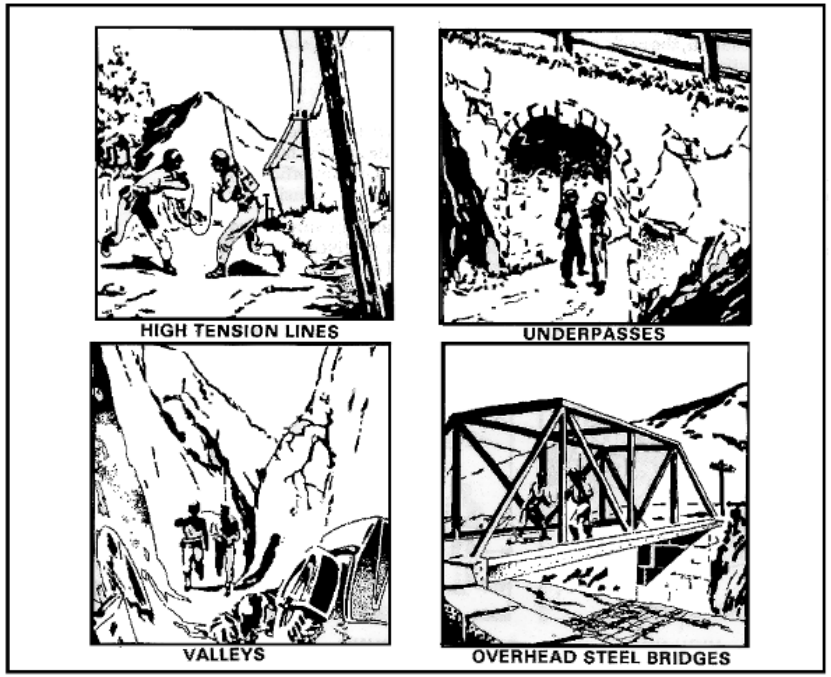


Figure 4-2. Poor sites for radio communications.

Site Selection – Tactics:

- **Command**: Locate stations away from the HQ/Command Post
  - Enemy Radio Direction Finding (RDF) on the station can attract bombardment
- **Cover & Concealment**: Locations should provide protection
  - Perfect Cover & Concealment impairs comms, choose a permissible amount depending on the range needed
- **Practicality**:
  - Remotely control if possible - operator is concealed while radio exposed
  - Whip antennas are hard to see but have 360° coverage, vulnerable to listening
  - Avoid open crests of hills, position somewhere safe behind the crests
  - Camouflage antennas and stations from aerial and ground observation, however **do not allow** antennas to touch foliage or camo material

Interference:

- **Natural Sources**:
  - Electrical, Solar, and Cosmic Storms
  - Precipitation static from charged particles (rain, snow, sand, smoke, and dust)
- **Man-made Interference**:
  - Machines (power lines, car engines, generators, motor, electronics)
  - Most man-made interference is vertically polarized, a **horizontal antenna** will reduce the amount of noise in the signal

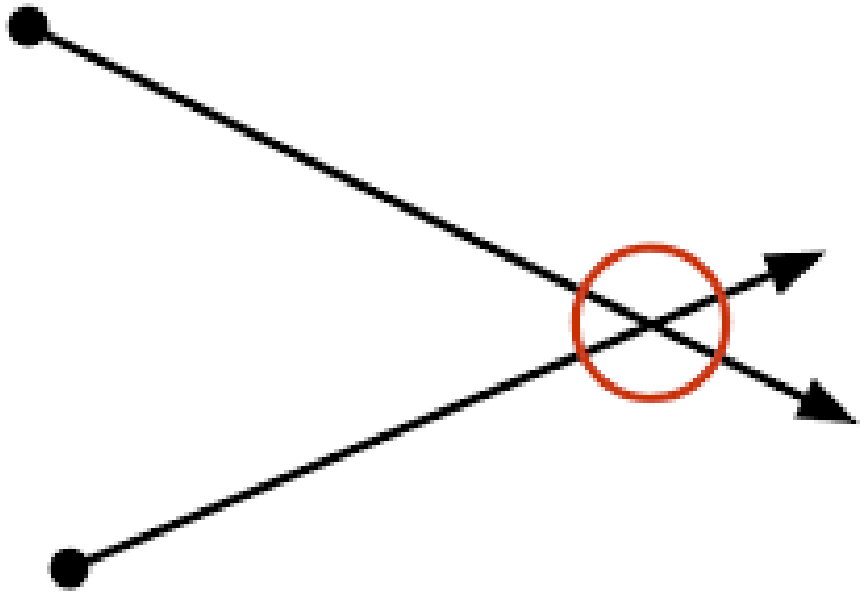
Electronic Warfare (EW)

EW – Interception:

- **Understand EW – What can the enemy do to us?**
  - **Interception**: The enemy knows you are here and given the number of stations operating on the same frequency, can estimate the size of your unit
  - **Interception**: If operating in the clear (un-encrypted) the enemy can understand exactly what you are saying
  - **Interception**: Via radio traffic pattern analysis, the enemy can easily figure out the Net Control Station (NCS) and identify the location of the HQ. Even without retaliatory action an increase in radio traffic may indicate to the enemy that an attack or movement is imminent.

EW – Radio Direction Finding:

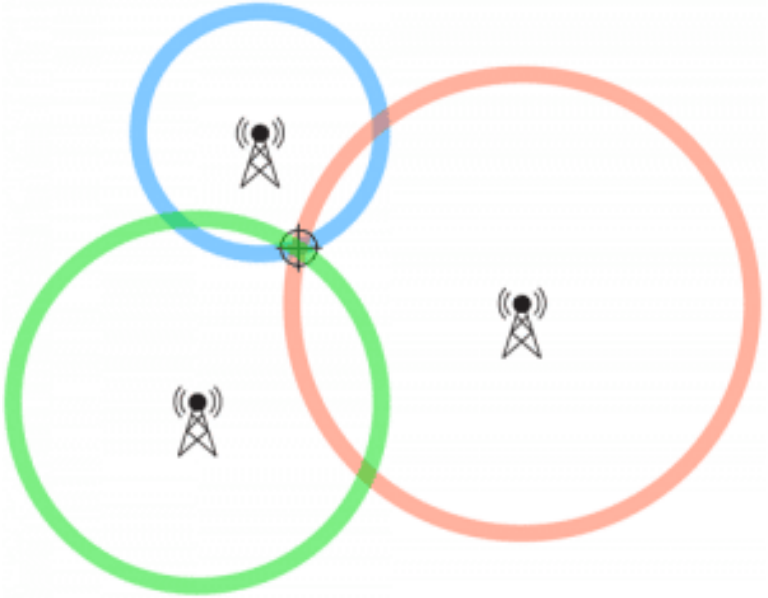
- **Understand EW – How can the enemy find us?**
  - **Radio Direction Finding (RDF)**: Via directional antennas the enemy may find the azimuth (bearing) of our position. If the enemy intercepts our transmissions with another bearing, we've been **cut** – the distance is known.



EW – Radio Direction Finding:

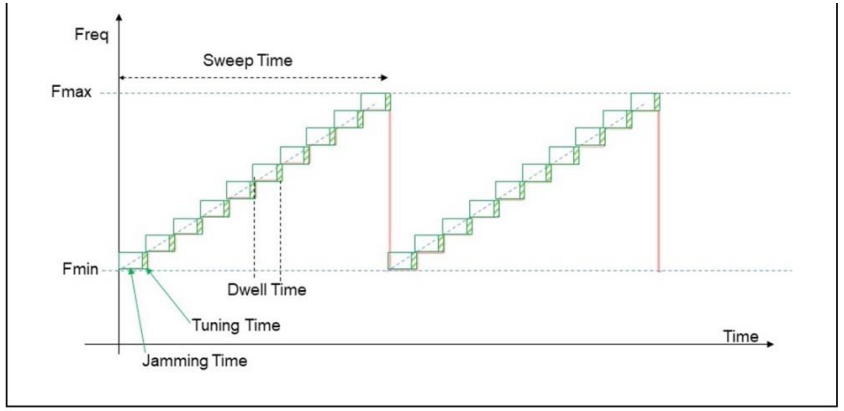
- **Understand EW – How can the enemy find us?**
  - **Radio Direction Finding (RDF)**: The interception of 3 or more bearings results in a **fix** and gives our location (aka *Triangulation*)
    - **Fixes** are often imperfect given conditions and equipment, but are enough to feed intel analysists a targeting area (artillery or airstrikes). Airborne RDF is much more accurate than ground-based, be aware of any airborne bogeys!

***Tip:** Lower power transmissions decrease the likelihood of a fix!

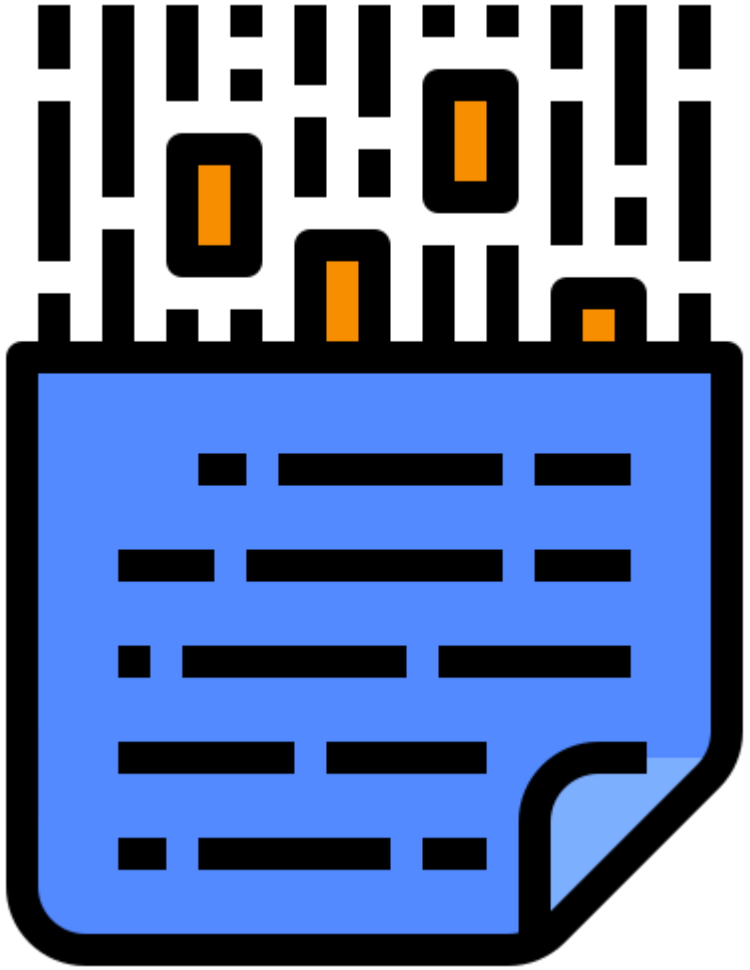


EW – Jamming:

- **Understand EW – How can the enemy screw with us?**
  - **Jamming**: The enemy does not need to destroy transmitting stations, simply jamming the receiver stations prevents communication.
    - With the same frequency and mode and enough power, messages won't get through!
  - **Jamming**: Many types of jamming can be used against you, some which cannot be detected! How to tell if you are being jammed:
    - Other station has been silent for an inordinate amount of time
    - The following signal noise tones are observed: Random, Stepped, Rotary, Pulse, *Wobbler*, Recorded Sounds, and **Sweep-through**



Emission Security & Transmission Security

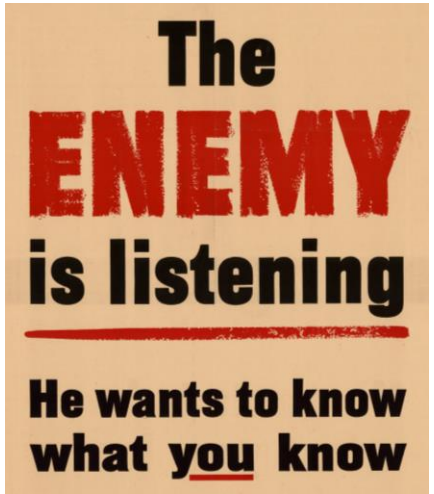


Signal Security (SIGSEC) - ENCON:

- **<u>Goal</u>: Ensure friendly use of radios is not exploitable by the enemy**
- **Emissions Control (ENCON): Do not transmit unless necessary for the mission!**
  - Make short transmissions, mask antenna locations, use directional antennas, and use the lowest possible power output to protect from enemy EW
  - **Radio Silence:** Can be used for deception if some stations operate on a free net and others remain silent unless in an emergency.
    - If the doesn't know we are out there (because he cannot pick up transmissions), he cannot target us nor jam us!

SIGSEC - TRANSEC:

- **A message transmitted in the clear is the enemy's greatest source of info!**
- **Transmission Security (TRANSEC):**
  - When the radio must be used, *keep transmission time to an absolute minimum* (**15 seconds MAX**), preplan messages to avoid sending compromising info or taking too long to transmit
  - Use brevity codes and encrypt the message if possible, rotate frequencies
  - Use authentication checks (such as a password or leader/follower statement) to prevent enemy imitative electronic deception



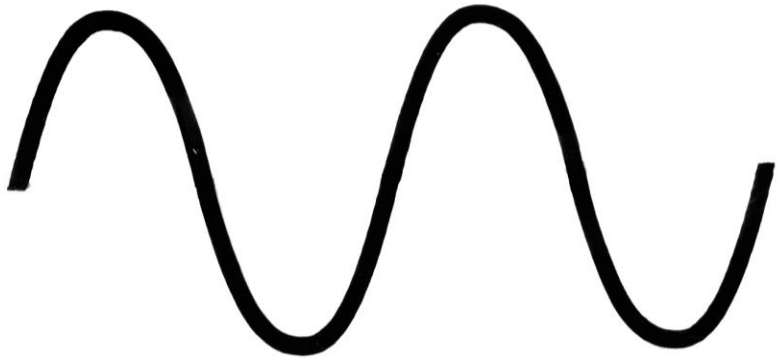
SIGSEC – Crypto & Physical Security:

- **Crypto Security deals with codes, keys, and COMSEC devices**
  - If you use an encryption method, the enemy cannot understand the message
    - **This is a false sense of security**, as if the enemy cannot get information he might attempt to jam or destroy the radio operator
- **Physical Security:** Common sense, do not let your radio get stolen or used by others. Destroy it if you know you will be captured.

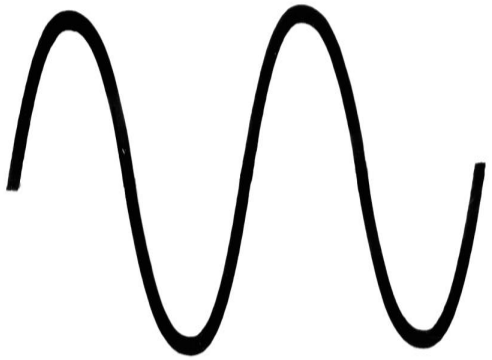
Radio Operation in Unusual Conditions

Choosing Frequencies for the Terrain:

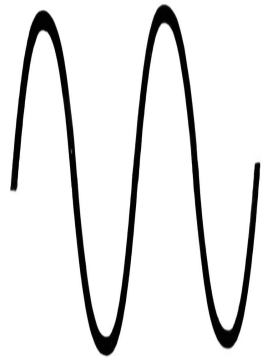
- **Shortwave radios operate in nearly all environments, but frequencies used on handhelds have issues in certain conditions**
  - This is because the wavelength requires room to avoid obstacles, shorter wavelengths are preferred in dense environments



VHF: Best in open terrain such as deserts, ocean, or the arctic – has the best range
-Can also duct using tropospheric conditions to "skip" over obstacles like mountains



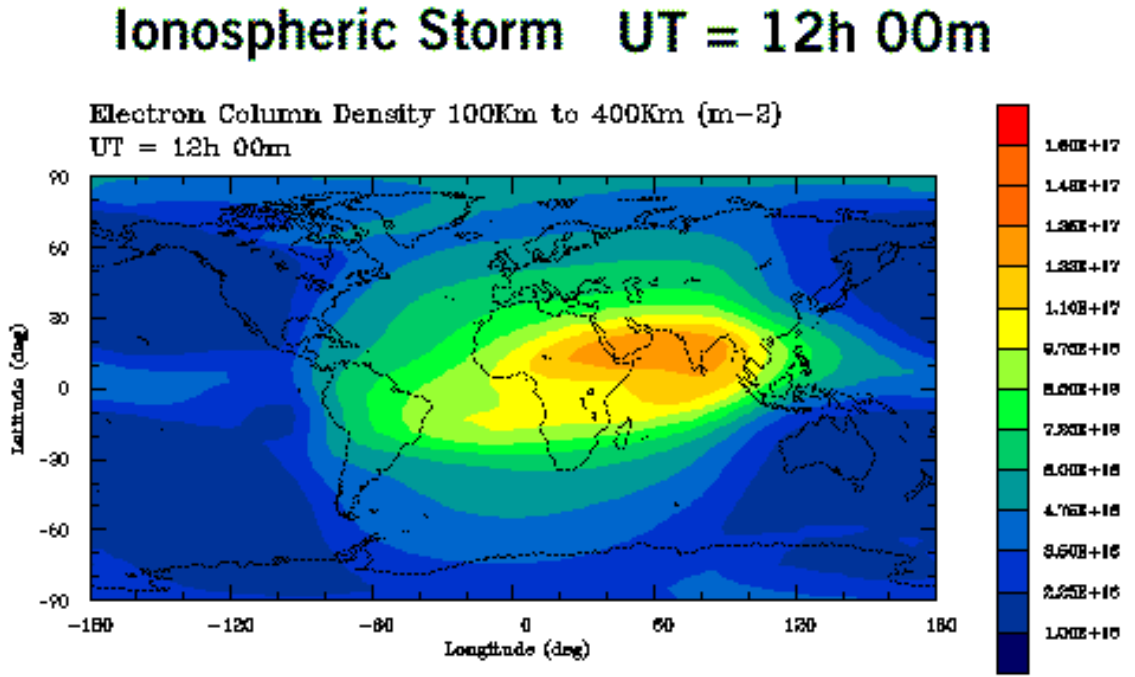
UHF: Best in more constrained environments such as woodland, jungle, or urban terrain



High UHF (700-900 MHz) or GHz: Best inside buildings or subterranean environments – has short range everywhere else

Arctic Conditions:

- **Limitations in Arctic Environments:**
  - **Ionospheric Disturbances**: Extremely cold areas tend to have more ionospheric storms and may completely block out certain frequencies for minutes or weeks at a time with strong static
    - Auroral activity (Northern Lights) may cause complete failure of comms



Arctic Conditions:

- **How to operate in Arctic Environments:**
  - Try to operate from vehicles or bases to help shelter for the operator
  - Deep snow and permafrost make it difficult to establish good electrical ground so *use a counterpoise* (but remember to keep it above the snow)
  - Frozen ground has poor conductivity ➔ Little to no groundwave propagation
  - Masts and cables for antennas will be brittle from the cold, be careful
  - A permanent antenna should have extra guy wires, preferably made from synthetics, to withstand heavy ice and wind loading.
  - Try warming up the battery for the radio set with body heat before use
  - Your breath moisture may freeze on the microphone so use a cover
  - Before cold radios are brought into warmth, wrap them up to prevent sweating on the radio, ensure all equipment is thoroughly dry before going back out

Jungle/Tropical Conditions:

- **Limitations in Jungle/Tropical Environments:**
  - Hot and humid environments increase maintenance needs for radios
  - Thick jungle growth acts like a vertically polarized absorbing screen for radio waves, antenna siting and selection is important

Jungle/Tropical Conditions:

- **How to operate in Jungle/Tropical Environments:**
  - Antennas should be located in clearings and as high as possible
  - Antenna cables/connectors should be kept off the ground to prevent moisture, fungus, or insect damage.
  - Dipole and ground plane antennas are more effective than whips – *horizontally polarized* antennas should be used
  - Vegetation must be cleared – wet foliage will ground a signal
  - Keep radios as dry as possible and in lighted areas to prevent fungus

Desert Conditions:

- **Limitations in Desert Environments:**
  - Desert terrain has poor electrical grounding so counterpoises are needed along with using complete antennas such as dipoles over whips as they would in jungle environments

Desert Conditions:

- **How to operate in Desert Environments:**
  - Keep radios out of the sun (overheating & battery drain)
  - Condensation may develop on equipment overnight, use tape for insulation
  - Sand will find its way into EVERYTHING, keep a toothbrush to clean out parts
  - Static electricity is prevalent in the Desert, ensure there is proper grounding for the antenna as well as insulation (via tape) on antenna edges to cut down on the noise
    - Static effect is less prevalent at higher frequencies, use these over lower ones

Mountains:

- **Limitations in Mountainous Environments:**
  - Same problems as in arctic terrains, transmission site selection critical
- **How to operate in Mountainous Environments:**
  - Relay stations become necessary (explained later)
  - Most transmissions will be Line of Sight (LOS) and groundwave propagation often impossible (poor ground conduction), thus a diploe (NVIS) or ground-plane antenna with a counterpoise should be used.
  - Maintenance needs are often similar as in arctic terrains

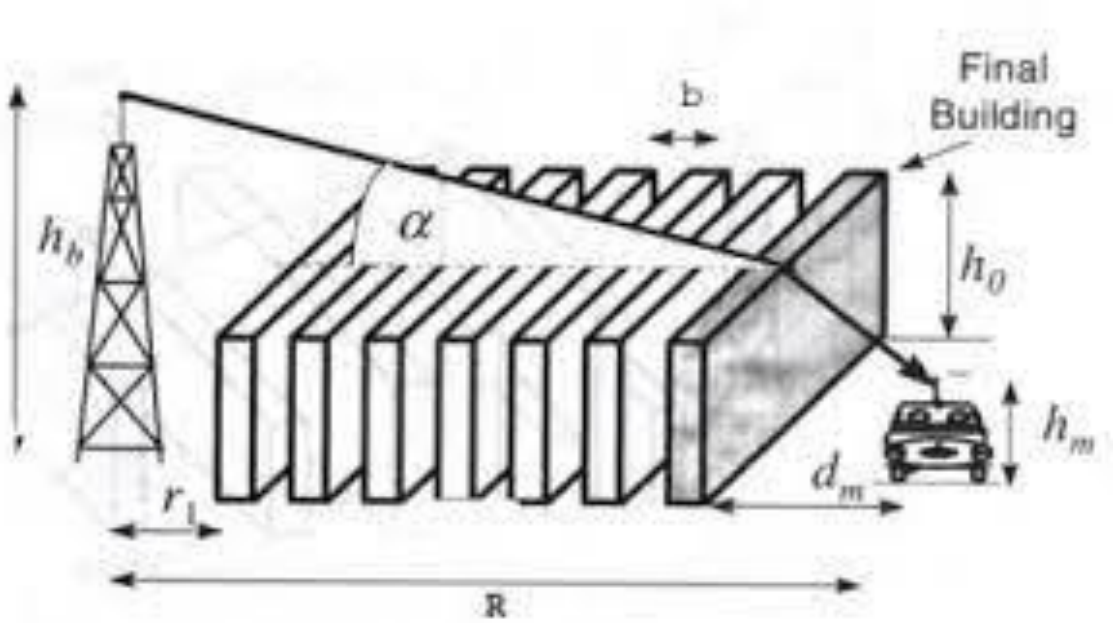
Radio Operation in Special Environments

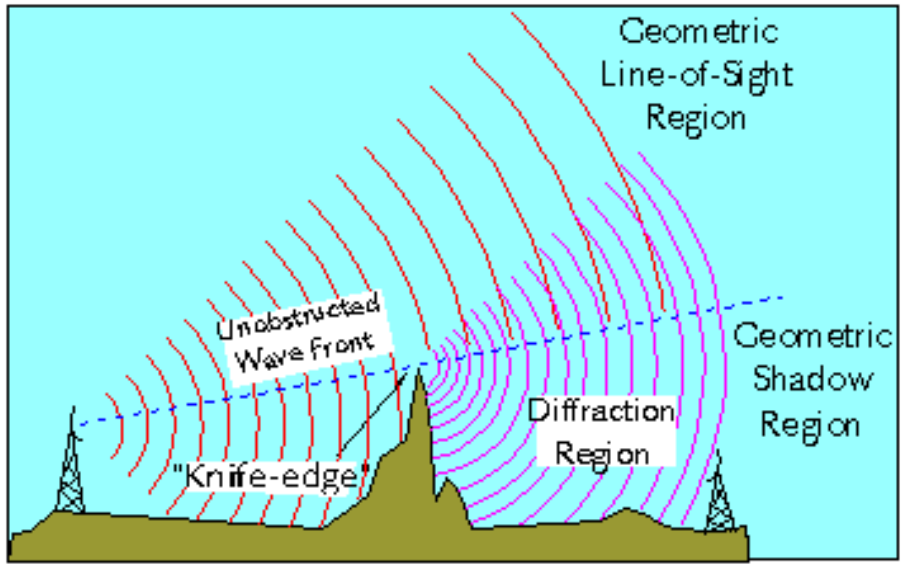
Urban Terrain:

- **Problems and tips for operating in an Urbanized Environment:**
  - Buildings and other obstacles will block transmission paths
  - Paved surfaces have poor conductivity – Need counterpoise
  - Powerlines and commercial radio stations generate noise
  - VHF is not effective in urban terrain, requires LOS which may be impossible
  - HF radios generally require NVIS antennas and may need a retransmission station to communicate with smaller units
  - Antennas MUST be concealed or blend in with surroundings to avoid the enemy using it to home in for bombardment, consider using water towers, civilian antenna towers, and church steeples
  - Store radio equipment inside buildings, ideally basements

Urban Terrain – Knife Edge Diffraction:

- **Buildings block radio waves, but can help make comms easier:**
  - Sharp, non-conductive objects (like mountain peaks or buildings) can cause radio waves to diffract over the top and down, allowing non-LOS comms
  - Use to advantage to communicate to smaller units around a high point
  - The enemy could also hear you even when concealed from sight





knife-edge effect

CBRN Environment:

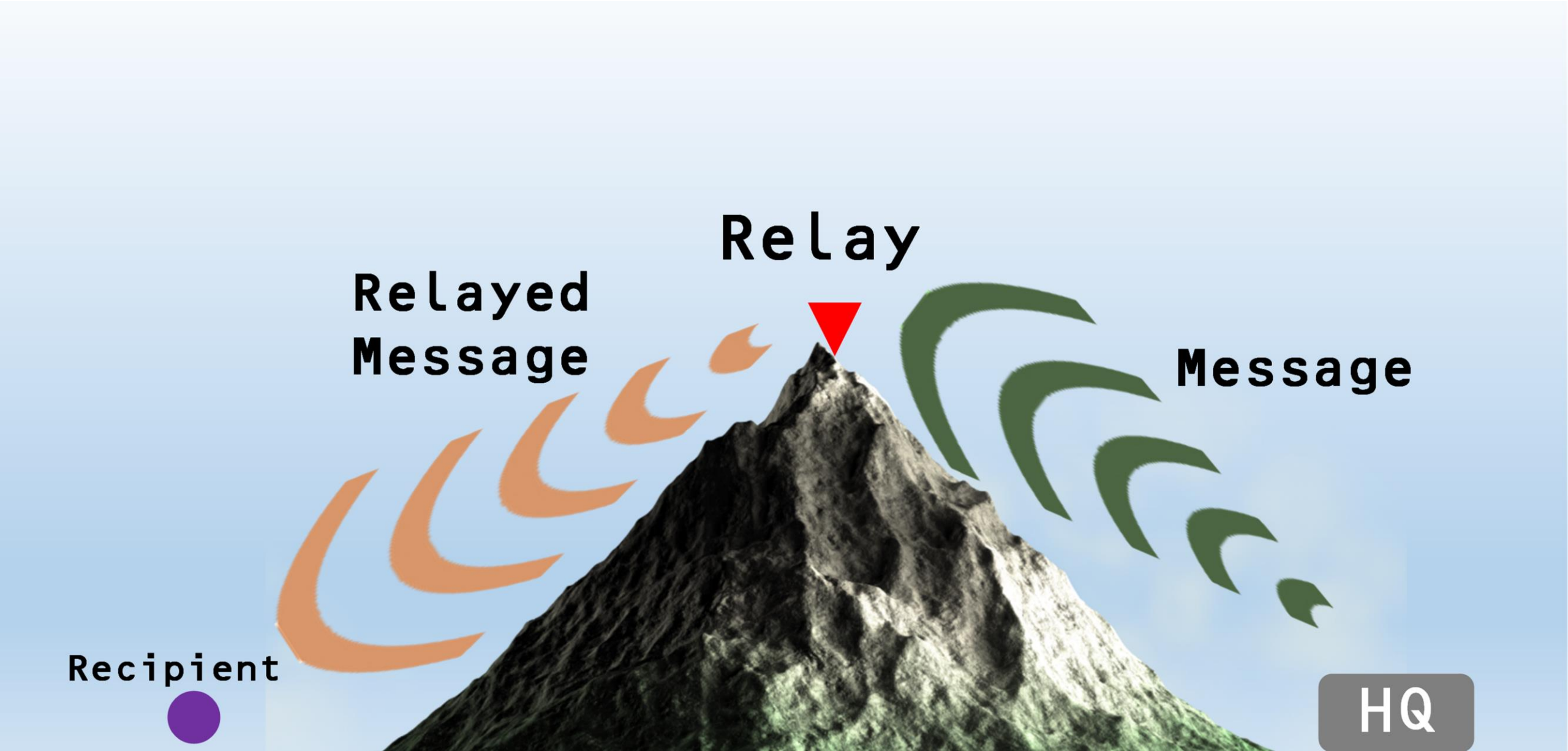
- **Dangers of a CBRN Environment:**
  - Nuclear weapons generate an Electromagnetic Pulse (EMP) which can enter the radio through the antenna or power system connections, breaking down or melting circuit components – destroying the radio
    - Harden against EMPs by making sure no antennas or cables are connected to a radio when not in use. Good grounding is a must against an EMP.
    - Radios may be stored in an EMP shield to prevent damage, any large and well sealed metal container (trash can) will work as long as the radio doesn't touch the body
  - If using a respirator, make sure you have the proper connections for a microphone and speaker to the mask

Relaying Techniques

Relaying:

- **Relaying Concept and use:**
  - Due to distance or elevation changes sometimes direct comms between a unit and another or HQ is not possible. Thus, radio operators should have posts in-between the points of contact to server as *relays.*
  - A relay receives the message from one operator then retransmits the message to the intended recipient. Ideally the relay is located at a high elevation.
  - Relaying should be conducted on separate frequencies as to avoid confusion and prevent easy jamming for the receivers
  - Relaying should be accomplished using directional antennas (COMSEC), thus the relaying station(s) should have **known, fixed locations**
  - Some automatic devices such as repeaters may be set up to act as relays

Relaying Example



EAPs/PACE Plans

EAPs/PACE:

- **Emergency Action Plans (EAPs) & PACE:**
  - Comms are a fragile and easily countered in a modern threat environment, therefore we need EAPs in place before missions so squads may act instantly
  - A proper EAP is short and covers all possible mitigating actions – a PACE Plan is an example of an EAP
  - **P**rimary, **A**lternate, **C**ontingency, and **E**mergency – When one method of comms fails or is compromised, immediately use the next available option
  - Typically PACE includes the use of different frequency bands or types of radios
  - PACE should also consider one-way messages, if encryption is not possible use a One Time Pad (OTP)

Example PACE Overview:

P	TAC Channels – Encrypted
A	Backup Frequencies – GMRS
C	Smart Phone Messaging App OR Lo-Ra
E	HQ gives one-way orders over HF

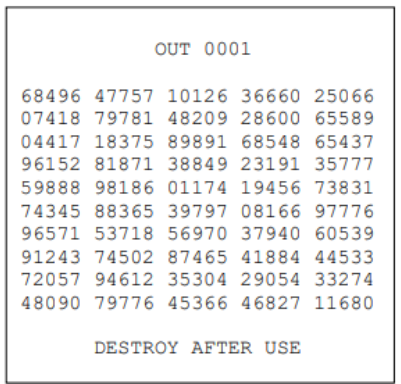
One Time Pad (OTP)

CODE TABLE NO.1

000 ABORT	253 DECODE	505 MILITARY	758 STREET
019 ACCEPT	262 DELAY	514 MONEY	767 SUBWAY
028 ACCESS	271 DIFFICULT	523 MONTH	776 SUCCESS
037 ADDRESS	280 DOCUMENT	532 MORNING	785 SUPPLY
046 AFFIRMATIVE	299 ENCODE	541 MORSE	794 SUPPORT
055 AGENT	307 EVENING	550 NEGATIVE	802 TELEPHONE
064 AIRPLANE	316 EXECUTE	569 NIGHT	811 TODAY
073 AIRPORT	325 FACTORY	578 OBSERVATION	820 TOMORROW
082 ANSWER	334 FAILED	587 PASSPORT	839 TRAIN
091 AUTHORITY	343 FERRY	596 PERSON	848 TRANSFER
109 BETWEEN	352 FLIGHT	604 PHOTOGRAPH	857 TRANSMIT
118 BORDER	361 FREQUENCY	613 POSITIVE	866 TRAVEL
127 BUILDING	370 HARBOUR	622 POSSIBLE	875 TRUCK
136 CANCEL	389 HELICOPTER	631 POWER	884 UNABLE TO
145 CHANGE	398 HIGHWAY	640 PRIORITY	893 URGENT
154 CIVILIAN	406 IDENTITY	659 PROBLEM	901 VERIFY
163 COMPROMISE	415 IMMEDIATE	668 QUESTION	910 WEEK
172 COMPUTER	424 IMPOSSIBLE	677 RADIO	929 WITHIN
181 CONFIRM	433 INFORMATION	686 RECEIVE	938 YESTERDAY
190 CONTACT	442 INSTRUCTIONS	695 RENDEZVOUS	947 .....
208 COORDINATE	451 LOCATE	703 REPEAT	956 .....
217 COUNTRY	460 LOCATION	712 RESERVATION	965 .....
226 COVERT	479 MAIL	721 ROUTINE	974 .....
235 CURRENT	488 MEETING	730 SATELLITE	983 .....
244 DANGER	497 MESSAGE	749 SHIP	992 .....

One Time Pads (OTP):

- **OTP Theory:**
  - While Digital Encryption for radios does exist and should be used, they are not 100% reliable for keeping messages safe
  - The only unbreakable form of encryption is the OTP and the message can be transmitted over analog, unsecured channels
  - As the name implies the cipher should only be used one-time to ensure the code cannot be figured out and decrypted by enemy
  - When to use OTPs: Sensitive Operations, one-way communication from an HQ to squads, when the possibility of enemy interception of messages exist



One Time Pads (OTP):

- **OTP Use:**
  - Follow OTP SOP to learn how to decode. Make sure at least 2 per squad (ideally commander and radio operator) are trained in decoding a OTP.
  - OTPs must be prepared ahead of time and securely kept in a booklet, as they are used the page with the key is ripped out and destroyed
  - Keep messages short and simple, use brevity codes to make messages shorter
  - Always repeat the key number and message at least twice to ensure the message is not decoded wrong or parts missed

Near-Vertical Incident Sky-Wave (NVIS) Antenna

HF Comms:

- **High Frequency (HF) Comms:**
  - Fast-moving or distant units often may only be communicated with HF
  - Under ideal conditions a ground wave from a vertical antenna has a max of about 50 miles, with worse conditions being only a couple miles. Sky waves will not return to Earth under 100 miles away, leaving a 50-75 mile wide zone where HF comms will not function.
  - NVIS antennas solve these 2 crucial issues with comms

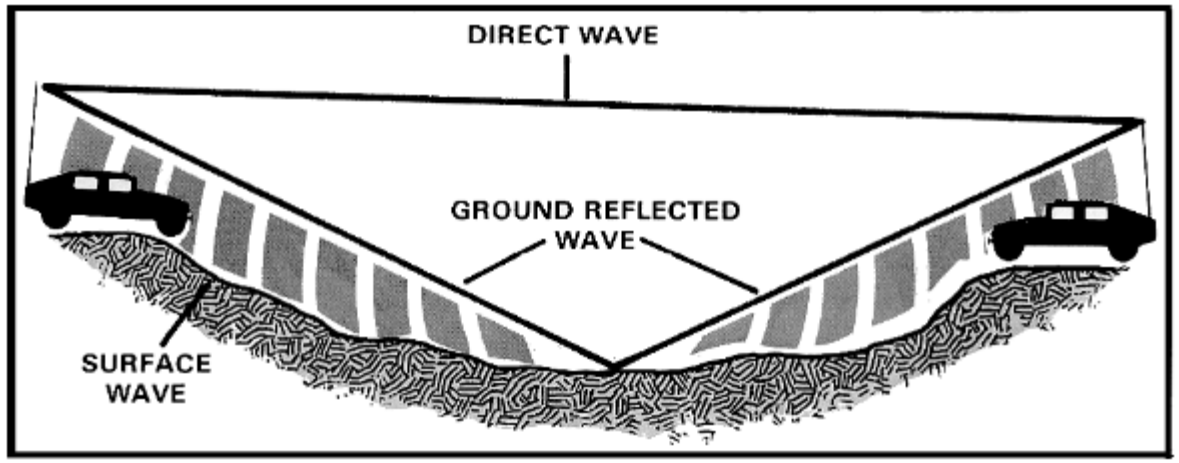
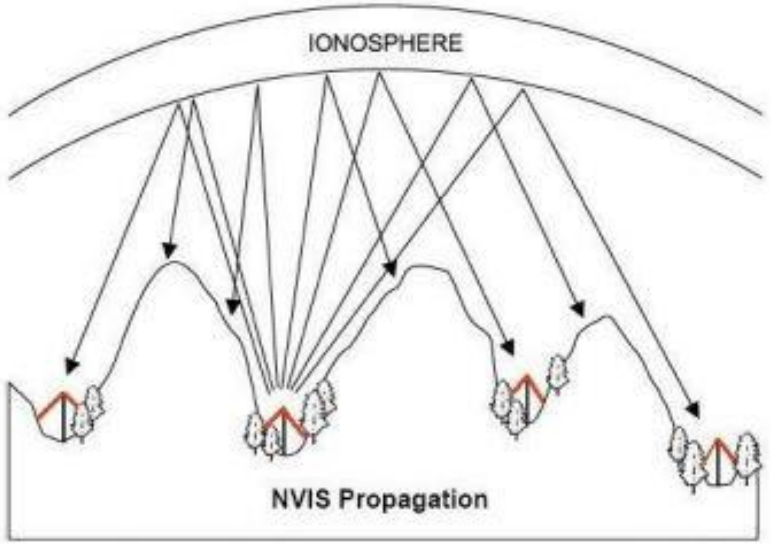
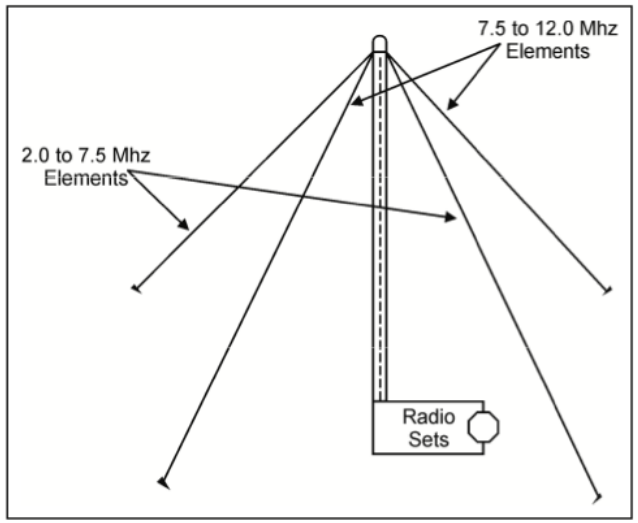


Figure 2-12. Possible routes for ground waves.

NVIS Concept:

- **NVIS:**
  - Waves radiated at too high of a frequency will continue into space, but at low enough frequencies it is reflected back to Earth at all angles, omnidirectionally, without a skip zone. This is a NVIS antenna.
  - NVIS antennas must radiate energy at angles >75° and should be a quarter wavelength off the ground and use 1.8-10 MHz frequencies
    - Typically a dipole, sloper, or loop antenna is used for NVIS





NVIS antenna, AS-2259/GR

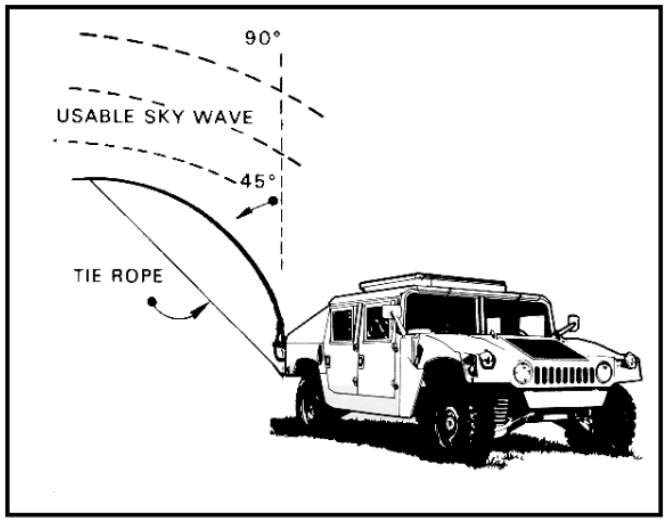


Figure M-9. Tying the whip antenna down.

Use of NVIS:

- **Advantages:**
  - Antenna directionality of little importance
  - Operator can be in a fixed, dug-in position at lower elevations
  - Terrain and foliage do not interfere with the radio waves
  - Hard to RDF locate, harder to jam, can use lower power
- **Disadvantages**:
  - Not good for long-range comms (≈300+ miles)
  - Improper antenna setup can cause ground waves to destructively interfere with the NVIS wave
  - Limited frequently range (2-4 MHz night & 4-10 MHz day)

END: START THE CLIMB