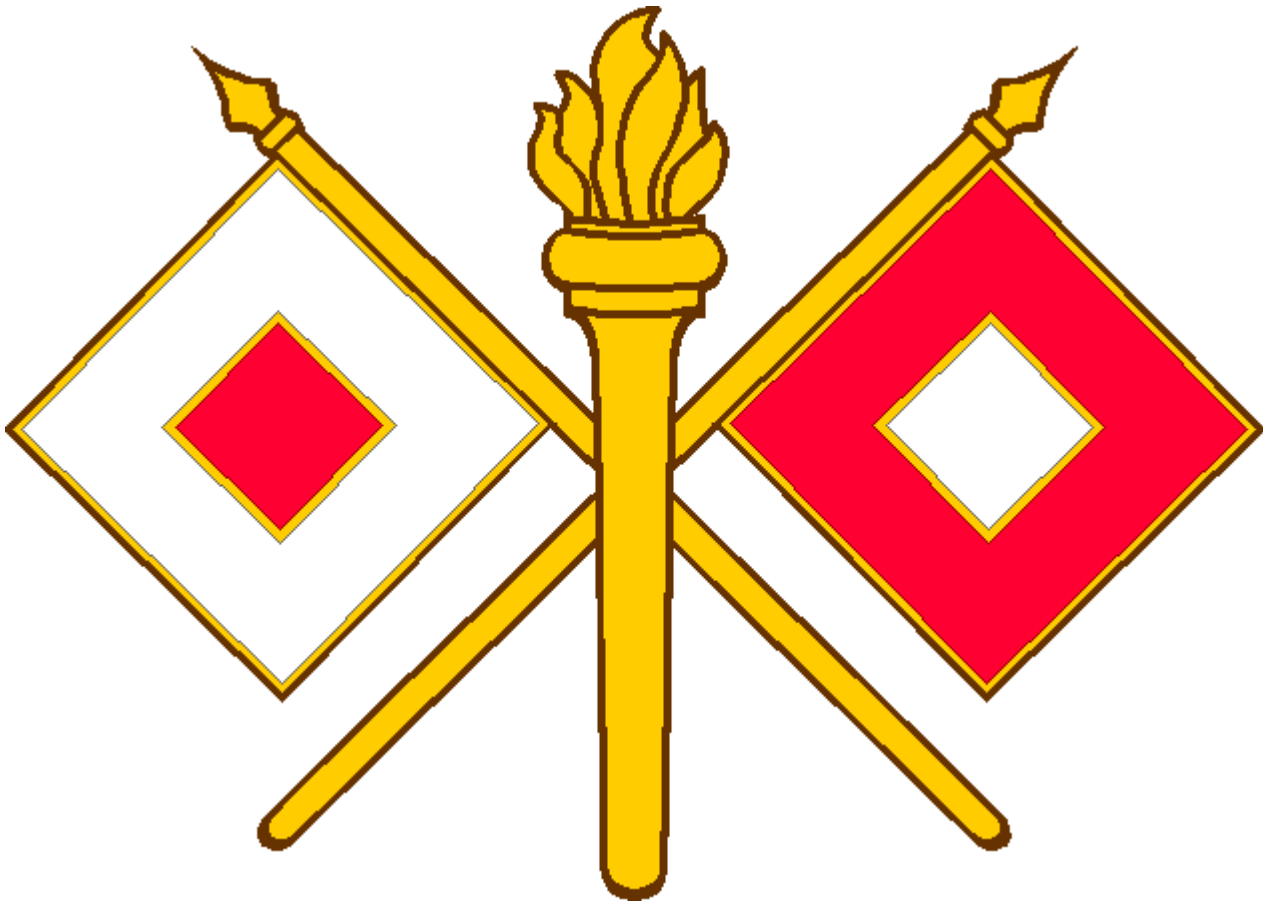


Signals Handbook for Small Teams

Volume 1:

Squad level and lower level communications.
Fundamentals.
Basic Manual Encryption.

1st Edition

Legal

Thanks

A special thanks to those that helped with this work:

Major Wiliam Cross, CSMR (Ret.)
Sgt Dan Morgan (Ret.)
Spc4 Thomas Dubas (Ret.)

And Thanks to My wife for putting up with my working on this project.

Table of Contents

Preface

Community protection teams, mutual assistance groups, airsofters, paintballers, constitutional militias, private security contractors, and even friends and family coming together for the common defense during a time of crisis, all have a myriad of modern communications devices available to them these days, but there has been little cohesive instruction for effective use of radios in a “tactical” situation.

We can find information on the internet, and in army field manuals, but that information is often piecemeal and not always relevant. Many military manuals are very equipment specific, and the Army communications structure has a tremendous amount of supporting staff and infrastructure that just is not available to a small group.

This series of handbooks is an attempt to provide a set of guidelines for effective tactical use of radios among small units, that will be universally relevant.

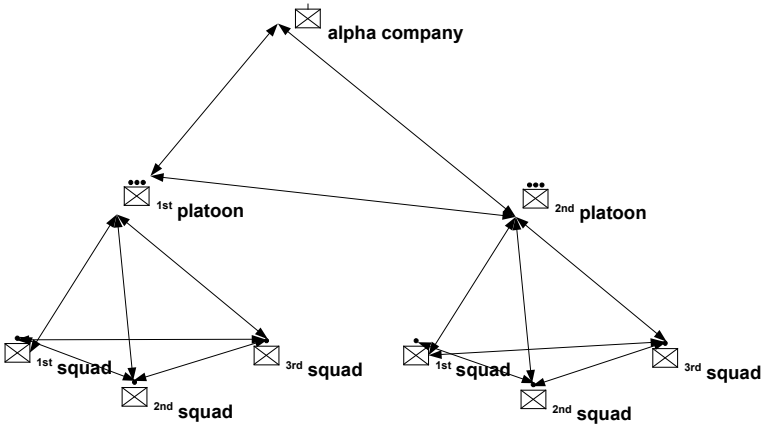
This volume, Volume One, focuses on handheld team and squad level radios. This is information everyone in a unit should know. It covers the fundamentals, and progresses to more advanced information.

Volume Two focuses on tasks that should fall under the responsibilities of the “radio guy” or signals officer. It expands upon the information in Volume One, and covers more administrative and planning topics.

Volume Three focuses on signals intelligence, scanning, jamming and electronic warfare.

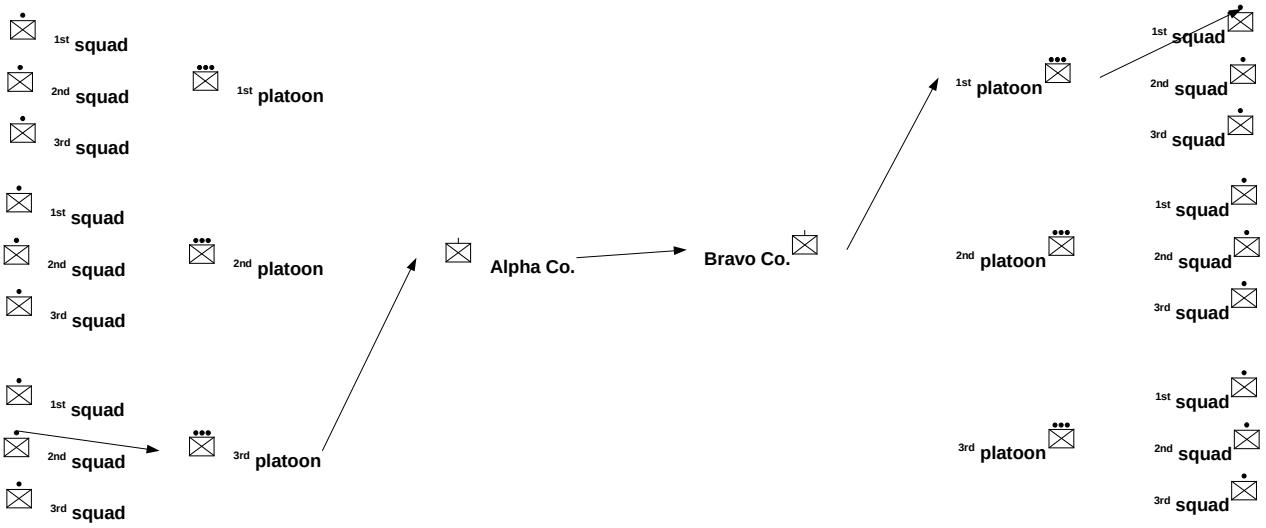
I. Introduction

"Shoot, Move Communicate!" That is the defining structure of modern small unit maneuver warfare.
For small tactical teams, we tend to model their operations on military procedures. The U.S. Army has a very hierarchical radio communications structure. A "squad radio" usually allows a squad leader to communicate to their next higher in the chain of command, the platoon leader. That channel of communication is shared by all the units within an echelon, under a command, so a squad leader can also communicate with other squad leaders within the same platoon as well. The platoon leadership will also have a channel of communications to their next higher chain of command, the company commander, and to the other platoons within their company.



In order for a squad in one chain of command to communicate to a unit in another chain of command, a message will go up the chain of command until it reaches a common parent unit, and then back down to the destination unit.

For example: 1st squad, 3rd platoon, Alpha company, needs to send a message to 1st squad, 1st platoon, Bravo company. The message would go from 1st squad to 3rd platoons radio operator, who would then pass it to Alpha companies radio operator, who would then pass it to Bravo companies operator (since they share the same "net" with their common battalion command.) Then Bravo companies operator would send the message to their own 1st platoon, which would then send it to their 1st squad.



Since this handbook is geared towards the tactical use of radios for small units, It will focus on the platoon level and below level of communications. The primary focus will be handheld radios. It is radio band and brand agnostic. It does not matter if the radios are HAM, CB, FRS, GMRS, MURS, DTR, land mobile, military surplus, public safety, marine VHF, IP based, or something else altogether. The procedures outlined here will facilitate better radio usage for any radio type.

From left to right; FRS, CB, HAM, Land Mobile, VHF Marine, & DirecTalk phone.

Realistically, radios such as these will only be able to communicate effectively for a mile or two, or even less, depending on the power level of the radio, terrain, and local RF noise.

II. Equipment needed.

In order for two people to effectively communicate via tactical radios, they will need some equipment:

A) Radios that operate on the same bands and modes. "Bands" are the range of frequencies that a radio operates on. Usually a "band" will coincide with the legal defined frequencies of a particular radio service. A FRS band radio operates on the frequencies that the FCC has set aside for FRS radios. A ham radio may operate on a number of ham "bands" defined by the FCC.

"Mode" describes the method by which a radio transmits and receives. AM, FM, and SSB are all different modes. If everyone in a unit has a radio that operates on a different radio band, or uses a different mode, then the radios are fairly useless. A small unit should standardize on what radio bands and modes will be used. Standardizing on brands or families of radios can also be useful because they will share common accessories.

1. Radios should be able to accept AA or AAA batteries, in addition to having rechargeable batteries. If there is a choice, use AA, as they have twice the capacity/runtime s AAA batteries. Long duration missions will quickly deplete rechargeable batteries, and it is much easier to source a local supply of common batteries, in order to be able to continue the mission. Some radios can accept regular batteries without modification, while others may need a special battery box or compartment in order to do so. As the batteries age, the run time goes down. You should have multiple batteries, and multiple chargers. Using a radio for 8 hours a day in a shooting class, and then recharging them in the hotel that night doesn't necessarily reflect real world usage. DO a field exercise.... how do your batteries really hold up. Remember, batteries don't do as well in cold weather. You may need to store spares against your body, to have them function. Get a baseline on how much normal usage your radio will last on a battery. Then pack at least as many batteries for the duration of your mission... then add 30 percent spares... It might last.

Having multiple ways to power your radio can be a life saver. Having a AA, or AAA battery pack, and adapter cables to power your radio off of a cigarette lighter, or car battery from alligator clips, are also highly recommended.

Rechargable battery, AA Pack, Cigaret Lighter, and power poles all as power methods

AA batteries may also be available from fire departments, and emergency services if your group is working in conjunction with local authorities.

2. It is preferable that radios at least be weather resistant/ weather proof. Waterproof is even better. Rain happens. Bad weather happens. A radio won't be very useful if it dies once it gets rained on. Waterproof helps if someone is forced to ford a body of water, or falls in water. Otherwise take precautions to protect a radio from water immersion. Small radios with “rubber duckie” antennas may be able to fit completely into zip-loc bags or clear “dry bags” for extra weather protection

3. Subdued or camouflage colors work better tactically than day-glo orange or safety yellow.

4.Antennas: Have several. Rubber duckies are durable, but fixed antennas may give you better range. A roll up j-pole, or antenna extension cable and some fishing line may allow you to temporarily get an antenna up in some trees, thus higher, thus longer range. Adapters to/from SMA, N, PL-239, Et.. turn-arounds, ect... allow you more improvised antenna options. Compatible directional antennas such as Yagi's and beams are also useful to reduce the chance of being detected, or slightly increase the range of a weak signal.

B) A secure radio pouch or holster. A radio pouch should lock securely. Positively locking buckles and zippers are good. Snaps and velcro can open up accidently, and should be avoided. Loosing a radio because a pouch came open not only reduces a teams ability to communicate, but also may give the enemy a working radio on the frequency that a unit is using, thus putting other friendly units in jeopardy. The pouch should securely attach to a persons gear. If non secure pouches are the only thing available, have the radio tethered to the person carrying it.

Many radios, or radio batteries have belt clips. I have found belt clips range from good to awful in quality. For light duty use, good belt clips are fine, however if you are using the radios in adverse conditions (crawling through bush, lots of dynamic movement, ect.)... you probably want something better than a belt clip.
Avoid MBITR radio holsters... MBITR's are huge, and most any other radio will be too small for a MBITR holster.

Radio in a Maxpedition radio holster

C) A handheld speaker microphone. Similar to the microphone a trucker uses on a CB radio, a speaker mic allows the radio to remain in it's pouch or holster while being used. If waterproof is an option, that s prefered. Some speaker mics also include a headphone jack, which is desirable if available.

Motorola Speaker/hand microphone

D) A headset, or earbud system. When noise discipline is a concern, having a radio speaker suddenly break the silence can compromise a unit, so a means of listening discreetly is a must. There are numerous systems that have pros and cons. Be aware that almost any headset will be hanging "stuff" outside your ear, thus occluding or attenuating some sounds so they will reduce your ability to hear outside sounds as well. This reduces your situational awareness.

Also, any headset or earbud system needs to be tested in a rigorous physical environment to insure that it stays in place and doesn't fall off. Small earbuds may benefit from using medical tape to hold cables in place, or even taping the bud in to the ear. Headsets may need headbands or straps to keep from falling off, especially when running, looking up or down, or when jumping.

Insure that microphones on headsets do not interfere with your cheek weld, when shouldering a rifle.

1. Open muff headsets. Open muff headsets tend to be lightweight headsets that do not completely enclose the ear. Since they do not enclose the ear, they don't reduce situational awareness as much as other forms of headsets. In high noise environments, open muff headsets tend to perform poorly, because they must compete with the ambient noise. They may come as "single muff" which only covers one ear, or "double muff" which covers both ears.

Heil Proset open muff headset

2. Closed muff headsets. Closed muff headsets completely cover the ear and usually are only double muff. By enclosing the ear, they reduce outside sounds. Closed muff headsets are good for high noise environments such as shooting ranges, helicopters, loud vehicles ect. The loud environments preclude good listening situational awareness, so using a closed muff headset in this case doesn't reduce any abilities. Using a closed muff headset in the field however, greatly hampers a persons ability to hear their surrounding, and should only be used in very special cases. Closed muff headsets can be very hot, and uncomfortable after prolonged use. They often cause sweaty ears in warm environments.

3. Electronic closed muff headsets. These are special type closed muff headsets. They incorporate battery powered microphones, that drive the speakers in the headset, allowing the wearer to hear the surrounding environment. They can often amplify sounds, actually improving the users situational awareness. Most electronic headset systems will mute the microphones if the sound is louder than a certain threshold, such as the firing of a gun, so those noises aren't amplified, and instead, are protected against. Electronic muff headsets are some of the most expensive headsets, and suffer the same discomfort issues as regular closed muff headsets. If the battery dies, or the electronics malfunction, it becomes an expensive closed muff headset.

TCI Liberator electronic closed cell headset

4.Earbuds. Earbuds are the small foam covered speakers that insert in the ear canal. Many Ipods and consumer personal audio devices use earbuds. Commercial audio earbuds can be used with a speaker microphone that has a headphone out port. Dedicated “surveillance earpices often have a speaker that clips to the back of a shirt collar, with a sound tube that goes to the ear, and a microphone and “Push To Talk' (PTT) button that clip to the users front centerline. Earbuds can be the least expensive option, but do dampen ambient sounds to reduce situational awareness.

Earbud with ear clip to hold it in place

Surveillance style earbud & microphone

5. Bone conduction headsets. Bone conduction headsets clip around the ear, and vibrate the bones in front of or behind the ears. The benefit of bone induction, is they do not occlude the ears at all, allowing full auditory situational awareness. They also allow a user to use regular hearing protection such as foam earplugs when needed. The downsides are that they are not good in high noise environments, and audio quality isn't great. Inexpensive consumer units tend to get poor reviews, do not stay on well, and have bad audio quality, where professional tactical sets review well, but cost several hundred dollars each.

E) Note taking tools. If a person is carrying a radio, they should also have the ability to take notes. They may need to record an encrypted message, pass a message along to another unit, record observations for later transmissions, note down long instructions, coordinates, or frequencies ect.

1. Waterproof note pad such as “rite n rain” pads. (because it might be raining when you have to write something down)
2. Two or more mechanical pencils. Pens and markers smear, and can run when wet. Mechanical pencils are easier to use, and don't require tools to sharpen. Two, incase one breaks.
3. Replacement leds for the mechanical pencils.
4. A watch, or other timepiece. Many people these days use cellphones as their personal time piece, but phones may compromise security in many ways, don't have long battery life, and their use may compromise light discipline. (Smartphone screens can stand out in an otherwise dark night.)
5. A small compass. Even a button compass will work. Many notes and observations may reference “North of our position”, or “east, south-east of the large boulder”, or “we are entering the west side entrance” Those messages are not as effective if a user doesn't know which way “north” is.
6. A small LED flashlight in red or blue. Sometimes it is so dark, you need a light with which to write with. Red and blue preserve night vision better than white. Just be aware of light discipline. A user may need to write under the cover of a tarp, poncho or other device so as not to have their reading light give their position away.
7. A pouch to keep all of the note taking equipment in one easy to access place. Having to take off a backpack and dig for pencils and notepads is not conducive to efficient operations. Keeping everything together, and within easy reach makes operations more efficient.

Contents of note taking kit

III. Small Team Radio and Signal Operations.
Standard Radio Operating Procedures.

A) Pre-Deployment.

Having a box of radio “stuff” does not mean it is ready for field use. Here are some guidelines for a pre-deployment radio check. If your group operates as buddy pairs, each member should check the other out to insure everything is good to go.

1. Make sure you are familiar with the radio and all of its functions. If you need, carry the manual, or a manual "cheat sheet" in a waterproof container.

2. Make sure the radio is in good working order. Check antennas, displays, seals, controls, ect.

3. Insure that any accessories are intact, and good working order.

4. Insure you have fully charged batteries, and have extra batteries available. For a mission or FTX, plan on two sets of batteries per day, for normal use. You will need more batteries for cold weather, and more as a contingency. (regular use of radios for FTX's will give you realistic expectations of battery life.)

5. Make sure your radio is mounted to your gear in a way that it will not be pulled loose while moving, especially movements such as going prone, running/crawling through brush ect. Also make sure the radio controls you need are accessible, but can't accidently be changed. Make sure your radio doesn't interfere with the operation of other equipment, such as shouldering your rifle, or accessing you trauma kit. Make sure all cables are secure, and will not get snagged on the environment. Make sure cables have enough length to allow full freedom of movement.

6. Insure you have relevant SOI information such as call signs, frequencies, codewords, authenticators, ect. This will be covered in Chapter: V. Signal Operating Instructions, pp 35.

7. Preform a commo check before departing on a mission/excercise. Insure your radio can hear and be heard properly. Some precautions may be necessary when performing commo checks. If you are in an area where unnecessary transmissions may compromise your group, you may have to forgo or modify your radio checks.

8. Insure you can do the following on your radios:
   a) lock the radio's controls. Most radios have a "lock" function so you don't accidentally change the channel or turn some other function on or off.
   b) Disable lights. Many radios will light up either display back lights or indicator LED’s when transmitting or receiving. These should be disabled for tactical operations so as to maintain light discipline.

c) Restore factory defaults. Many radios have a function that resets all of their memory and settings to the factory default state. Just like the radio came out of the box. It is usually accomplished by holding one or several buttons when powering up the radio. If a position is about to be overrun, or radios must be left behind somewhere, resetting a radio to defaults means that if the radio is captured, none of the frequencies/channels are programmed in, so it makes it more difficult for an opponent to use the radio against you.

d) Store and edit frequencies in memory, including tones, offsets, ect.

9. Have a plan (and any necessary equipment) to destroy sensitive documents and materials. If your plan to destroy your code sheet, and observation notes includes burning them, you need a lighter and some accelerant, ect... (this will be covered in more detail in the Sensitive Materials section.) Chapter XIII. Sensitive Materials, pp 73.

B) TRANSEC.

Two of the key principles in military radio work are the concepts of COMSEC, or Communications Security, and TRANSEC or Transmission Security. TRANSEC procedures attempt to reduce the probability of transmissions being detected, radio located, or jammed. COMSEC procedures attempt to reduce the ability of the opponent from understanding the contents of the transmission. COMSEC will be discussed in depth in Chapter VIII. Comsec, pp 50.

The opponent may attempt to listen in on our transmissions. Even if the transmissions are encrypted, they can gain insight to our operations just by receiving the signal. They may attempt radio direction finding (RDF), or radiolocation. Radio Direction Finding is determining the direction, relative to the detector, that a transmitter is operating. Radiolocation is the process of determining the physical location of a transmitter. Radiolocation may use RDF, or other methods to determine a transmitters location.

In order to for an opponent to successfully intercept, RDF or radiolocate a transmitter, a number of conditions must be met:
1. The opponents receivers must be with in range of the transmitters.
2. The opponents receivers must be listening on the frequencies that the transmitters are using.
3. The opponents receivers must have enough time to get a bearing.

Knowing this we can employ a number of means to improve TRANSEC.

1. Keep transmissions as short as possible. Only transmit when essential, and keep the message as short as necessary.

2. Transmit using as little power as necessary. By using less power, you reduce the area that the opponents receivers must be in. If they can't hear you, they can't intercept, RDF, or radiolocate you.

3. Change frequencies and bands often. How often depends on a lot of factors... amount of traffic you pass, how much attention you have drawn to your group, what equipment you have available, ect... Often could be once a month, once a week, once a day, once an hour, or after every transmission. The

U.S. military has been using frequency hopping radios for decades that change frequencies over 100 times per second.... it is excellent TRANSEC. Your frequency changes should be planned as part of your Signals Operating Instructions (discussed in depth in Chapter V. Signals Operating Instructions, pp 35.)

4. Deceit and deception: Use one or more decoy transmitters. Having a radio set to VOX, with a pre-recorded loop, (and long pauses) or a radio set up as a repeater, fed by a radio they are less likely to monitor.

5. Disable the intercept equipment and/or operator. Rules of engagement define what is acceptable, and what isn't. It gets easier by using a decoy, as mentioned above.

6. Interference: If you know how multiple DF units are linked to triangulate, interfere or jam the link... If they can't share bearings they can't get a fix.

7. Don't use radios. While it seems like a no brainer, just because you have a radio, doesn't mean you MUST use it. Sometimes alternatives are the better choice: hard wires, runners, semaphores, signal mirrors, flashlights, whistles, ect.

C) On Deployment Radio procedures:

1. All exchanges on air follow a set format, with a beginning, middle and an end, and use a range of "set" words and phrases, used to achieve speed and clarity of meaning when using voice radio communications systems in the battlefield. These are known as "Pro words" which is the abbreviation of the phrase "Procedural Words"

2. C.R.A.P.S.H.O.O.T.
To send a message use the following routine:

•COMPOSE your message in your head or if necessary write it down, and if time permits, rehearse it.

•RELAX, take a deep breath, listen to the channel, so you're not in a panic, nor are you trying to talk over someone else who is already on air; especially necessary when you, or they, are under fire.

•ACTIVATE the Push To Talk Button (PTT) on your radio, carefully and positively.

•PAUSE for one second before you talk. A common fault with excited or new operators is to talk as they begin to push the PTT button, which results in the first few words of your message being chopped off and not transmitted, requiring the other station to request that you repeat it.

•SPEAK slowly, clearly, with pauses and do not shout, so you can be easily understood. Remember NO contractions.

•"HAIL": hail the station or stations you want, by using their callsign twice. Then identify yourself with the prowords "THIS IS" and your callsign. The double callsign functions as a sort of "bing-bong" pay attention people signal. This is an essential tool in the battlefield. Sometimes people get confused and start with their own callsign first. It is not the end of the world if this happens. If there is no reply, just try again. "You Are, I Am" is a way to remember the order.

•OVER: send the content of your message, using the proword "OVER" at the end of each transmission. OVER means that you expect or need a reply, it is sometimes defined as a "receipt" or as an "invitation" to transmit.

•OUT: use "OUT" to formally end the communications session. OUT means "I have finished talking to you, no response is required, expected or desired". Therefore never use the classic error "over and out" as a combined Proword, its a contradiction in terms, meaning "I want you to talk to me and shut up!"

•TRAFFIC: having finished, keep listening for more incoming traffic, or move on to your next batch of traffic.

3. Use the NATO Phonetic alphabet as appropriate:

Letter	Word	Spoken as		Letter	Word	Spoken as
A	ALPHA	AL FAH		N	NOVEMBER	NO VEM BER
B	BRAVO	BRAH VOH		O	OSCAR	OSS CAH
C	CHARLIE	CHAR LEE		P	PAPA	PAH PAH
D	DELTA	DELL TAH		Q	QUBEC	KEH BECK
E	ECHO	ECK OH		R	ROMEO	ROW ME OH
F	FOXTROT	FOKS TROT		S	SIERRA	SEE AIR RAH
G	GOLF	GOLF		T	TANGO	TANG GO
H	HOTEL	HOH TELL		U	UNIFORM	YOU NEE FORM
I	INDIA	IN DEE AH		V	VICTOR	VIK TAH
J	JULIETT	JEW LEE ETT		W	WHISKEY	WISS KEY
K	KILO	KEY LOH		X	X-RAY	ECKS RAY
L	LIMA	LEE MAH		Y	YANKEE	YANG KEY
M	MIKE	MIKE		Z	ZULU	ZOO LOO

4. When giving numbers over the radio, spell them out.
"100" is "one zero zero" not "one hundred"

Be aware that the numbers 3, 4, 5 and 9 are especially susceptible to readability issues. For example "five" can be confused for the word "fire". Therefore each is provided with an alternate expression for when reception is poor. Thus you also get "TREE", "FOWER" and "FIFE" and "NINER". Finally, never use "Oh" for the number 0, always use "ZERO

When writing numbers and letters, do the following to reduce ambiguity for handwritten text:
a) The number “zero” should have a diagonal slash through it to distinguish it from the letter “O” (as in Oscar)
b) The number “seven”, and letter “Z” (as in Zulu) should have a horizontal line through them to distinguish them from “1” and “2” respectively.

The below chart lists the military prefered pronunciation for numbers. They are more understandable when spoken as listed below:

0	ZE RO
1	WUN
2	TOO
3	TREE
4	FOW ER
5	FIFE
6	SIX
7	SEV EN
8	AIT
9	NIN ER

5. When speaking on the radio, especially in combat, it is very easy to shout, and for the pitch of your voice to rise. All of these things will mean that your messages will not be understood. It is vital that you speak slowly, clearly, and never use contractions like "isn't", "I'll" or "they're". Contractions can be very easily lost or misunderstood. "Can't" may sound like "can" ect.... which can have dire consequences.

6. Unkey every 5 to 10 seconds to allow for emergency traffic to break in. Do not use “BREAK” as described below when doing this.

7. Unless there is a busy net, do not use call signs after the initial hail and response.

8. Prowords: In order to reduce ambiguity, a number of procedure words (prowords) have been defined. These should be be used whenever possible. This reduces confusion, and thus reduces the number of unnecessary transmissions needed to accurately get a message across.

As mentioned above, OVER and OUT are two prowords with specific meanings. Typically OUT would be the equivaliant of saying “goodbye” on a telephone, and then hanging up. It means no reply is expected. OUT should only be given by the station that initiated the conversation. (an exception is when used in conjunction with prowords that specify OUT... i.e. WAIT OUT.) When a station declares OUT, they should still stay on frequency and listen for a few moments in case their last transmission was unreadable, or the receiving party needs clarification. OVER should be used at the end of all other transmissions, so as to remove any doubt that the sending station is finished for the moment, and expecting a reply.

The prowords: COPY, ROGER, and WILCO, also have similar, but distinctly different meanings.

ROGER essentially means “I understand”. COPY means “I understand, and have written it down”.

WILCO is short for “Will Comply” which means “I understand, and will carry out the instructions”

A list of most common prowords follows:

AFFIRMATIVE	Used in place of the word “*yes”*, as it can be lost in transmission.
ALL STATIONS	Used in place of an individual callsign when the signal is intended for every station on the network. For example: "ALL STATIONS, ALL STATIONS, THIS IS FOXTROT ONE, I HAVE CONTROL, I SAY AGAIN, I HAVE CONTROL, STAND BY, OUT"
ANY STATION	Used in place of an individual callsign when the signal is intended to gain a response from any other random station on the network. For example when requesting a RADIO CHECK, as in: **"**HELLO, ANY STATION, THIS IS GOLF ONE, RADIO CHECK, OVER**".**

BREAK	Used to indicate the separation of different parts of the message. May also be used to indicate you are going to temporarily stop transmitting to allow stations with higher priority traffic to get through.
CALL SIGN	This Proword indicates that the following text is a CALL SIGN, that is the subject of the message, and that the station itself is not actually being called. For example: "KILO THREE, KILO THREE, THIS IS KILO SIX, ADVISE CALL SIGN KILO TWO, THAT THEIR RADIO IS JAMMING CHANNEL EIGHT THREE SIX, OVER"
CONTACT	Used to declare "contact" with an enemy. At this point all non-related traffic MUST stop to give priority to messages related to this engagement. Often repeated two or three times, replacing the more normal "HELLO", "ALL STATIONS" Pro words. If able you must provide useful intelligence, otherwise your message simply acts as a warning to other stations. Once the initial warning has been issued, either a *CONTACT REPORT* or a *SITREP* should be given, "CONTACT, CONTACT, CONTACT, (THIS IS HOTEL TWO ONE), SIX O'CLOCK, TWO FIVE METERS, RIGHT SIDE OF BUILDING, SEVEN TANGOS APPROACHING FAST, ALL WEAPONS, OPEN FIRE, OUT". Note the order in which the information is sent. It is done like this just in case the communications are cut off, giving the receiving stations their best chance of responding effectively. • First the network gets a warning of the presence of the enemy. • If time permits, next should come the stations callsign, so the unit knows who sent the message. Remember the enemy may try to deceive you. • Then a direction in relation to the axis of march or observation, which is always 12 o'clock. Now the unit knows which way to look, in this case, behind them! This is always done first, as it significantly reduces the possible locations for the enemy, especially at short range, where time is critical. • This is followed by a range estimation in meters, so the unit knows how far out the enemy is, here its twenty five meters. • Then a brief description of where, what, how many, and their activity, so now the unit knows what to look for. • Next is the order identifying which unit or units should shoot, in this case all of them. • Then we have the actual order to shoot. This can be delayed with EXECUTE TO FOLLOW, STAND BY or WAIT ONE. • And finally we have OUT, meaning I have finished, no need to respond, I'm busy. Again if time permits, a commander may ask "....ENEMY SEEN, NOT SEEN?..." Meaning has everybody in the unit spotted the enemy, to which other stations, will

	respond with either "AFFIRMATIVE, ENEMY SEEN, CALL SIGN OUT" or "NEGATIVE, ENEMY NOT SEEN, CALL SIGN OVER". You should then provide further information to help the others find the enemy. Wherever possible, you should give as much detail as you can, including, TANGO Type#, weapons, antennas, uniforms and insignia, and attitude: relaxed, cautious, performing a particular tactical manoeuver, like flanking right – it all helps prioritize the targets.
CORRECTION	an error has been made in this transmission. Transmission will continue with the last word or specified portion correctly transmitted, for example: "ALPHA FOUR ONE, THIS IS UNIFORM THREE TWO, MY CORRECTION IS...."
DECIMAL	Used to verbally marked the decimal point in a number to prevent confusion, for example: ""...SEVEN, SIX, DECIMAL, TWO, ONE..."
DISREGARD	"DISREGARD (THIS) (TRANSMISSION), OUT" This transmission is in error. Disregard it. This proword shall not be used to cancel any message that has been completely transmitted and for which an acknowledgement has been received. It is always ended with the "OUT" pro word to close the message. For example: "...BELIEVE ENEMY IS NEAR YOUR POSITION, DISREGARD, OUT"
DO NOT ANSWER	An instruction to one or more stations NOT to transmit or respond to a message for their own safety. "WARLOCK FIVE, WARLOCK FIVE, THIS IS WARLOCK SIX, DO NOT ANSWER, EIGHT TANGOS AT POSITION SIERRA, OUT" Often used by a Commander sending orders "in the blind",(without a response) which is usually supported by a prearranged Authentication code.
ENDEX	"End Exercise" - The signal that is sent to end a military exercise. All units should acknowledge this message. The word "ENDEX" is often repeated two or three times before saying "OVER", for example: "ENDEX, ENDEX, ENDEX, ALL STATIONS ACKNOWLEDGE, OVER"
I SAY AGAIN	I am saying my entire transmission again, or the portion indicated. "ALL STATIONS, ALL STATIONS, THIS IS NETWORK CONTROL, I SAY AGAIN..." Do NOT> use the word "repeat"See also "ALL AFTER X", "ALL BEFORE X", "WORD AFTER X", "WORD BEFORE X", and "SAY AGAIN".
I SPELL	I shall spell the next word phonetically using the standard NATO Phonetic Code for extra clarity, for example: "...THIS IS WARLOCK ONE, I SPELL "WITCH", WHISKY INDIA TANGO CHARLIE HOTEL, OVER"
NEGATIVE	Used instead of the word *“no”,* as this can be lost in transmission. See also "AFFIRMATIVE", "CORRECT", "ROGER" and "WRONG".
OUT	This is the end of my transmission to you and no answer is required or expected. Never used with "OVER" as in the incorrect signal "over and out" which is a

	contradiction in terms, essentially "talk to me and shut up".
OVER	This is the end of my transmission to you and a response is necessary. Go ahead and transmit. Never used with "OUT" as in the incorrect signal "over and out", which is a contradiction in terms, essentially "talk to me and shut up".
RADIO CHECK	"Can anyone hear me?" "How loud/clear is my transmission?"
ROGER (THAT)	1. I have received and understood your last transmission satisfactorily. 2. Used in place of the words "that is right", to mean "yes" or "correct". The word "right" is exclusively used for giving some kind of spacial directions. For example: "ROMEO ONE, THIS IS JULIET TWO, ROGER THAT, OUT" ROGER is never used with "WILCO", as in "roger, wilco", as the function of "ROGER" is implicit in the "WILCO" proword. NB: The addition of "THAT" is common practice, often being used in non-radio speech as an acknowledgement or agreement.
SAY AGAIN	A request to another station to send either all of their last transmission, or that portion indicated by the "ALL AFTER X" "ALL BEFORE X", "WORD AFTER X" or "WORD BEFORE X" prowords. "OSCAR TWO FIVE, THIS IS OSCAR ACTUAL, SAY AGAIN, OVER" Do NOT say "repeat".
I SET (SET)	Indicates that whatever follows is encrypted. If there are multiple methods of encryption, then the sending station should also indicate what encryption is being used. For example: “BRAVO SIX, THIS IS BRAVO ONE, WE ARE AT LOCATION, I SET, APPLE, CHARLIE, FOXTROT, NOVEMBER, BRAVO, TANGO, INDIA, MIKE. OVER” This means use encryption sheet “APPLE” to decode “CFNBTDIM.”
SIGNING OFF	Sent when the station is shutting down and ceasing radio operations altogether. Used as an acknowledgement to the instruction to "CLOSE DOWN". If there is a Network Control Station, or the station is part of an operational formation in the field, it is normal to seek permission to close down from the authorized station or commander. For example: "HELLO NOVEMBER ACTUAL, THIS IS NOVEMBER EIGHT, REQUEST PERMISSION TO CLOSE DOWN, OVER" "NOVEMBER EIGHT, THIS IS NOVEMBER ACTUAL, CLOSE DOWN IN FIVE MIKES, OVER" "NOVEMBER ACTUAL, THIS IS NOVEMBER EIGHT, WILCO, OUT". And five minutes later: "THIS IS NOVEMBER EIGHT, SIGNING OFF, OUT" It is recommended to wait an additional minute or two just in case there is any last moment traffic that needs to be passed to the station signing off.
SILENCE	This proword is repeated three or more times, and used to order the cessation of transmission on this channel/frequency immediately. Radio silence will be maintained until lifted. Used when absolute stealth is required for that network.

	When an authentication system is in force, the message imposing silence is to be provided with an Authentication Code. For example: "ALL STATIONS, ALL STATIONS, THIS IS NETWORK CONTROL, SILENCE, SILENCE, SILENCE, AUTHENTICATION NOVEMBER ECHO, OUT"
SILENCE LIFTED	Radio silence is lifted, proceed with normal operations. When an authentication system is in force, the transmission lifting silence is to be provided with an Authentication Code.
SIT REP	A reference to, or a request for a "Situation Report", for example: "ZULU ONE ONE, ZULU ONE ONE, SIT REP, OVER"
SPEAK SLOWER	Your transmission is at too fast a speed. Reduce speed of transmission.
SPELL X	Please spell the X word phonetically using the standard NATO Phonetic Code for extra clarity. If the word requiring spelling was unheard or unclear, use the Pro words "WORD BEFORE X" or "WORD AFTER X" to guide the operator to the required target word. For example: "VICTOR THREE, THIS IS VICTOR ACTUAL, SPELL WORD AFTER INSIDE, OVER"
STAND BY	A request for a pause in the exchange. If followed by "OVER" the other station must acknowledge the request with "STANDING BY", and usually "OUT". If the message is "STAND BY, OUT", no acknowledgement is required, but it does require the other station to remain alert for the follow up transmission. This latter is used when an incoming signal could compromise the station's security, or the operator is too busy. For example "ALPHA TWO SIX, THIS IS SIERRA THREE TWO, STAND BY, OVER" See also "WAIT" and "WAIT ONE".
STANDING BY	The acknowledgement to the request "STAND BY, OVER", always finished with "OUT", as in: "ALPHA TWO SIX, STANDING BY, OUT"
THIS IS X	This transmission is from the station whose CALL SIGN immediately follows. See also "FROM X" and "TO X".
UNKNOWN STATION	The identity of the station with whom I am attempting to establish communication is unknown. Used at the start of a transmission in place of the CALL SIGN of a known station.
WAIT	A request to suspend the conversation for a few seconds. Used as an alternative to "STAND-BY", but more urgent. The other station must NOT attempt to recontact the original signaler, and MUST wait on standby until they return, or until concern for the unit's situation becomes critical, warranting the risk of breaking the implied radio silence. It can also be used at less critical moments when the operator needs literally just a few seconds to sort something out. They will begin transmitting again almost immediately. For example: "CONTACT, WAIT, OUT"

WAIT ONE	As per "WAIT", but a request to suspend the conversation for one minute rather than a few seconds. The other station may attempt to recontact the original signaler after one minute has passed. Alternative numbers can also be used, as in "WAIT FIVE".
WILCO	I have received your signal, understand it, and will comply. To be used only by the station addressed. For example: "ECHO TWO, THIS IS HOTEL SIX, WILCO, OUT" Since the meaning of "ROGER" is included in that of WILCO, the two Pro words are never used together, as in "roger, wilco". See ROGER.

More general prowords:

ACKNOWLEDGE	Used to demand and provide a response from one station to another when their operational status is in doubt. For example: "ALPHA TWO ZERO, ALPHA TWO ZERO, THIS IS BRAVO ONE ZERO, ACKNOWLEDGE, OVER." "BRAVO ONE ZERO, THIS IS ALPHA TWO ZERO, ACKNOWLEDGE, STAND BY, OUT."
ALL AFTER X	This is used to refer to a latter portion of a message. For example to request it's repetition. See also "SAY AGAIN".
ALL BEFORE X	This is used to refer to a previous portion of a message. For example to request it's repetition. See also "SAY AGAIN".
AUTHENTICATE X	A challenge to provide proof of authority to issue orders. Where "X" is the challenge. This procedure is used when the identity of the station is uncertain or suspect, and the orders or request's validity needs to be confirmed. For example: "OSCAR TWO ONE, OSCAR TWO ONE", THIS IS OSCAR TWO TWO, AUTHENTICATE X-RAY YANKEE, OVER"
AUTHENTICATION	The reply to the challenge "AUTHENTICATE", giving the correct authentication code. This procedure is used when the identity of the station is uncertain or suspect, and the orders or request's validity needs to be confirmed. For example: "...(MY) AUTHENTICATION (IS) VICTOR OVER" "...(I) AUTHENTICATE VICTOR, OVER"
CASEVAC	A request for casualty evacuation by any means. See also MEDEVAC.
CLOSE DOWN	An order to shut down and turn off your radio, immediately or at the time specified. An acknowledgement is required.
EXECUTE	Carry out the purpose of the message or signal to which this applies. For example:

	"....EXECUTE PLAN BRAVO IN TEN MIKES, OUT"
EXECUTE TO FOLLOW	Action on the message which proceeds or follows is to be carried out upon receipt of the Proword "EXECUTE". For Example: ...PREPARE TO SWITCH TO PLAN BRAVO, EXECUTE TO FOLLOW, OUT"
EXEMPT/EXCEPT	The CALL SIGNS immediately following are exempted from the collective call, as follows: "ALL STATIONS, THIS IS OVERLORD, EXEMPT, YANKEE FOUR ONE, ZULU FOUR FIVE, IMMEDIATELY EXECUTE WINCHESTER, OUT.
GRID X	Used as a prefix to an alpha/numeric or simply a numeric string giving a map coordinate, where "X" is the coordinate. Used rather than FIGURES, so it is clear that the numbers being sent are positional data.
IMMEDIATELY EXECUTE	The action on the message or signal following is to be carried out immediately on completion of this transmission, without delay!
I VERIFY	That which follows has been verified at your request and is repeated. To be used only as a reply to "VERIFY". This is used to confirm the truth of a statement or a piece of intelligence.
MARK	Used to "mark" a precise moment in time, to ensure accuracy. Preceded by either "AT MY MARK" or "ON MY MARK", then "MARK". Used for example for synchronizing watches or actions such as an attack.
MEDIVAC	A more specialized request for casualty evacuation, requiring a purpose built ambulance and medical crew. see also CASEVAC.
MINIMIZE	Please limit your transmissions to essential traffic. Emergency operational traffic is in progress. MINIMIZE is imposed by the Net Controller or by the Incident Commander.
MINIMIZE LIFTED	The "MINIMIZE" order is lifted by either the Net Controller or by the Incident Commander.
MORE TO FOLLOW/	Transmitting station has additional traffic for the receiving station, please wait.
NOTHING HEARD (OVER)	Used when no reply is received from a called station, thus alerting others to the fact that you have not heard a return signal. This is important, as another station may be in range and able to hear the called station, and relay the messages, while others may simply presume that they heard nothing because they are out of range of the station being hailed.
RELAY (TO) X	Transmit this message to all "CALL SIGNS", or to the "CALL SIGN" immediately following this Proword. When the coverage of a set of stations overlap, messages can be passed along the line, far further than one radio can do by itself.
TIME CHECK	A request for the current correct time, given in 24 hour format for the time

	zone of the theatre of operations. "ZULU" equals GMT, and is the default time zone. The time giver uses the "MARK" Proword to ensure accuracy, as follows: "...THE TIME AT MY MARK, WILL BE FOURTEEN THIRTY SIX ZULU PRECISELY....MARK, OVER"
VERIFY	Verify entire message (or portion indicated) with the originator and send the correct version. Used when the receiving station has a doubt about the content of the original message.
WORD AFTER X	Used to refer to a word that follows the stated word in a message. See "ALL AFTER X", "ALL BEFORE X", "SAY AGAIN" and "WORD BEFORE X"
WORD BEFORE	Used to refer to a word that proceeds the stated word in a message. See "ALL AFTER X", "ALL BEFORE X", "SAY AGAIN" and "WORD AFTER X"

9. When the identity of a transmitting station is uncertain or suspect, and the orders, request's or information's validity needs to be confirmed, the receiving station can issue a challenge in the form of a demand that the sender AUTHENTICATE their message. Units meeting in the field, not using the same password and challenge, can also use this Authentication Code to aide in confirming friendly status. There may be a single authenticator word, 2 authenticator words or an authenticator sheet.

If the receiving stations need to maintain radio silence, or if command believes that receiving stations might not trust an urgent or unusual order, the transmitting station can "blind" authenticate a message, by sending the full authenticator, and not wait for a challenge and reply. In this instance, "blind" refers to transmitting without receiving or expecting a response. Often used when a response would risk compromise to the answering station.

More information on authentication can be found in Chapter V. Signals Operating Instructions, pp 35.

10. Only use words that are expected by the receiver. Including prowords, planned words, or common mission words. If you are using an unusual word, do not leave doubt. Spell it out.

11. Examples:

Overlong Transmissions:

B1: "Charlie 3, Charlie 3, this is Bravo 1, over"
C3: "Bravo 1, this is Charlie 3, I have good copy, over"
B1: "Charlie 3, this is Bravo 1, Move to location .. ah... wait one" -pause- "uh, move to location Titan, over"
C3: "Bravo 1, This is Charlie 3, good copy. We will move to location Titan, over"
B1: "Charlie 3, this is Bravo 1, Roger, out"
C3: " Bravo 1, this is Charlie 3, out"

compare that to this exchange, that passes the same information:

B1: "Charlie 3, Charlie 3, this is Bravo 1, over"
C1: "This is Charlie 3, over"

B1: “Move to location Titan, Over”
C1: “Wilco, Over”
B1: “Roger, Out”

Both exchanges convey the same information, but the second is much more concise.

11. Demobilization (de-mob)

a)At the conclusion of an operation/mission/excercise, inspect the radio and related equipment and make sure it is still in good working order, clean, and dry and that it does not require any service before the next deployment.

b)Clear any memory, or encryption that may compromise COMSEC.

c) Remove batteries so they do not leak and damage the radio.

d) Secure or destroy any COMSEC material as necessary. Document as necessary.

e) Recharge any batteries or other devices that use rechargeable batteries.

f) Evaluate radio performance, note anything that needs to change for the next deployment, and pass on any comments, complaints, and suggestions to higher authorities.

IV. Standard Messages:

When should you communicate, and when shouldn't you?

Generally, to help preserve transmission security, you should only transmit when it is relevant to the mission, or the security of operations. Football scores are usually not relevant. Enemy seen, usually is.

When sending reports, report accurate information. "Heavy shelling" or "strong resistance" is not nearly as informative as "approximately 24 mortar shells" or "two heavy machine guns"

Report specific numbers. "nine men" is more accurate than "a squad"

Do not use relative times such as "We move in 30 minutes", instead use absolute times such as "We move at 1530" because it is less likely to be misunderstood.

A) Date Time Groups:

Date Time Group (DTG) is the U.S. militaries format for showing the date and time.
It uses the Day, Hour, Minute, Timezone, Month, Year format: DDHHMM (Z) MON YY

Because U.S. Allies have several different date formats (England, for instance, uses DDMMYY, whereas many people in the U.S. use MMDDYY... so 04/05/15 would mean April 5th, 2015 to an American, and it would mean 4th of May, 2015 to an Englishman. Because of this the DTG uses a three letter abbreviation for the month to remove any ambiguity.

The time zone designator is crucial for military operations because they have operations going on around the world. Most time zones are referenced based on how many hours different they are from Greenwich Mean Time:

Time zone name	Letter	UTC offset
Alpha Time Zone	A	+1:00
Bravo Time Zone	B	+2:00
Charlie Time Zone	C	+3:00
Delta Time Zone	D	+4:00
Echo Time Zone	E	+5:00
Foxtrot Time Zone	F	+6:00
Golf Time Zone	G	+7:00
Hotel Time Zone	H	+8:00
India Time Zone	I	+9:00
Kilo Time Zone	K	+10:00
Lima Time Zone	L	+11:00
Mike Time Zone	M	+12:00
November Time Zone	N	-1:00
Oscar Time Zone	O	-2:00
Papa Time Zone	P	-3:00
Quebec Time Zone	Q	-4:00
Romeo Time Zone	R	-5:00
Sierra Time Zone	S	-6:00
Tango Time Zone	T	-7:00
Uniform Time Zone	U	-8:00
Victor Time Zone	V	-9:00
Whiskey Time Zone	W	-10:00
X-ray Time Zone	X	-11:00
Yankee Time Zone	Y	-12:00
Zulu Time Zone	Z	0:00

The letter “J” is used to indicate the observers local time.

141800JFeb15 is February 14, 2015 at 6:00pm local time.
21030530ZJan14 is January 21, 2014 at 3:05 and 30 seconds AM, Greenwich Mean Time

Small groups do not have to use the military DTG format, but should decide on a standard they everyone will use. If a group is near another timezone, or works with groups in other timezones, then there should be some standard to indicate the time zone referenced, so as to reduce any confusion.

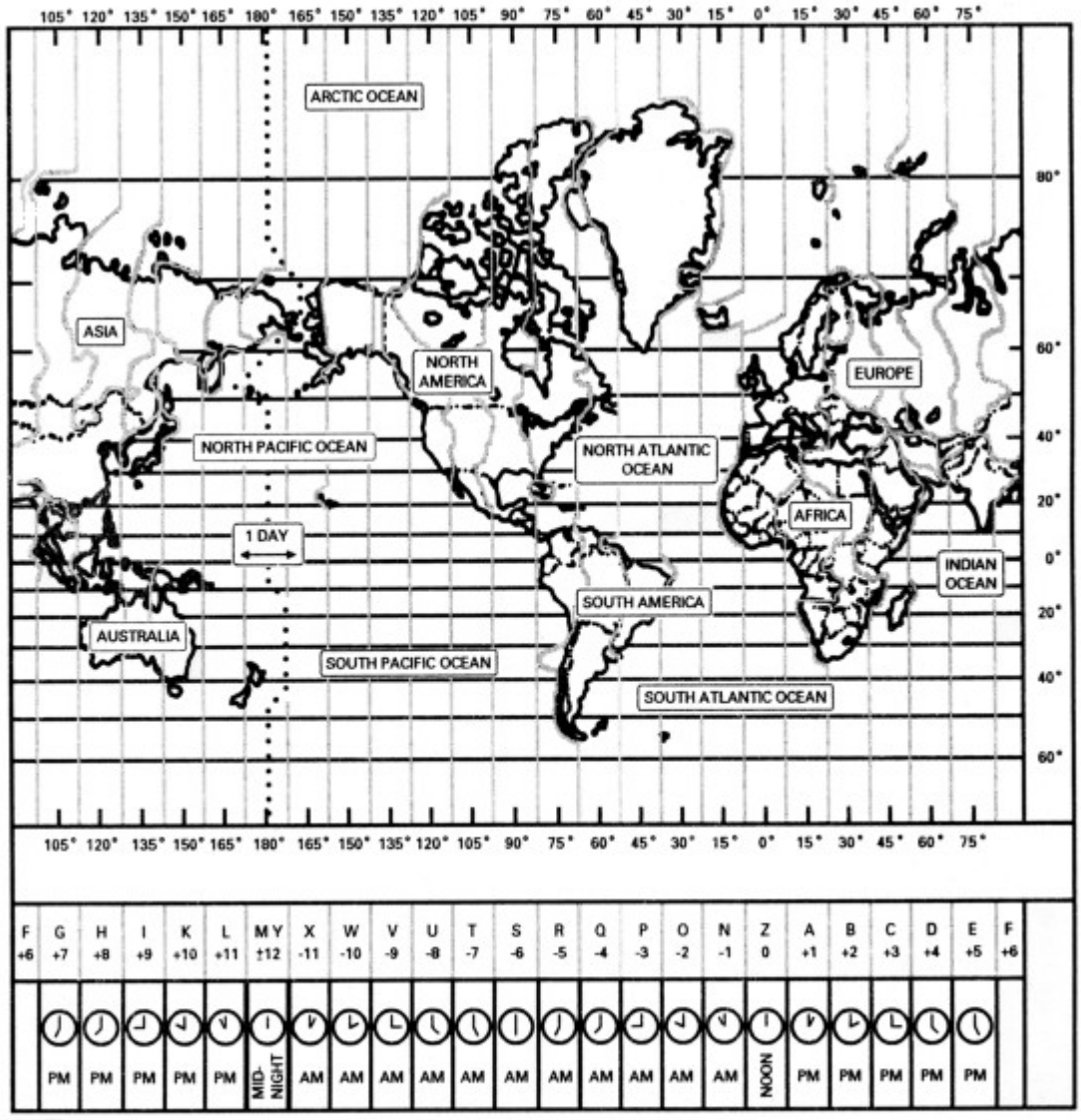


Figure 2-2. Time zone chart.

Illustration Courtesy U.S. Department of Defense

The following are messages commonly sent during tactical operations by armed forces. They should be adapted to your specific situations for best effect.

B) Spot reports:

Generally, a spot report means the reporting unit has detected enemy, or unknown unit activity (and hopefully is unobserved.)

The mnemonic: SALUTE helps with remembering what should go in a spot report.

Size: How big is the unit observed?

Activity: What are they doing? How are they carrying themselves?

Location: Where are they?

Uniform: What are they wearing?

Time: When were they observed? (or what range of time)

Equipment: What equipment/weapons/packs/radios/vehicles, ect. did they have with them?

Accuracy is extremely important. DO NOT GUESS OR MAKE ASSUMPTIONS! If you see 4 people and hear a few more do not report "about seven people" report "four people seen, plus others heard".

Sending and receiving stations should write all spot reports down immediately.

Not every spot report needs to be transmitted immediatly. Mission parameters should dictate when reports are sent. If an enemy unit is headed out of your area, and listening for radio transmissions, your spot report may tip them off that you are nearby. That could have them change their plans, and become a bigger threat. If, however, they are headed towards other teams on your side, the report may alert your teams of the impending approach, and allow them to be ready, or react appropriately.

C) Contact reports:

Similar to spot reports, but geared for other units travelling with the team. See the description for the proword CONTACT in the chart above.

D) SITREP:

A situation report is a concise statement indicating a units activities and readiness to higher commands. Before deployment, there should be a clear expectations of what should be in a SITREP, and how often they should be sent, (Daily, twice daily, at specific times, ect...)

A SITREP may include: Unit, Time covered, General situation, including activities of the previous 24 hours, planned activities for the next 24 hours, Intelligence collection or analysis that may be relevant, Operational issues that may affect a units ability to respond, personnel and logistics issues and concerns, readiness to move assessments (i.e. BRAVO 2 can be ready to move in 12 hours), any change in status of sensitive items/COMSEC/OPSEC, ect... There are many different formats.

The "8-Line" includes:
Unit call Sign, Current position, Recent activity, Casualties, Ammo & equipment status, Enemy KIA,

Intel, your intention.

The UK Land Forces SITREP is smaller with: Time of report, Own Forces, Enemy Forces, and Intentions.

E) Mission progress reports, and unit movement reports:

So that leadership can track friendly forces, units should report changes in movement, such as arriving at a rally point, changing general direction of travel, stopping for a long duration, and similar. Additionally, reports of mission progress should be made as necessary. All of these reports should be pre-planned before the mission starts, so there is no ambiguity. Sometimes there is a tendency to over report your own movement. Don't give a play by play, only report as the mission plan dictates.

F) Medevac requests:

The Army's medivac request is based on the premise of a helicopter pickup. Small units without air evac capabilities need to adapt the Army's 9-line format to one that is appropriate to their circumstance.

The Army 9-line request includes:

Line 1: Location of pickup site- this is given in an MGRS 6-8 digit grid.

Line 2: Frequency and call-sign at pickup site- this is the frequency and call-sign that you will be talking to the incoming MEDEVAC aircraft on. In most cases this is a predetermined, non-encrypted channel that is set-aside for MEDEVAC. If possible write this on all 9Line cards prior to mission.

Line 3: Number of patients by precedence-

A- Urgent (surgical)- i.e. requires in-flight surgeon to perform surgery while en route to hospital.

B- Urgent (non-surgical)- i.e. patient has arterial bleed that can be stabilized until arrive to hospital

C- Priority- i.e. injuries that are not immediately life threatening but could become life threatening eventually

D- Routine- i.e. patient requires regular medical care but unit cannot transport them by their own means.

E- Convenience- i.e. non life-threatening care provided to personnel in a combat zone.

Line 4: Special Equipment required-

A- None

B- Hoist

C- Extraction Equipment- i.e. jungle penetrator

D- Ventilation

Line 5: Number of Patients by type:

A- Litter- cannot walk on their own

B- Ambulatory- able to self move to MEDEVAC platform

Line 6: Security of Pickup area-

N- No enemy troops in area

P- Possible enemy troops in area (approach with caution)

E- Enemy troops in area (approach with caution)

X-Enemy troops in area (armed escort required)

Line 7: Method of Marking at pickup site (important: always ensure marking equipment is available to the marking personnel. If you are going to throw purple smoke, ensure you have purple smoke on hand)

A- Panels- i.e. VS-17 panel

B- Pyrotechnical equipment- i.e. pen flare, red star cluster

C- Smoke signal- (provide smoke color)

D- None

E- Other- i.e. IR flash or beacon

Line 8: Patient Nationality and Status

A- US Military

B- US Civilian

C- Non-US Military

D- Non-US Citizen

E- EPW (Enemy Prisoner of War)

Line 9: NBC Contamination

A- Nuclear

B- Biological

C- Chemical

Here is how an Army 9-line would be transmitted over radio with the unit Victor Two (V2) requesting the medevac from Here is an example 9-Line, and how it would be transmitted over radio with the unit Victor Two (V2) requesting the medevac from Bravo Five (B5):

	Air-Medevac 9-Line request			DTG:	Unit:
1	Location (UTM/Lat-Long)			(1) 18SWP12314517	
2	Callsign & Frequency			(2) 027.000MHz, Victor Two	
3	Number of Patients/ Precedence			(3) Alpha-1, Bravo-3	
	A- Urgent (less than 2 hours to save life)			B- Surgical Urgent	
	C- Priority	D- Routine		E-Convience	
4	Special Equipment Required			(4) Alpha	
	A- None	B- Hoist	C- Extraction	D-Ventilator	E- Jungle penetrator
5	Number of patients by Typr			(5) Alpha -4	
	L- Litter			A- Ambulatory (walking)	
6	Security at LZ			(6) Papa	
	N- No enemy			E- Enemy in area	
	P- Possible enemy			X- Armed escort required	
7	LZ Marking Method			(7) Charlie- Green	
	A-Panels	B- Pyro	C- Smoke	D- None	E- Other
8	Nationality/Status			(8) Alpha-4	
	A- Friendly Military	B- Friendly Civilian		C- Non Allied Military	
	D- Non Allied Civilian			E- Enemy POW	
9	Terrain/Obstacles			(9) None	
Notes:					

Bravo Five (B5):

V2:“Bravo five, Bravo five, this is Victor two, request 9 line medivac, over”

B5: “Victor two this is Bravo five prepared to copy, over”

V2: “Line one, one eight sierra whisky papa one two tree one four fife one seven” *(here they are giving their location as an eight digit MRGS grid: 18SWP12314517)*

V2: “Line two, two seven zero zero Victor Two” *(here V2 indicates they will be on radio frequency 27.00 Mhz, and their call-sign V2)*

V2: “Line tree, alpha one, bravo tree” *(Here, V2 indicates they have 1 surgical urgent patient, and 3 non-surgical urgent patients)*

V2: “Line four, alpha” *(no special equipment required)*

V2: “Line five, alpha four” *(This indicates none of the patients can walk on their own.)*

V2: “Line six, papa” *(This indicates there are possibly enemy troops in the area, approach with caution)*

V2: “Line seven, charlie green” *(This indicates the pick-up area is marked with green smoke.)*

V2: “Line eight, alpha four” *(This indicates all patients are U.S. military.)*

V2: “Line nine, none”

V2: “How copy over?”

At this point, B5 would read back the 9 lines to insure proper copy.

For small teams, location should be in whatever format the team is most familiar with. If it is home turf, it coud be referenced to code named locations, or street addresses, or Lat/Long, or UTM grids.

Generally patient nationality is not relevant. NBC status can probably be left off unless it is an actual issue for that report. The other lines may or may not be relevant, depending on the resources available to perform a pick-up.

This example also has everything sent in the clear, If COMSEC is a concern, locations, and frequencies should be code words, or encrypted to protect the info.

V. Signals Operating Instructions.

Standard operating procedures, by definition, stay the same. The proword: OVER will always mean "end of transmission, and awaiting your reply" Signals Operating Instructions (SOI's), on the other hand, are a set of instructions and signals that change at regular intervals, and standardize communications across a command to make communications more efficient, and facilitate identifying friends and foes.

The U.S. Army typically generates SOI's at the Theater level, and distributes them down to the Battalion level. Anything below the Battalion level is only given the parts of an SOI that are applicable to that unit and mission.

For small independent units, it makes the most sense to generate their SOI's at the highest level of common regular command. A state militia may have one SOI for company to company communications, and each company would have their own separate SOI for communications within that company. If several companies are working in the same area, then they would need to share a common SOI, typically originating from the host company, or the statewide command.

What an SOI should contain:

1. Effective timeframe. This should indicate when the SOI goes into effect, and when it expires. Many Division level SOI's include 30 days worth of information, some of which changes daily. They may only pass on 10 days worth to Companies, so as to avoid the chance of compromise. Small units, however often don't have the resources to devote to generating, maintaining and distributing lots of SOI's, so optempo, COMSEC, and common sense should define how long an SOI is good for. It may make sense to have a training SOI that changes once a year, or once a quarter ect. A civil search and rescue mission may need a SOI that lasts for the duration of the mission and doesn't change. A guerrilla group performing one operation per month could probably be fine with a new SOI per month, while an Army Ranger unit performing 3 direct action missions per night probably should get a new SOI every day.

2. Unit identifiers. You need to know who is talking. A standard of identification should be part of th SOI. Depending on the COMSEC concerns, and the mission, different approaches can be used for I.D. For instance, a civil search and rescue mission, may best be served by function I.D.'s such as "Search One", "Search Two", or "Base". In a non-tactical administrative setting, regular names or unit names or nick names can be used, as long as everyone knows them. Ron, Frank, Thomas, Skinny, Chigger, Chief, 1st team, 2nd team...ect.

If COMSEC is an issue, you would use call signs or codenames that obscure who the actual unit or person is. The U.S. Army has adopted a system of using a letter, number, letter system for Company call signs, such as Alpha Seven Charlie (A7C), or Whisky Five Delta (W5D). Depending on the SOI, these call signs change either per operation, or daily. So Bravo company might be A7C one day, and W5D the next. Much like the effective timeframe for an SOI, the duration for a callsign should be

considered based on COMSEC concerns and optempo.

Subunits within a company are typically appended numbers to the companies callsign. For example: If Bravo companies callsign for the day is Charlie Seven Delta, 1st platoon of Bravo company would Charlie Seven Delta One. 2Nd platoon would be Charlie Seven Delta Two. Generally ***6 is the company commander, ***5 is the XO, so Charlie Seven Delta Six would be Bravo Companies commander in the above example. Additional subunits become additional numbers appended to the call sign, so second squad, of first platoon would be "Charlie Seven Delta One Two"

Within a company, using full callsigns can be a mouthful. Imagine: "Charlie Seven Delta Three One, Charlie Seven Delta Three One, this is Charlie Seven Delta Two, Over." … that can get confusing, so when appropriate, a unit can go to abbreviated call signs. If the radio net only has Bravo company on it, then "Charlie Seven Delta Three One" becomes "Three One" So the above transmission becomes "Three One, Three One, this is Two, Over." If there are other companies on the radio net, using the last letter of the company callsign, with the subunit numbers is appropriate. "Delta Three One, Delta Three One, This is Delta Two, Over."

A unit should always use their full callsign when joining a net, after a SOI dictated callsign change, when radio reception is poor, when on a net one is not normally on, or when requested by command or net control. Once a radio net is underway, command or net control will indicate "Use abbreviated callsigns" or "Use full callsigns."

While the Army's callsign system offers good COMSEC, it may be overkill for small units. Since most units will be smaller than company strength, their subunit call sign would never change. That doesn't help operational security much. Small unit leadership needs to determine what is the smallest unit that will get a unique identifier, and what units will be identified as subunits. It may make sense to scale the Army's system down to make it fit.

Code names are an alternative to the letter, number, letter system the U.S. Army uses. When used correctly, codenames can provide decent operational security (OPSEC)

When choosing codenames, use the following guidelines:

A. Don't use single syllable words. "Hoe" and "Bow" can be too easily confused with "No" and "Go"

B. Make sure your codewords are all distinct. Having "Huey", "Dewy" and "Louie" as codenames is begging to have one confused for another. Especially, since often the very beginning of a transmission will get cut out, so if you don't hear the "L" in "Louie" it will get mistaken for "Huey"

C. Don't use codenames that relate to the content of what the name is describing. "This is Tiny calling Longshot, Tiny calling Longshot..." I will conclude that Tiny is either the largest or smallest member of your team, and Longshot is probably a precision rifleman, or indirect fire of some sort.

D. Don't make codenames that are hard to pronounce, or are too long. "antidisestablishmentarianism" is a crappy codename. (and definitely not a brevity code)

E. Change codenames regularly. If your codes are compromised, and you aren't aware of the compromise, regular changing will negate that specific compromise.

F. Everyone that needs to know a codename MUST know it

3. An SOI should also have a radio frequency assignment section.

Spectrum management and frequency allocation will be covered in depth in Volume 2.

Functions, not units should be assigned frequencies. What does this mean? Some poorly done SOI's will define the commander as channel 6, 1st team as channel 1 ect... That has people changing channels a lot, and increases the possibility of two units trying to reach each other missing because they go to the other channel. A proper frequency/channel assignment will define the purpose of the frequency, (and alternates). For example; Channel 1 is Team 1's intra team frequency, only to be used between members of the same team. Channel 6 is the command net, for use between teams, and command. In this example, team leaders and command stay on channel 6. The Team 1 leader, may have a second radio, or delegate that to another team mate (usually the second in command) who talks to the rest of the team on channel 1.

4. An SOI will also have non- radio signals. Pyro (flares), smoke, Hi Vis panels, whistles, horns, other sound signals. For small units, it is important that everyone has the equipment needed to carry out non radio signals. It isn't very effective to specify flare(pyro) signals, if no one has a flare.

Also consider the effective range of non radio signals. How far away can flares be seen? How far away can whistles be heard? That will affect use.

A) Flares may specify color and type. For example:

Green starburst flare= medevac required.

Red starburst Flare = troops in contact.

Red and Green flares together = we are being overrun.

(just make sure each unit has 2 sets of red and green flares.)

B) Whistles and horns may be useful for alerts, or movement commands. For example:

continuous blast: ALARM
3 long blasts: ASSEMBLE
1 long blast: MOVE OUT or ATTACK
2 long blasts: WITHDRAW
1 long and 1 short blast: RIGHT FLANK PULL IN
1 short and 1 long blast: LEFT FLANK PULL IN
2 short and 1 long blast: SHIFT LEFT
1 long and 2 short blasts: SHIFT RIGHT
4 short blasts: REGROUP
1 long, 1 short, 1 long blast: ASSEMBLE ON LEADER

Visual signals: Strobe, Smoke, Flare, and Hi-Viz panel

5. An SOI may have phone tagging systems, Switchboard layouts, and field phone instructions. While not as prevalent these days, If your unit is using field phones, the SOI can have instructions such as:

Creek OP phone: Wire Blue, Switchboard input 1

Gate OP phone: Wire Red, Switchboard input 2

Command Post phone: Wire White, Switchboard input 3.

These may also be issued as a separate SOI for wired coms.

Surplus Army field phones

6. An SOI should have a IFF (Identify Friend or Foe) section as well.

IFF relies on information that only your team members will know, to identify friends and enemies. It may seem a bit redundant to have IFF procedures for a small group, because everyone usually knows everyone else. The problems arise when trying to ID at distance, or when camouflage is being well used. Is the guy in a ghillie suit really the same one that left earlier, or was he captured, and an enemy is now using his suit to get closer?

A) Challenge response words: a pair of non related words that change regularly. The first word is the challenge, with the second word being the response. For example: challenge: “elephant” and reply “pizza” The reply should never be given without the challenge first, or a crafty enemy might ask for the reply, then disable you, and now use the reply you gave them to get behind your lines.

When approaching a fixed position, the challenge should always come from the fixed location, not the approaching unit.

Words chosen should be multisyllable, so as to avoid confusion. Words should be unrelated, or an enemy may guess the response word. “Marco”/”Polo” or “Babe”/”Ruth” are poor choices for challenge reply words.

Challenge /response words should never be used over radio, or they are compromised after the first time they are used. We use authenticators discussed below for radio IFF.

B) Duress words: A word to be used during Challenge/Response situations to indicate that the person is giving the response against their will. If your challenge/ response for the day is elephant/pizza, and the duress word is “continent” a challenge of “elephant” getting the reply of “continent” means that the person is being forced to reply against their will. Possibly someone else in their group is compromised, or enemy.

C) Running password: If a friendly unit is in contact, and running back towards their own lines, the running password is usually yelled out to the friendly lines as they approached before a challenge is issued.... It should be obvious to defenders on the line that the approaching troops are in contact, and once a running password has been used, it should not be used again.

D) Number combination: Usually a number and “rule.” For example: the combination number is “13” and the rule is “challenge plus response equals combination number” So if you are challenged with “6” the reply is “7” because 6+7=13. This can be used if the normal challenge/response word pair has been compromised, and new ones haven't been issued. It can also be used at longer distances, such as the number of times to flash a flashlight, or car headlights, or toots on a whistle, ect.

E) Vehicle IFF: When conducting operations where you can't allow hostile enemy close up, vehicles need a means of marking IFF. IFF signals for vehicles should only be set up only when the vehicle is in a proscribed area. For example, if you are approaching your units headquarters from home, don't put up your IFF signals the moment you leave the house. Wait until you are just about to reach the HQ's first observation post. This reduces the chance of an enemy picking up on it. It may make sense to combine a number combination. For example... on arrival of the front gate display an orange and yellow square in your front left windshield. Stop 100m from the gate. When the gate guard positively ID's your car, they will flash a light a number of times. Respond by flashing your head lights so the total is 10.

F) Night Vision/darkness IFF. If your unit has night vision, ways to positively ID friendly units are helpful. IR. strobes are the best choice. Some can be programmed to strobe in certain patterns. This is useful for large organizations. If IR strobes are not available look at other options (and test them first) such as IR reflective clothing, patches, bands ect.

G) Vehicle darkness IFF. Combining vehicle IFF and darkness IFF. At night, it is hard to tell most vehicles apart. A colored gel filter (clear colored plastic) over a headlight, or an additional colored light in the dash, or a strobe light are all options. If the vehicles are operating without lights, then chemical lightsticks on the antenna or dash helps ID them (it is somewhat a compromise of light discipline, so only use when appropriate.) If using IR night vision, regular IR IFF methods work for vehicles too.

H) Concealed position IFF: If you have friendly troops approaching a hidden observation post, you don't want the hidden observers to give up their position by issuing the challenge word. We want the point man of our friendly forces to have some signal that can indicate that he knows he is approaching the hidden OP, and that he is friendly. Usually the signal is an arm gesture, or object hold. Once the signal is recognized, the observer would make a discrete noise (such as a "hiss" or "shh") to let the pointman know he is seen. The pointman would then say or hand signal (depending on noise discipline) how many total (including himself) people are behind him in his team. That prevents an enemy from "coat tailing" and following a returning patrol in to their base.
Examples of different gestures:
Hold left arm straight out.
Hold rifle in front, by barrel end, stock down.
Elbow up, hand in front of mouth, palm out.

These different signals are easy to maintain and should be able to be seen in low light as well.

GRAPH- Concealed IFF

7. Radio authentication /IFF: IFF for radio is a little more challenging, because it is much easier for the enemy to listen in without being detected. We will look at two approaches here. The first method is much like the challenge/response system. It uses an authenticator word, and "rule". The best authenticator words are 10 letter isograms. That is, a 10 letter word, where no letter repeats.

"CAMPGROUND" fits the requirements, so we will use it as an example. A simple rule would be "corresponding number"

B6: "Bravo one, Authenticate Papa, over"

B1: "I authenticate four, over" *(because "P" is the 4th letter in the word)*

B6: "Roger, Out"

We can change the rule, and use the same word. For instance, if the rule becomes "corresponding number times 2, then minus 1" Well thats a little more complicated, but if we are authenticating "P",

the answer is “7” (P is the 4th letter, times 2 = 8, then minus 1=7) The benefit is that it makes it a little harder to determine what the authenticator word is.

While the word has 10 letters, it is really only effective for 4-6 authentications. Much like the TV show “Wheel of Fortune” after enough letters show up, you can guess the word.

“LU****JA*K” can only be a few words. The chances of the enemy correctly guessing “LUMBERJACK” go up with each letter used.

A more advanced method is to use 2 letters, with a rule such as add, or multiply them.
For example, If the word is “LUMBERJACK” and our rule is add the 2 values then:

B6 “Bravo One, Authenticate Mike, Romeo over”

B1 “I Authenticate nine, over” (M=3, R=6, 3+6=9)

B6 “Roger, you are authentic. Out”

This method will allow a few more authentications before the word becomes compromised.

There is a more advanced authentication system we can use called DRYAD, that will be covered in Chapter VII. Advanced Authentication: DRYAD, pp 48.

8. Communications specific codewords:

A) Radio frequencies. Having codes for frequencies is handy for radio coms. This is an exception to the sequential codewords rule.... For example if I use snake names in alphabetical order, that helps me remember Anaconda is Ch1, Boa constrictor is Ch2, Cobra is Ch3, Diamondback is CH4... ect.

Saying on the radio "Change to channel 4" gives anyone eavesdropping the hint they need to also change channels, whereas "Diamondback, Diamondback" tells them nothing.

B) You need a codeword for if the radios are compromised.... i.e. during a fight, the enemy captures one of your team radios. If you say over the air " The bad guys just grabbed Ron's radio" then everyone knows what is up, if however your compromise codeword is "watergate" then saying "watergate, watergate" lets everyone know that it is compromised, without letting the enemy know that you know. The team leader may then respond with "Diamondback, Diamondback" so everyone knows to change to channel four. The TL may then use the compromised radio as a deception, for instance, and say on the original channel. "Alpha team... flank to our left, their right" while actually ordering a flanking maneuver to the opposite side.

C) Have a codeword for wiping the radio. In the U.S. military, most radios have a "zero" function that wipes out all of the frequency hopping tables and COMSEC encryption keys, essentially resetting the radio to factory defaults. If a position is about to be overrun, or a radio must be abandoned, the radio operator announces to the net their callsign, the codeword, and then zeros the radio. This guarantees that the radio falling into the enemy hands does not compromise the rest of the radio net. It also lets the net know how serious your trouble is. (If your radios have it... it is good to know how to reset to factory defaults, so the bad guys can't use the radio against your team)

D) The same guidelines for creating codenames also applies to codewords.

9. Professional SOI's may also include an index, distribution list (so you know who has received it, which helps in determining if it has been compromised), encryption keys, frequency hop tables, codewords, operation codes, handling procedures, destruction procedures, ect.

10. Here is an example SOI: *(with notes in italics)*

Effective: 10/1/2015 through 10/30/2015
ID codenames: changes at 24:00 local

	10/1-3	10/4-6	10/7-9	10/10-12	10/13-15	10/16-18	10/19-21	10/22-24	10/25-27	10/28-30
Command	Liberator	Dragonfly	Beagle	Maverick	Deputy	Apache	Alabama	Cardinal	Hornet	Cowboy
Team 1	Thunder 1	Beetle 3	Boxer	Goose	Ranger	Iroquois	Georgia	Robin	Raptor	Indian
Team 2	Thunder 2	Hornet 1	Greyhound	Iceman	Marshal	Comanche	Tennessee	Vulture	Eagle	Pirate
Team 3	Lightning 1	Hornet 7	Shepard	Betty Blu	Trooper	Kiowa	Virgina	Falcon	Tomcat	Ninja
Medevac	Lightning 2	Beetle 4	Bloodhound	SnakeDr.	Sheriff	Blackhawk	Arkansas	Buzzard	Phantom	Samurai

(Note, this uses several different formats to help with OPSEC. Codenames change every three days. To help throw any enemy listeners off, notice how there is a "Hornet 7"... that may cause the enemy to wonder where hornet 1-6 are... you don't want to repeat numbering patterns. Also notice that the codenames generally follow a similar theme each time they change, but you can't determine a units function based on the name.)

Frequency Assignments:

	10/1-3	10/4-6	10/7-9	10/10-12	10/13-15	10/16-18	10/19-21	10/22-24	10/25-27	10/28-30
Cmd Pri	FRS 6	FRS 17	FRS 6	FRS 7	FRS 11	FRS 22	FRS 7	FRS 16	FRS 1	FRS 3
Cmd Alt	FRS 16	FRS 2	FRS 3	FRS 12	FRS 1	FRS 11	FRS 17	FRS 6	FRS 22	FRS 1
T1 Pri	FRS 1	FRS 12	FRS 21	FRS 16	FRS 12	FRS 7	FRS 8	FRS 17	FRS 21	FRS 7
T1 Alt	FRS 11	FRS 1	FRS 4	FRS 6	FRS 2	FRS 18	FRS 18	FRS 7	FRS 2	FRS 11
T2 Pri	FRS 2	FRS 22	FRS 16	FRS 3	FRS 13	FRS 21	FRS 9	FRS 18	FRS 3	FRS 13
T2 Alt	FRS 12	FRS 3	FRS 1	FRS 13	FRS 3	FRS 2	FRS 19	FRS 8	FRS 20	FRS 17
T3 Pri	FRS 3	FRS 19	FRS 17	FRS 11	FRS 14	FRS 8	FRS 10	FRS 19	FRS 19	FRS 21
T3 Alt	FRS 13	FRS 3	FRS 2	FRS 21	FRS 4	FRS 19	FRS 20	FRS 9	FRS 4	FRS 2
Medvac Pri	FRS 5	FRS 5	FRS 5	FRS 5	FRS 5	FRS 5	FRS 5	FRS 5	FRS 5	FRS 5
Medvac Alt	FRS 15	FRS 15	FRS 15	FRS 15	FRS 15	FRS 15	FRS 15	FRS 15	FRS 15	FRS 15
Car to Car Pri	CB 1	CB 1	CB 17	CB 17	CB 2	CB 2	CB 28	CB 28	CB 5	CB 5
Car to Car Alt	CB 5	CB 5	CB 39	CB 39	CB 3	CB 3	CB 6	CB 6	CB 11	CB 11
Long Pri	7.275 LSB	7.225 LSB	7.300 LSB	7.250 LSB	7.290 LSB	7.240 LSB	7.265 LSB	7.280 LSB	7.240 LSB	7.275 LSB
Long Alt	14.275 USB	14.250 USB	14.325 USB	14.310 USB	14.300 USB	14.290 USB	14.270 USB	14.320 USB	14.310 USB	14.280 USB
Guard	CB 10	CB 10	CB 10	CB 10	CB 10	CB 10	CB 10	CB 10	CB 10	CB 10

Note: This plan uses 3 types of radios. 22 channel FRS/GMRS bubblepack radios for most coms, 40 channel CB radios for vehicle (Car to Car) coms and guard, and HAM HF radio for long distance coms.

It assumes the command post will be able to monitor both primary and alternate FRS command channels, the CB guard channel, and both HF HAM channels when HF is used in a mission.

This chart can change drastically based on equipment available, and mission requirements. Some thought into frequency planning and spectrum management is a must.

Since they are more "emergency" type functions, the Medevac channels, and guard channels don't change, so are less likely to be forgotten.
The Guard channel is usually not used, unless there is a problem on the normal radio channels. With this plan, each team would need to carry at least one CB radio so that if FRS is being jammed/not working, they can still contact via guard channel.

Frequency Codewords:
Primary frequency:"Anaconda"
Alternate Frequency: "Cottonmouth"
Guard Channel: "Diamondback"

COMSEC Codewords:
Enemy is listening in: "Watergate Green"
A radio has been captured/compromised: "Watergate Red"
We are about to be over run, and are wiping all radios and COMSEC: "Niagra Falls"

Pyro signals:
Medical emergency: 1 green starburst flare

In Contact: 1 red starburst flare
Being over run: 1 red and 1 green starburst flare

Sound signals (Whistle, horn):

continuous blast: ALARM
3 long blasts: ASSEMBLE
1 long blast: MOVE OUT or ATTACK
2 long blasts: WITHDRAW
1 long and 1 short blast: RIGHT FLANK PULL IN
1 short and 1 long blast: LEFT FLANK PULL IN
2 short and 1 long blast: SHIFT LEFT
1 long and 2 short blasts: SHIFT RIGHT
4 short blasts: REGROUP
1 long, 1 short, 1 long blast: ASSEMBLE ON LEADER

Vehicle IFF: 1 red and 1 blue square in corner of windshield (day)
1 green light out windshield (night)

IFF:

	10/1-3	10/4-6	10/7-9	10/10-12	10/13-15	10/16-18	10/19-21	10/22-24	10/25-27	10/28-30
Challenge	Elephant	Handcart	Lampshade	Television	Halibut	Popcorn	New York	Showtime	Broadway	Trashcan
Response	Pizza	Cocacola	Passport	Lemonade	Typhoon	Basket	Baseball	Bedspread	Streetcar	Steamer
Duress	Continent	Continent	Continent	Continent	Continent	Continent	Continent	Continent	Continent	Continent
Running	Horseshoe	Horseshoe	Wakeboard	Wakeboard	Ostrich	Ostrich	Emerald	Emerald	Rosebud	Rosebud
Number	14	7	9	10	15	13	8	12	11	16
Radio Auth	CAMPGROUND	LUMBERJACK	AFTERSHOCK	NIGHTMARES	PATHFINDER	DOWNSTREAM	BLACKSMITH	CLOTHESPIN	TRAMPOLINE	MALNOURISH

Concealed gesture: Hold non gun hand on top of head

Note that the duress password doesn't change. Duress should hardly ever get used.. and you don't want someone forgetting it if they really under duress.

If I had night vision operations, I would add their signals to the IFF chart.

VI. Signals in Mission Planning

A missions communication plan is different from an SOI. SOI's provide an over-arching commonality to be used by all units in an AO, for a given timeframe. Mission COMPLANs on the other hand, take the parts of the SOI that are relevant for that mission, and format them for practical use. Imagine two companies from the same division performing different missions in an AO. If one company runs into the other during their mission, having a common set of IFF signals, call signs, and radio frequencies mean that the two companies can communicate, and ID them selves, and avoid friendly fire. SOI's also allow for much faster integration of disparate units if a mission's needs change unexpectedly.

Army COMPLANs typically set links within a unit, and then to the next echelon up. For example:

A platoon may have squad radios for the platoon leader to talk to his 3 squad leaders (the lowest echelon), and a platoon radio operator with different equipment that talks to the company leadership, and other platoons with in his company (the next echelon up). The company HQ will have the platoon radio net, and a radio to talk to battalion, and the other companies in the same battalion (next echelon up)

If a squad in one company needed to send a message to a squad in another company, unless the mission had prior arrangements, the message would go squad, platoon, company, battalion, back down to receiving company, to receiving platoon, squad, ect...

For each echelon of communications, we want to plan for multiple ways of communicating.

We use the acronym PACE to help with the planning.

Primary
Alternate
Contingency
Emergency

It is important to remember that “PACE” is just a guideline, and not an absolute rule.

For example:

Scenario: Your group has 2 teams of 4, performing recon patrols. (Bravo one and Bravo two)
You have a 6 person team standing by as a quick reaction force (Bravo three)
Your leadership is Bravo six, and there is a defense element at your base of 4 people, (Bravo 4)
Your group also has a mutual aid agreement with a neighboring group. (Charlie 6)

The COMPLAN may look like this:

Within the teams (lowest echelon)

Primary: Hand signals
Alternate 1: team radio ch 1 (these channels would have been defined in the SOI)

Alternate 2: Team radio ch 11
Contingency: Yell
Emergency: Whistle

Or

Primary: Hand signals
Alternate: Whisper/voice
Contingency: Yell
Emergency: Whistle.

Notice, the second COMPLAN doesn't involve radios. Maybe not everyone has a radio, or maybe the enemy has strong SIGINT capabilities. Just because you have a radio, doesn't mean you have to use it. SOIs and COMPLANS do work as planning tools even if you don't have radios. This COMPLAN works because the team members should be within range of all of the listed methods of communication.

For the next echelon up, to allow B1 or B2 to call and ask for the quick react force, we assume they will be farther away than the intrateam COMPLAN allows for.

So it might look like:
Primary: Radio Ch 6
Alternate: Radio Ch 16
Contingency: HAM HF radio 14.275Mhz USB *(This and the "regular" radio channels would all be pre defined in the SOI)*
Emergency: 3 gunshots followed by flare. *(and the flare meanings would be outlined in the SOI.)*

Notice this COMPLAN has 2 different radio systems. Ham HF takes a little time to set up, which is why it is a contingency in this plan. The gunshots and flare grab attention, which make them appropriate for an emergency signal.

The next echelon up would be between your groups leadership, and the neighboring groups leadership.

It's COMPLAN might look like this:

Primary: Telephone *(make sure you have their numbers, and they yours)*
Alternate 1: Text messages
Alternate 2: Email
Contingency 1: HAM radio HF on 14.275Mhz USB at 18:00 local and 20:00 local
Contingency 2: HAM radio HF on 7.275Mhz LSB at 18:15 and 20:15 local
Emergency: Courier

This plan uses 2 different HF HAM frequencies on different bands to allow flexibility in different atmospheric conditions. While courier isn't fast, if the other group is a distance away, "emergency" may dictate a courier as a measure of last resort.

The COMPLAN should also include mission specific codewords, and Days and times of scheduled communications.

PART 2

Everything up to this point should be usable by anyone in a group using radios at all times.

For a civil mission, or training exercise where the focus is not on radio, the SOI and COMPLAN can be the same thing and as simple as:

All radios CH 1=primary, CH2 =Alternate. Cellphone= contingency, aerial flare= emergency.

Authentication word is "CAMPGROUND"

ID's are name unless otherwise assigned.

The above SOI/COMPLAN is simple and to the point, and appropriate for the simple application it is being used for. As complexity is needed, or signals other than radio, or more IFF, ect... then more of the COMPLAN and SOI get added.

It is important in training to at least use the minimum SOI/COMPLAN during any mission or activity briefings, so participants will get used to the format, and understand the use of them.

The rest of this handbook covers advanced authentication, encryption, COMSEC, and jamming. In the real world, it probably will not be used as much, because it adds a layer of complexity to training that may take away from the main lesson. (I.E. if you are training to patrol, wait until almost everyone has patrolling down solid before adding the complexity of encryption to the lessons)

It is information that is still essential to learn, and should be practiced somewhat regularly, so that it can be used when needed.

VII. Advanced Authentication
DRYAD

The simple radio authentication method listed in Chapter V, Signals Operating Instructions, pp 35. sometimes is not sufficient because it does not allow for enough authentications before becoming compromised. The U.S. army developed a system originally codenamed “DRYAD”, which saw regular use up until digital encryption became widespread.

The DRYAD system uses a chart similar to the one that follows on the next page.
The top “UID” is unique I.D. the example DRYAD sheet uses the word “APPLE” as the I.D. Each DRYAD sheet will have a different name, to keep them differentiated. It is much easier to say “Make sure everyone has DRYAD sheet APPLE” instead of “Make sure everyone has the DRYAD sheet that starts with: 'AUZM'.” The “Start DTG” and “End DTG” are the Date Time Group fields for when the dryad sheet is in use. Also known as the “cryptoperiod.” A long mission may issue several DRYAD sheets, and cryptoperiod is the time each sheet is in effect. The “Distribution” field allows each sheet to be individually numbered or named for accountability. More info on accountability is covered in Chapter XIII. Comsec Materials, pp 73.

The alphabet is listed in a column on the left. Across the top are the numbers 0-9, and the alphabet, split into groups of 2-4 letters. These lines across the top have several functions which will be discussed later.

To authenticate, the person requesting authentication picks a letter in the left hand column, and then picks a random letter from the alphabet (which will be in the row.) The responder will find the corresponding letter on their copy of the DRYAD sheet, and respond with the letter below the one chosen.

For example:

“Bravo One, This is Bravo Six... Authenticate Delta Victor, Over”

We go down to row “D”, and then go across to the letter “V”. We see that the letter immediately under it is the letter “K” so B1 would respond “Bravo Six, This is Bravo One... I Authenticate Kilo, Over.”

It is important that both parties mark authenticators once they have been used, so they are not re-used.

This method allows us 625 Authentications, instead of the 4-6 we get from a single authentication word. We can have even stronger authentication by using two-factor authentication. Instead of just responding with the letter, we can have a rule that adds a second factor to the response. We could use the numbers from the top row, or the matching letters from the top rows, or have another positional relation. Consider these different rules for the same “Authenticate Delta Qubec...”

Rule: Letter below plus number = “Kilo, two”
Rule: Letter below plus next letter below = “”Kilo Uncle”
Rule: Letter below plus corresponding reference letter (the letters in the alphabet just above the numbers) = “Kilo, Juliet”
Just remember to not make it too complicated so you don't make mistakes.

For Training Use Only						UID:	APPLE			
Start DTG:					End DTG:					
Distribution:										
	ABCD	**EFG**	**HIJ**	**KL**	**MN**	**OPQ**	**RS**	**TUV**	**WX**	**YZ**
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
A	AUZM	KJE	WRY	CB	HT	PXD	QI	SFG	LO	VN
B	SABV	ILR	HQD	ZF	TJ	CYM	PE	UKO	XG	WN
C	SGRB	HAU	DWQ	LN	OI	TEK	YP	JZF	MV	XC
D	NYSO	QJK	MAV	RH	WT	ZXE	UP	IFL	BG	CD
E	GZHV	XMI	AJK	UQ	RS	YCE	PB	DLT	FO	WN
F	VTYJ	BRS	LMH	WD	ZI	QKX	AU	OGF	NE	PC
	ABCD	**EFG**	**HIJ**	**KL**	**MN**	**OPQ**	**RS**	**TUV**	**WX**	**YZ**
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
G	XSIJ	PGD	ZTL	RY	KE	BQV	OM	CNU	HF	AW
H	QAJU	VYR	ILF	MZ	WT	PBX	NO	DKC	SH	EG
I	JVPX	CQH	SIU	KE	WO	RML	AY	DGT	FZ	NB
J	LDSW	GBI	ECU	QH	YN	ROK	FP	JXV	ZA	TM
K	LGWI	UXZ	QRM	PT	YJ	SOV	FA	CBD	EK	NH
L	HGQE	JSY	CRN	BM	PO	DAU	KZ	FTL	IX	WV
	ABCD	**EFG**	**HIJ**	**KL**	**MN**	**OPQ**	**RS**	**TUV**	**WX**	**YZ**
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
M	ZTRP	BEH	GVQ	UI	KN	JDY	SM	WFA	OX	CL
N	RVAE	PWT	KCQ	OJ	IF	SZD	UG	MBH	YL	NX
O	CKBI	OEQ	HAL	GM	WU	DRS	YF	PVX	NZ	JT
P	PDTN	XVW	GHE	AL	UR	CYI	OZ	JSM	KQ	BF
Q	QEZB	CSH	LJX	YV	TW	RFI	KA	PUG	NO	DM
R	LIEZ	BNR	VFJ	YU	KH	OPM	DA	MCG	SQ	TX
	ABCD	**EFG**	**HIJ**	**KL**	**MN**	**OPQ**	**RS**	**TUV**	**WX**	**YZ**
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
S	HANP	TQE	FGB	SW	CY	VDU	ZK	JXI	OR	LM
T	XNZR	COI	FTG	AY	PB	KVS	DH	JQW	UM	LE
U	MCFR	YKZ	DBT	PS	EA	XIQ	WU	HLG	VN	OJ
V	BEYC	HUJ	XPL	IM	VQ	NKD	TW	GAR	OS	ZF
W	ZXWA	TED	LMJ	RU	SF	ONB	HP	IQK	YC	VG
X	IVBD	YSN	RPC	FW	KM	AOZ	JX	HLU	QG	ET
Y	SVXM	BDU	WTG	JN	ZO	HFQ	IA	PKL	CR	YE
Z	HXFB	NYP	DCU	MG	SE	OIW	VT	QRZ	LJ	AK

VIII. COMSEC

Communications Security or COMSEC is preventing the enemy from learning the content of your communications. Whereas Transmission Security (TRANSEC) is preventing the enemy from detecting your signals.

If I see Bob lean over and whisper to Jane, then I can determine that Bob is transmitting information to Jane, but not what that information is. That is TRANSEC. If Ralph gets up to leave, and a note falls out of his pocket, and I pick it up and read it, I may not have seen who sent the note, but since I can read the content of it, COMSEC is compromised. If I overhear Ralph whisper to Bob, then I have detected both the transmission of information, and the content of it. That is COMSEC and TRANSEC.

COMSEC and TRANSEC fall under the broader category of Operational Security, or OPSEC. OPSEC is the process of protection information that an enemy or opponent can use against you.

Information that generally falls under OPSEC includes (but is not limited to):

1) Capabilities. What can you do? (includes skills and equipment and training)
2) Limitations. What are you not able to do?
3.) Locations. Where are you now? Where have you been? Where are you going? Where do you frequent?
4. Makeup. How big is your group? How well trained are they? What is their experience? What is the chain of command?
5. Communications details. Everything in the COMPLAN and SOI can be useful to a capable enemy.
6. Logistics. What material do you have? How long will it last?

While COMSEC and OPSEC are important, insuring them come at a price of time, or financial cost, or complexity. A group needs to balance the threat level to the COMSEC requirements.

The U.S. Military generally uses TRANSEC and COMSEC measures at all times in war zones, because they are often up against well equipped and well trained enemies. A small group, however may not need to go all out on COMSEC procedures. When considering what measures to implement, there are several factors to consider.

1) What is the threat?
2) What is their technical capability?
3) What is their persistance?

Administrative duties in a non-threat environment generally don't require any COMSEC. Indeed, most commercial business radio operators operate this way. There is very little threat to a stranger hearing a radio from a hotel asking maintenance to go to room 1805 to unclog a stopped toilet. Even on military bases in the U.S. there are lots of admin coms that are sent in the clear.

Likewise, civil support operations usually don't need a lot of effort put into COMSEC. There is no “enemy” to be a threat. A search and rescue after a natural disaster, or helping a special event with coms or other duties can easily use radios with little risk.

If there is a threat but little capability, or persistance, then rudimentary COMSEC will often suffice. Looting after storms or natural disasters, or the outbreak of civil unrest may result in criminals and

opportunists going out and becoming a threat to your group. They most likely will not have radio intercept capabilities, unless they just happen to be using radios similar tor yours and on the same frequencies. Because of the nature of looters, they will not be persistent in intercepting signals, so simple use of codewords or codebooks (discussed in the next chapter) should suffice.

If the threat is persistent and capable, then at minimum, codewords that change frequently, or preferably some form of full encryption. Codebooks with DRYAD sheets (chapter X) and one time pads (chapter XI) should be used if electronic encryption systems are not available.

If the threat is very capable such as state sponsored actors, professional agencies, or governments then if radios must be used, encryption is mandatory, although not using radios unless absolutely necessary may be the best course.

U.S. Army SIGINT, photo courtesy of U.S. Department of Defense

IX. DRYAD and simple encryption

	ABCD	EFG	HIJ	KL	MN	OPQ	RS	TUV	WX	YZ
	0	1	2	3	4	5	6	7	8	9
A	AUZM	KJE	WRY	CB	HT	PXD	QI	SFG	LO	VN
B	SABV	ILR	HQD	ZF	TJ	CYM	PE	UKO	XG	WN
C	SGRB	HAU	DWQ	LN	OI	TEK	YP	JZF	MV	XC
D	NYSO	QJK	MAV	RH	WT	ZXE	UP	IFL	BG	CD
E	GZHV	XMI	AJK	UQ	RS	YCE	PB	DLT	FO	WN
F	VTYJ	BRS	LMH	WD	ZI	QKX	AU	OGF	NE	PC

The section above is from DRYAD sheet "APPLE" shown earlier. In addition to using it to authenticate, it can also be used to provide simple encryption.

Typically the words "I SET" are used to indicate that what follows is encrypted. If I want to send a new radio frequency, and that frequency is 144.52 Mhz, I would send :

I Set :Charlie, Hotel, Oscar, India, Echo, Quebec.

"Charlie" defines what row I am using. Since the first number I want to send is "1", I go to the column under one, down to the row where "Charlie" is and I see a box with three letters: "HAU" I can use any of the three letters. In this instance I used "H" (Hotel). For the second number; "4", my options are "O" or "I". Since my third digit is also "4", I end up using both "Oscar" and "India". "Echo" and "Quebec" are under the columns for "5" and "2" respectively.

A general rule for encoding frequencies is that it is always 3 digits in megahertz, and anything after three digits is after the decimal place. So 14.313Mhz would be encoded as "014313"

Lets decode the following encrypted number:

I Set: Foxtrot, Echo, Alpha, Golf, Kilo, Whisky, Juliet, Papa.

The solution is on the next page.

I Set: Foxtrot, Echo, Alpha, Golf, Kilo, Whisky, Juliet, Papa.

	ABCD	EFG	HIJ	KL	MN	OPQ	RS	TUV	WX	YZ
	0	1	2	3	4	5	6	7	8	9
A	AUZM	KJE	WRY	CB	HT	PXD	QI	SFG	LO	VN
B	SABV	ILR	HQD	ZF	TJ	CYM	PE	UKO	XG	WN
C	SGRB	HAU	DWQ	LN	OI	TEK	YP	JZF	MV	XC
D	NYSO	QJK	MAV	RH	WT	ZXE	UP	IFL	BG	CD
E	GZHV	XMI	AJK	UQ	RS	YCE	PB	DLT	FO	WN
F	VTYJ	BRS	LMH	WD	ZI	QKX	AU	OGF	NE	PC

The first letter sets us to row “F”. When we go across and find the “E” for “Echo” we see it is in the “8” column. “Alpha” is in the “6” column. “Golf” is in the “7” column. “Kilo”, “Whiskey”, “Juliet”, and “Papa” are in the “5”, “3”, “0” and “9” columns respectively. So we put it to gether and we get “8675309” (The famous phone number from the song “Jenny” by Tommy Tutone.)

If I want to encrypt a longer number, or a number that has a lot of repeating digits, I have two options. We will use 1-800-588-2300 as an example.
The problem is that my number to encrypt has “8” three times, but I only have 2 keys in any one column on the DRYAD sheet. This leaves me with two options.

Option one. Reuse a key letter. This is easier to do, but is a little less secure. Only use this option if you believe your opponent doesn't have strong cryptanalysis capabilities.
If we decide to use row “B”, then 18005882300 would encrypt as:

I Set: Bravo, Romeo, X-ray, Victor, Alpha, Charlie, Golf, X-ray, Hotel, Zulu, Sierra, Bravo.

Notice “X-ray” appears twice... that gives your opponent a clue. It may not be enough, but depends a lot on what the number represents. If they know it is a frequency, and have an idea of what type of radios you use, it may be enough to give it away. If there is no or little context, it is less likely to be compromised.

Option two. Break the encryption into two parts. For this example, we will send the “180058” encrypted on row “C”, and then use row “E” for the second half, (82300.)
to do this, we simply add the word “BREAK”, followed by the next row we want to use, and then the encryption.

The first half, “180058” on line “C” comes out as “HMSGTV.” The second half, “82300” encrypted with line “E” comes out as “FXUGZ” Notice the letter “G” appears in each half. It represents a “0” in both lines. That is something we want to avoid, because it defeats the purpose of the break. So instead of using row “E”, we'll use row “D”. “82300” when encrypted with row “D” comes out as “GMRNY” We put the two halves together: C “HMSGTV”/D “GMRNY”

I Set Charlie, Hotel, Mike, Sierra, Golf, Tango, Victor, Break, Delta, Golf, Mike, Romeo, November, Yankee.

Make sure that you mark every used letter off of your DRYAD sheet as you use them for both sending and receiving. If letters get reused, they can compromise both encryption and authentication.

The DRYAD sheet can also be used to encrypt words, or very small messages. The same concept as encrypting numbers is used, except that the letter at the top of the column (just above the number) is used.

	ABCD	EFG	HIJ	KL	MN	OPQ	RS	TUV	WX	YZ
	0	1	2	3	4	5	6	7	8	9
A	AUZM	KJE	WRY	CB	HT	PXD	QI	SFG	LO	VN
B	SABV	ILR	HQD	ZF	TJ	CYM	PE	UKO	XG	WN
C	SGRB	HAU	DWQ	LN	OI	TEK	YP	JZF	MV	XC
D	NYSO	QJK	MAV	RH	WT	ZXE	UP	IFL	BG	CD
E	GZHV	XMI	AJK	UQ	RS	YCE	PB	DLT	FO	WN
F	VTYJ	BRS	LMH	WD	ZI	QKX	AU	OGF	NE	PC

If, for example, a patrol goes out for longer than expected, and needs the challenge/response words from the SOI for their expected day of return, those words can be sent using the DRYAD sheet.

If the challenge and response words are: “trashcan” and “steamer” we encrypt each word using a different row from the DRYAD sheet. Notice: “trashcan” has the letter “a” twice, and “steamer” has two of the letter “e”. Just like long numbers, we can reuse the key letter (slightly less secure) or break each word (slightly more secure, but a little more effort.) Since these are just random words, the enemy doesn't have much context to help with decrypting them, so it should be safe to reuse one key letter. If the word being sent has lots of repeating letters, then it should probably be broken down to multiple lines. (Like “banana”)

I will encrypt “trashcan” using line “E”. I find the letter “T” at the top (just above number “7”) and come down to row “E”. that lands on letter “D” “R”=”P”, “A”=”G”, “S”=”B”, “H”=”A”, and “C”,”A”,”N” are “H”, “G”, and “S” respectively.

I Set Echo, Delta, Papa, Golf, Bravo, Alpha, Hotel, Golf, Sierra.

Notice, unlike numbers, you can only use the one letter directly under the letter you are encrypting. On row

Decrypt the following:

I Set Foxtrot, Delta, Golf, Zulu, Tango, Bravo, Alpha, Hotel, Victor, Yankee, Whiskey.

The solution is on the next page.

	ABCD	EFG	HIJ	KL	MN	OPQ	RS	TUV	WX	YZ
	0	1	2	3	4	5	6	7	8	9
A	AUZM	KJE	WRY	CB	HT	PXD	QI	SFG	LO	VN
B	SABV	ILR	HQD	ZF	TJ	CYM	PE	UKO	XG	WN
C	SGRB	HAU	DWQ	LN	OI	TEK	YP	JZF	MV	XC
D	NYSO	QJK	MAV	RH	WT	ZXE	UP	IFL	BG	CD
E	GZHV	XMI	AJK	UQ	RS	YCE	PB	DLT	FO	WN
F	VTYJ	BRS	LMH	WD	ZI	QKX	AU	OGF	NE	PC

I Set Foxtrot, Delta, Golf, Zulu, Tango, Bravo, Alpha, Hotel, Victor, Yankee, Whiskey.

"Foxtrot" tells us that we use row "F". When we find the letter "Delta" on row "F", and then go straight up we find it lands on the letter "L". Likewise, "Golf" goes up to "U". "Zulu" corresponds with "M".

Fully decrypted the solution is "LUMBERJACK"

Short encryption that can be done with the DRYAD sheet is handy for things like the 9-line MEDEVAC form presented earlier. The coordinates, and frequencies, and smoke color can be encrypted to protect the team on the ground. The rest of the info from the 9-line is not very actionable by the enemy, so that could be left in the "clear."

X. Codebooks

Codebooks are another tool that help with COMSEC. A codebook by itself shouldn't be considered encryption. It can be used in the clear for low threat situations, against opponents with low capabilities or persistance, but should only be used with other encryption when used in the presence of more advanced adversaries. Codebook material by itself offers the same level of security as code words as discussed earlier. Codebooks typically have common words and phrases, and each word or phrase will have a OPCODE code, numerical code, or both. Some words will also have a specified “to follow” section.

Here is an example codebook:

OPCODE	NUM Code	Term(s)	Data to Follow
ABC	000	Abort	
ADE	019	Address	
AEF	028	Affirmative	
AGH	037	Aircraft (fixed wing)	Qty: 2 digit 01-99
AIJ	046	Aircraft (large unmanned)	Qty: 2 digit 01-99
AKL	055	Aircraft (rotary winged)	Qty: 2 digit 01-99
AMN	064	Aircraft (small unmanned)	Qty: 2 digit 01-99
AOP	073	Armed Men	Qty: 2 digit 01-98 If more than 100, then three digit
			with the first two being "00" followed by how many hundred.
AQR	082	Attack	
AST	091	Barn/Shed	
AUV	109	Bearing (Magnetic)	3 digit compass bearing
AWX	118	Bearing (true)	3 digit compass bearing
AYZ	127	Boat/Ship	Qty: 2 digit 01-99
BBD	136	Border	
BDF	145	Building	
BEG	154	Car	Qty: 2 digit 01-99
BFH	163	Cave	
BGI	172	Checkpoint	
BHJ	181	Civilian	Qty: 2 digit 01-98 If more than 100, then three digit
			with the first two being "00" followed by how many hundred.
BIK	190	Clearing	
BJL	209	Compromise	
BKM	218	Computer	
BLN	227	Coordinate	
BMO	236	Creek	
BNP	245	Danger	
BOQ	254	Distance	Single Digit in 100's of meters
BPR	263	Do Not Answer	
BQS	272	Dog	
BRT	281	Door	
BSU	290	East	
BTV	359	Execute	
BUW	368	Farm	
BVX	377	Fence	
BWY	386	Figures	Use 99 to indicate last digits
BXZ	395	Forward this message to:	
BZA	429	Frequency	In Mhz. 7 digits XXX.XXXX
			So 14.3 Mhz is 0143000

OPCODE	NUMcode	Term(s)	Data to Follow
CAD	438	Friendly	
CBE	447	Gate	
CCF	456	Grid	Should be predetermined 6, 8, or 10 digit grid
CDG	465	Harbor	
CEH	474	Hill	
CFI	483	Home Base	
CGJ	492	I see	
CHK	510	Immediate	
CIL	529	Impossible	
CJM	538	Instruction	
CKN	547	Light Armor	Qty: 2 digit 01-99
CLO	556	Livestock	
CMP	565	Location	
CNQ	574	Medevac	
COR	583	Message Readibility	One figure: 1 to 5
CPS	592	Mountain	
CQT	608	Moving Away From	
CRU	617	Moving Towards	
CGX	620	My Location	
CSV	626	Negative	
CTW	635	North	
CUX	644	North East	
CVY	653	North West	
CWZ	662	Observe (ed)	
CXA	671	Possible	
CYB	680	Priority	
CZC	737	Probable	
DAE	746	Radio	
DBF	755	Rally	
DCG	764	Range	
DDH	773	Remain in place	
DEI	782	River	
DFJ	791	Road	
DGK	819	Sattellite Dish	
DHL	828	Signal Strength	One figure: 1 to 9
DIM	837	Soldiers	Qty: 2 digit 01-98 If more than 100, then three digit
			with the first two being "00" followed by how many hundred.
DJN	846	South	
DKO	855	South East	
DLP	864	South West	
DMQ	873	Street	
DNR	882	Tanks	Qty: 2 digit 01-99
DOS	891	Telephone	
DPT	909	Time	
DQU	918	Train	
DRV	927	Train Tracks	
DSW	936	Transmit	
DTX	945	Travel	
DUY	954	Truck	Qty: 2 digit 01-99
DVZ	963	Unknown	
DWA	972	Unseen	
DXB	981	Valley	
DYC	985	We Are	

Depending on how we plan to use the code book, we can use either the numbers (numerical code), or letters (OPCODE codes.)
OPCODE codes originated from early radio where morse code was the primary means of sending and receiving messages. In order to reduce the number of characters that had to be sent, some common 3-letter codes were created to represent longer messages. "Q" codes are still used in amateur radio.

Some common radio Q-codes are

QRO: Increase transmit power
QRP: Decrease transmit power
QRT: I am shutting down my radio
QRZ: Who is this?

Sending just the three letters takes far less time than sending the whole message in morse code.
The numerical code numbers work the same way.

If there is any information in the "to follow" column for a code, that info must always be sent, and will always be a pre determined length. For example "AGH"/"037" are the codes for fixed wing aircraft. We see that the "to follow" column indicates 2 digits, to indicate the quantity of aircraft. So four aircraft would be AGH04, or 03704 depending on which format used.

Some entries allow for 2 or 3 digit formats. The codes for "soldiers" "DIM"/"837" is an example. If there are fewer than 100 soldiers than the default 2 digit number will suffice. If there were 32 soldiers then "DIM32" or "83732" work. If there are more than 100 soldiers, then we need additional digits. If there were 320 soldiers, then "837320" might get mistaken for 83732 0?? with the "0" being mistaken for the first digit of the next numerical code. To avoid confusion, if the two specified digits are "00" then that means that there will be a third digit to indicate approximate size in hundreds. 837003 becomes Soldiers 003, which means approximately 300 soldiers.

If we need precision I can send "soldiers 99 figures 320 99 (the 99 indicates that it is the end of the figures.) So 320 soldiers becomes 83799 38632099

Here is a full example: I want to send a partial spot report to note that I see 12 unknown, armed men 200 meters north of my location.

First, I write out the message in plain text:
"I see 12 unknown armed men 200m north of my location."

Then I fit what words and phrases I can from the codebook:
"Observe unknown armed men(12) distance 200m north."

Notice I have left out the "I" as in "I observe", and "location" from :"north of my location", because those are assumed.

If we convert that to OPCODEs we get:
"CWZ DVZ AOP(12) BOQ (2) CTW"

If we use numerical codes we get:
"662 963 073(12) 254(2) 635

Decode the following:
"963154029540461744 7"

Solution:

963= “unknown”
154= “car” and the next 2 digits are the qty, so qty=2
954= “truck” and the next 2 digits are also qty, so qty =4
617= “Moving towards”
447= “gate”

So the result is unknown car qty 2, and trucks qty 4, moving towards gate.
In plain english that translates as “Two unknown cars, and 4 trucks are approaching the gate.”

If we represented the same with OPCODEs it would result in this:
“DVZBEG04DUY04CRUCBE” (DVZ BEG(04) DUY(04) CRU CBE)

XI. Using DRYAD for advanced encryption

As mentioned in the previous chapter, codebooks by themselves are not strong encryption. However when used in conjunction with the simple encryption offered by a DRYAD sheet, short messages can be quickly encrypted.

Using the example from above: “Two unknown cars, and 4 trucks are approaching the gate,” we have the coded versions of “ DVZBEG04DUY04CRUCBE” or “ 96315402954046174447” depending on if we use numerical codes or OPCODEs. We will go through the process of encrypting from either format.

First we want to break the letters or numbers to 5 letter groups to make managing it a little easier. 96315402954046174447 becomes 96315 40295 40461 7447

Using the DRYAD example from earlier:

	ABCD	EFG	HIJ	KL	MN	OPQ	RS	TUV	WX	YZ
	0	1	2	3	4	5	6	7	8	9
A	AUZM	KJE	WRY	CB	HT	PXD	QI	SFG	LO	VN
B	SABV	ILR	HQD	ZF	TJ	CYM	PE	UKO	XG	WN
C	SGRB	HAU	DWQ	LN	OI	TEK	YP	JZF	MV	XC
D	NYSO	QJK	MAV	RH	WT	ZXE	UP	IFL	BG	CD
E	GZHV	XMI	AJK	UQ	RS	YCE	PB	DLT	FO	WN
F	VTYJ	BRS	LMH	WD	ZI	QKX	AU	OGF	NE	PC

If we use row “F”, then 96315 encodes as “FPAWBQ”. F sets the row, “P” is under the number “9”, “A” is under the number “6” ect...

We have several options how to proceed. Which ever option is used should be decided before hand. Option one is to use a new row for each 5 letter break. This gives the most characters sent, but is easy and secure.

Option two is to keep using one row for the whole message. This means some characters may repeat, so isn't as secure against professional cryptanalysis, but is the fastest and easiest.

Option three is to use one row until there are no more un-repeating characters, and then “break” to start another row.

Here are all three options for comparison:
Original: 96315 40295 40461 7447

Option one:
FPAWBQ ERGAWY DWNTUQ CJOIZ *Notice, this is the longest because it adds a letter to each group*

Option two:
FPAWBQ ZVLCK ITZUR OIZG *Notice the “4” is repeated five times, so we have several “Z” and “I”'s that may help a professional cryptanalysis.*

Option three:
FPAWBQ ZVLCK IT “BREAK” ERPX DS “BREAK” DWI *Since each row allows the number “4”*

twice, and my coded message has the number "4" five times, that becomes the place I break the message.

Using OPCODEs works the same. The biggest difference is the fact that each letter only has a single match on a row of the DRYAD sheet, while numbers have 2 to 4 matches, so repeating characters happen more often.

The message from earlier: "DVZBEG04DUY04CRUCBE"

and the DRYAD extract:

	ABCD	EFG	HIJ	KL	MN	OPQ	RS	TUV	WX	YZ
	0	1	2	3	4	5	6	7	8	9
A	AUZM	KJE	WRY	CB	HT	PXD	QI	SFG	LO	VN
B	SABV	ILR	HQD	ZF	TJ	CYM	PE	UKO	XG	WN
C	SGRB	HAU	DWQ	LN	OI	TEK	YP	JZF	MV	XC
D	NYSO	QJK	MAV	RH	WT	ZXE	UP	IFL	BG	CD
E	GZHV	XMI	AJK	UQ	RS	YCE	PB	DLT	FO	WN
F	VTYJ	BRS	LMH	WD	ZI	QKX	AU	OGF	NE	PC

If we break it into 5 character groups we get DVZBE G04DU Y04CR UCBE

Again, we can use the same three options to encrypt the OPCODEs. Since there is a mixture of letters and numbers, you need to decode as you decrypt, or the numbers may throw off your decryption.

Option one FJFCTB EIRAVL DCNWSP CZRGH *Again, this is the most characters sent, but is easy to do.*

Option two: FJFCTB SVZJG PJIYA GYTB *The letters "C", "B", and "E" repeat several times in the original so they repeat in the encryption. This method is the easiest, and has the fewest characters, but is the most susceptible to professional cryptanalysis.*

Option three: FJFCTB SVZ "BREAK' EVL WGRHP "BREAK" DLSZX *Very secure, but the lomgest to send. Remember the first letter after "BREAK" sets the new row to decrypt from.*

Decrypt and decode the following messages using the codebook from the previous chapter, and the extract from the DRYAD sheet above.

Message one coded with OPCODEs, encrypted new row for each 5 character group (option one)
AZLNAHCIRKJBFAFYON

Message two coded with numerical codeS, encrypted all on one row (option two)
CMLJDOYHZPWSGVQTARNKX

Solutions:

Message one: “AZLNAHCIRKJBFAFYON”

	ABCD	EFG	HIJ	KL	MN	OPQ	RS	TUV	WX	YZ
	0	1	2	3	4	5	6	7	8	9
A	AUZM	KJE	WRY	CB	HT	PXD	QI	SFG	LO	VN
B	SABV	ILR	HQD	ZF	TJ	CYM	PE	UKO	XG	WN
C	SGRB	HAU	DWQ	LN	OI	TEK	YP	JZF	MV	XC
D	NYSO	QJK	MAV	RH	WT	ZXE	UP	IFL	BG	CD
E	GZHV	XMI	AJK	UQ	RS	YCE	PB	DLT	FO	WN
F	VTYJ	BRS	LMH	WD	ZI	QKX	AU	OGF	NE	PC

We know it is OPCODE with each 5 character group on a new row. That means each 5 character group has 6 characters because the first letter sets what row is to be used. So we want to break it up into 6 letter groups:

“AZLNAH CIRKJB FAFYON”

Because the message uses OPCODEs and not numerical codes, each character could represent a letter or number. Since I don't yet know which, I will put both down when I decrypt, and then once I decode using the code book, I can determine which is appropriate.

The cipher text“AZLNAH” means use row “A” to decrypt “ZLNAH”
In Letters ZLNAH decrypts to CWZAM. *If I go to row “A”, and go across to the letter “Z”, I find it is directly under “C” ect...*

Numbers decrypt to 08902

The next group, “CIRKJB” means that “IRKJB” decrypts with row “C”

I get “NCQTD” and “40570” for decrypting letters and numbers respectivly.

Finally “FAFYON” decrypts to “RCVTW” and “67078”

So I have CWZAM ZNQTD RCVTW as my decrypted letters, and
08902 40570 67078 as my decrypted numbers.

Now, I have to decode them with my code book.

CWZ= Observe (d)
AMN= Small unmanned aircraft
CQT=Moving away from
DRV=Train Tracks
CTW=North

So, the message is that the sender has “observed a small unmanned aircraft moving away from the train tracks in a northerly direction.”
Notice that we didn't need to use the decrypted numbers in this example. Sometimes that happens.

OPCODE	NUMcode	Term(s)	Data to Follow
ABC	000	Abort	
ADE	019	Address	
AEF	028	Affirmative	
AGH	037	Aircraft (fixed wing)	Qty: 2 digit 01-99
AIJ	046	Aircraft (large unmanned)	Qty: 2 digit 01-99
AKL	055	Aircraft (rotary winged)	Qty: 2 digit 01-99
AMN	064	Aircraft (small unmanned)	Qty: 2 digit 01-99
AOP	073	Armed Men	Qty: 2 digit 01-98 If more than 100, then three digit
			with the first two being "00" followed by how many hundred.
AQR	082	Attack	
AST	091	Barn/Shed	
AUV	109	Bearing (Magnetic)	3 digit compass bearing
AWX	118	Bearing (true)	3 digit compass bearing
AYZ	127	Boat/Ship	Qty: 2 digit 01-99
BBD	136	Border	
BDF	145	Building	
BEG	154	Car	Qty: 2 digit 01-99
BFH	163	Cave	
BGI	172	Checkpoint	
BHJ	181	Civilian	Qty: 2 digit 01-98 If more than 100, then three digit
			with the first two being "00" followed by how many hundred.
BIK	190	Clearing	
BJL	209	Compromise	
BKM	218	Computer	
BLN	227	Coordinate	
BMO	236	Creek	
BNP	245	Danger	
BOQ	254	Distance	Single Digit in 100's of meters
BPR	263	Do Not Answer	
BQS	272	Dog	
BRT	281	Door	
BSU	290	East	
BTV	359	Execute	
BUW	368	Farm	
BVX	377	Fence	
BWY	386	Figures	Use 99 to indicate last digits
BXZ	395	Forward this message to:	
BZA	429	Frequency	In Mhz. 7 digits XXX.XXXX
			So 14.3 Mhz is 0143000

OPCODE	NUMcode	Term(s)	Data to Follow
CAD	438	Friendly	
CBE	447	Gate	
CCF	456	Grid	Should be predetermined 6, 8, or 10 digit grid
CDG	465	Harbor	
CEH	474	Hill	
CFI	483	Home Base	
CGJ	492	I see	
CHK	510	Immediate	
CIL	529	Impossible	
CJM	538	Instruction	
CKN	547	Light Armor	Qty: 2 digit 01-99
CLO	556	Livestock	
CMP	565	Location	
CNQ	574	Medevac	
COR	583	Message Readibility	One figure: 1 to 5
CPS	592	Mountain	
CQT	608	Moving Away From	
CRU	617	Moving Towards	
CGX	620	My Location	
CSV	626	Negative	
CTW	635	North	
CUX	644	North East	
CVY	653	North West	
CWZ	662	Observe (ed)	
CXA	671	Possible	
CYB	680	Priority	
CZC	737	Probable	
DAE	746	Radio	
DBF	755	Rally	
DCG	764	Range	
DDH	773	Remain in place	
DEI	782	River	
DFJ	791	Road	
DGK	819	Sattellite Dish	
DHL	828	Signal Strength	One figure: 1 to 9
DIM	837	Soldiers	Qty: 2 digit 01-98 If more than 100, then three digit
			with the first two being "00" followed by how many hundred.
DJN	846	South	
DKO	855	South East	
DLP	864	South West	
DMQ	873	Street	
DNR	882	Tanks	Qty: 2 digit 01-99
DOS	891	Telephone	
DPT	909	Time	
DQU	918	Train	
DRV	927	Train Tracks	
DSW	936	Transmit	
DTX	945	Travel	
DUY	954	Truck	Qty: 2 digit 01-99
DVZ	963	Unknown	
DWA	972	Unseen	
DXB	981	Valley	
DYC	985	We Are	

Message two: CMLJDOYHZPWSGVQTARNKX, encoded with numerical codes, and encrypted all on one row.

	ABCD	EFG	HIJ	KL	MN	OPQ	RS	TUV	WX	YZ
	0	1	2	3	4	5	6	7	8	9
A	AUZM	KJE	WRY	CB	HT	PXD	QI	SFG	LO	VN
B	SABV	ILR	HQD	ZF	TJ	CYM	PE	UKO	XG	WN
C	SGRB	HAU	DWQ	LN	OI	TEK	YP	JZF	MV	XC
D	NYSO	QJK	MAV	RH	WT	ZXE	UP	IFL	BG	CD
E	GZHV	XMI	AJK	UQ	RS	YCE	PB	DLT	FO	WN
F	VTYJ	BRS	LMH	WD	ZI	QKX	AU	OGF	NE	PC

The first letter again indicates that it will decrypt using row “C”
I'll break it into 5 character groups just for ease of keeping track. So I get:

MLJDO YHZPW SGVQT ARNKX

Going Across row “C” to the letter “M” I find it is in column 8.
“L” is under 3, “J” is under 7, “D” is under 2, and “O” is under 4

That gives me 83724

YHZPW decrypts to 61762
SGVQT decrypts to 00825
And ARNKX decrypts to 10359

My full decrypted (but still encoded) message is 83724 61762 00825 10359.

In my codebook, I look up “837” and see that is “soldiers” and that the next 2 digits are how many, so I know that it is saying 24 soldiers “837(24)”

Looking at the next three numbers, “617” decodes to “moving towards”

“620” decodes as “My location”
“082” = “Attack”
“510” = Immediate”
“359” = “Execute”

Written out it reads: “soldiers (qty 24) moving towards my location. Attack, immediate, execute.”So the message is saying “24 soldiers heading towards my location. Attack now!”(“execute” means to carry out the instructions now)

A DRYAD sheet is a very versatile tool for the radio communicator. It can be used to authenticate, and encrypt small messages. When used in conjunction with a codebook, it can encrypt even longer more detailed messages.

XII. One Time Pads

Sometimes codebook and DRYAD encryption just is not enough for more complex and detailed messages. Imagine sending a full spot report (SALUTE), or SITREP. A DRYAD sheet would be quickly used up. For longer messages, we use a one time pad. When handled properly, one time pads (OTP's) provide mathematically unbreakable encryption.

One time pads are created by generating random numbers or letters, and those characters become the key.
Here is an example of a number based OTP:

0901

88265 31416 11104 80868 66789
36783 52386 23053 88185 93175
94518 61094 29730 03669 09794
80266 26735 47249 85094 61967
24597 84354 29142 36645 10627
79456 71091 32395 36984 77902
51195 08089 58390 92642 57007
98555 90811 88925 08587 55604
84461 81143 61985 19704 30098
36421 42037 39103 43817 18912

A letter based OTB is laid out the same, but with A-Z instead of 0-9.

Functionally, number based OTP's are easier to use, but can not carry as much information, while letter based OTP's carry more information, but require extra steps on encryption and decryption.

To use a OTP, first we need a message. We will use “The cow jumped over the moon” as our example message, and use the number OTP above to encrypt our message.

We need for each letter to be represented by a number so we will use a simple A=1, B=2,...Z=26 formula for now. To prevent misinterpretation, we will need every number that represents a letter to be two digits, so A=01, B=02,... If we don't then 1214 can become “ABAD” or “LN” because we don't know if it is 1-2-1-4, or 12-14. Making every letter 2 digits solves that problem.

code	A	B	C	D	E	F	G	H	I	J	K	L	M	N
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14
O	P	Q	R	S	T	U	V	W	X	Y	Z	?	!	_
15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
0	1	2	3	4	5	6	7	8	9	+	-	*	/	=
30	31	32	33	34	35	36	37	38	39	40	41	42	43	44

Starting with “THECOW...” The letter “T” is the 20th letter of the alaphabet. “H” is 8th, and “E” is 5th. “C”, “O”, “W”, are 3rd, 15th, and 23rd respectivly, so THECOW is represented by 20,08,05,03,15&23, or 200805031523.
“JUMPEDOVERTHEMOON” converts to “10211316050415220518200805131515 14”

Just as we have done before, we will break it up into blocks of five numbers for easy readibility.

2008050315231021131605041522051820080513151514 becomes:

20080 50315 23102 11316 05041 52205 18200 80513 15151 4

(Notice that it takes 46 characters to represent 23 letters.)

On the worksheet below, Each row lables “OTP Key” is a row from the OTP example above. The row “Message” is for the numbers that have been converted from the letters

OTP	88265	31416	11104	80868	66789
Message		20080	50315	23102	11316
Ciphertext					
OTP	36783	52386	23053	88185	93175
Message	05041	52205	52205	18200	15151
Ciphertext					
OTP	94518	61094	29730	03669	09794
Message	40000				
Ciphertext					

Notice that the first message block has been left empty. We leave the first block alone, so we have a reference to make sure we are using the correct OTP.

To encrypt, we simply add each digit from the OTP to the message digit below. If there is no number

in the message field, then essentially you are adding “0”.

If we look at the second OTB block, we see the number 31416 above the message block 20080. We are NOT adding the two numbers together. Instead, we add each digit individually. If the sum is more than 9, then drop the tens place. For instance, if I add 5 to 8, the answer is 13, but I only put “3” in the ciphertext block.

31416 and 20080:
3+2=5
1+0=1
4+0=4
1+8=9
6+0=6
so 51496 goes in the ciphertext block

We get the following as a result:

OTP Key	88265	31416	11104	80868	66789
Message		20080	50315	23102	11316
Ciphertext	88265	51496	61419	03960	77095
OTP Key	36783	52386	23053	88185	93175
Message	05041	52205	52205	18200	15151
Ciphertext	31724	04581	75258	96385	08226
OTP Key	94518	61094	29730	03669	09794
Message	40000				
Ciphertext	34518				

So “The cow jumped over the moon” becomes

88265 51496 61419 03960 77095

31724 04581 75258 96385 08226

34518

Decrypting is just as easy. Simply take the cipher text, and subtract the OTP key, and the result should be the number representation for the letters.

If we receive the above message, first we make sure we have the correct OTP. The first 5 numbers should be 88265. If they are the same, then we have the correct pad.

To decrypt the next two blocks: 51496 61419, I subtract the digits from the corresponding key: 31416 11104

5-3=2
1-1=0
4-4=0
9-1=8
6-6=0

6-1=5
1-1=0
4-1=3
1-0=1
9-4=5

We get 20080 50315

When we break it back into digit pairs:

20=T
08=H
05=E
03=C
15=O

The start of "the cow..."

Since the alphabet goes from 01-26, there are a lot of 2 digit numbers available. We can define a few for special purposes. If we want numbers we will use the values 30 – 39.
The number 1776, would convert to 31 37 37 36 before encryption.

code	A	B	C	D	E	F	G	H	I	J	K	L	M	N
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14
O	P	Q	R	S	T	U	V	W	X	Y	Z	?	!	_
15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
0	1	2	3	4	5	6	7	8	9	+	-	*	/	=
30	31	32	33	34	35	36	37	38	39	40	41	42	43	44

If we want to incorporate our codebook, we will use the value "00" to mark the beginning and end of encoded messages. This allows us to fit more information in less space.

For example, if I use the OPCODE code AOP (from the codebook example earlier) to indicate armed men, it requires a two digit quantity to indicate the number of people. 12 armed men is coded as

AOP12.

To convert it to numbers A=01, 0=15, P=16,... and the numbers convert as 31, 32 (for 1, 2) before encryption. The result is “00011516313200”. Note the “00” at the start and finish, to indicate that it is a code book reference.

Earlier in Chapter X, Codebooks, pp 56, we used the following example for codebooks:

“I see 12 unknown armed men 200m north of my location.”

and using our codebook, it encoded as:

CWZ DVZ AOP12 BOQ2 CTW

That converts to numbers as follows:

03 23 26 04 22 26 01 15 16 31 32 02 15 17 32 03 20 23 *notice that “12” converts to “31 32”*

Since we are using our codebook we need to mark the codebook sections with the“00” at the beginning and end.

When block grouped :

00032 32604 22260 11516 31321 51732 03202 300

When combined with the OTP key (starting with the second block)

31416 11104 80868 66789 36783 52386 23053 03669
This is the encrypted result:
31448 43708 02028 77295 67004 03018 26255 33669

With this table:

code	A	B	C	D	E	F	G	H	I	J	K	L	M	N
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14
O	P	Q	R	S	T	U	V	W	X	Y	Z	?	!	_
15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
0	1	2	3	4	5	6	7	8	9	+	-	*	/	=
30	31	32	33	34	35	36	37	38	39	40	41	42	43	44

and this OTP:

88265 31416 11104 80868 66789
36783 52386 23053 88185 93175
94518 61094 29730 03669 09794
80266 26735 47249 85094 61967
24597 84354 29142 36645 10627
79456 71091 32395 36984 77902
51195 08089 58390 92642 57007
98555 90811 88925 08587 55604
84461 81143 61985 19704 30098

36421 42037 39103 43817 18912

Decrypt the following:

88265 31456 21606 90988 76982
36863 04307 31195 89687 94265
44518

The solution:

Ciphertext	88265	31456	21606	90988	76982
Key	88265	31416	11104	80868	66789
Decrypted					
Ciphertext	36863	04307	31195	98687	94265
Key	36783	52386	23053	88185	93175
Decrypted					
Ciphertext	44518				
Key	94518				
Decrypted					

Once we add the ciphertext digits with the key digits we get this:

Ciphertext	88265	31456	21606	90988	76982
Key	88265	31416	11104	80868	66789
Decrypted	Verified	00040	10502	10120	10203
Ciphertext	36863	04307	31195	98687	94265
Key	36783	52386	23053	88185	93175
Decrypted	00180	52021	18142	01502	01190
Ciphertext	44518				
Key	94518				

Decrypted	50000				

00040 10502 10120 10203 00180 52021 18142 01502 01190 5

That gives us 00, 04, 01, 05, 02, 10, 12, 01, 02, 03, 00, 18, 05, 20, 21, 18, 14, 20, 15, 02, 01, 19, 05

The 00 means what follows is encoded
04, 01, 05 =DAE
02, 10, 12 =BJL
01, 02, 03 =ABC
00 =end of encoded
18, 05, 20, 21, 18, 14= RETURN
20, 15= TO
02, 01, 19, 05= BASE

If we look up DAE, BJL, & ABC in the codebook we see that it reads “Radio Compromise Abort”
So the full message is: “Radios compromise. Abort!, Return to base.”

If we use a letter based OTP key, it adds a few steps to encrypt. Basically we have to take the key, and convert it to numbers first, and then combine it with the number value from the text we want to encrypt, and then convert it back into letters. The same process is required on decryption. The only advantage is that it cuts the number of characters needed in half. “ABC” is 3 charcters, but the number representation is “010203”. That is twice the number of characters.

There are also methods of number based OTP's that use a conversion table that works in concert with a codebook to be a bit more efficient, and provides better number distribution, but that will not be covered in this handbook. More information can be found here:

One time pads

Conversion Tables

Security:
One time pads, and any notepads or scrap paper used to do the conversions and encryption/decryption should be destroyed immediatly after use. As the name implies, one time pads should only be used once. Reuse of a onetime pad makes it susceptible to cryptanalysis attack. Destruction should be witnessed and documented when possible.

XIII. Sensitive Materials

SOI's, COMPLANS, DRYAD sheets, Codebooks, and One Time Pads, can all compromise a groups operational security if they fall into enemy hands. Special care and consideration should be given to these sensitive materials and handling.

A) Whoever is responsible for sensitive material should be the only one allowed to distribute it or make any copies.
B) Ideally, each copy should have a unique identifying number, such as “1 of 15”, or “Copy #7”
C) There should be an accountability log of the sensitive material distribution. Anyone that receives or transfers sensitive material should sign and date the accountability log indicating the change, and the ID number of the material. This is essential for several reasons:

1) If sensitive material is captured by the enemy, checking the log will indicate who specifically needs to be notified, and have new sensitive materials issued.

2) If there is a sensitive material is discovered unsecured, the log can determine who was responsible for the breach.

3) Once sensitive material has expired, the log will help to insure that all copies are accounted for and destroyed, so that it does not compromise information some time in the future.

D) Sensitive materials should only be given to those who need it. Someone who doesn't operate a radio, doesn't need the radio authentication materials. An evaluation should be made to determine if sensitive material should even be allowed go into the field. SOI's, for example, should never have hard copies taken out on field operations, and relevant information that a field unit needs should be memorized. If something from an SOI needs to be written down, it should be done with the consent of a commanding officer, and treated as sensitive COMSEC material.
E) Sensitive material should be kept secure at ALL times!

1) If it is being carried on someones person, it should be on their first line (on stuff they are not likely to have to ditch, or leave behind in an emergency) in a tethered container or in a positively secured pocket that buckles or zips so that it can't accidentally fall out of a pocket. Additionally, all sensitive materials should be kept in one location, and that location needs to be known to others in the group, especially leaders, so if the person carrying it is disabled, injured, or killed, the sensitive material can be quickly retrieved and accounted for.

2) If the sensitive material is not on someones person, it should be kept in a secure locked container, preferably in a location that can be kept under observation. If anti-tamper seals are available, they are a good tool to help insure the integrity of the material.

F) If the security or integrity of sensitive material is suspect or compromised, cease using it immediately, and notify leadership, and anyone who may be affected.
G) There must be plans and capabilities to quickly destroy sensitive material if capture or overrun is imminent. If the plan includes burning materials, then there should be a container that will not let burning chunks blow out, there should be an accelerant, and multiple sources of ignition. If the plan is to use a shredder, it should be at least a cross cut shredder, and have multiple means of powering. This is also why it is important for units afield to carry only what is absolutely necessary. Printing sensitive materials small, on thin paper gives more options to quickly shred, burn, hide or eat, (yes, eat!) compromising materials.

XIV. Jamming

Jamming occurs when a radio receiver cannot receive a transmitted signal due to either the transmitted signal being blocked, or a competing stronger signal overwhelms the receiver so that the transmitted signal can not be heard.

Some jamming is unintentional. Faulty electronics, power transformers, or electric motors may create radio energy that can jam transmissions. Someone who accidentally presses on, or sits on their radio key button may also inadvertantly jam your radios. Additionally, if other people in the same area are using compatible radios on the same frequencies or channels as your group, that may be considered inadvertant jamming.

Intentional Jamming is the purposeful disruption of your radio signals. While it is technically illegal jam radio signals in the United States, even by Federal agencies, it is something that can be easily accomplished by technology.

It is important to distinguish interference from reception issues. If 2 radios are at a distance that is near exceeding their range, that can sometimes be mistaken for jamming. If no signal is heard, or it cuts out and drops out, it is probably a signal range issue. If instead there are voices, sounds, tones, music, repetitive or mechanical noises, or a quiet carrier, then it is jamming or inteference of some sort.

If your group regularly uses radios, it should have jamming/interference reports that should be filled out any time jamming or interference is encountered. These reports can be very useful for a groups intelligence efforts, and help mitigate any inadvertant jamming problems.

A jamming report should include:

1. Date and Time the interference was detected
2. Duration of the interference
3. Who detected the interference
4. What equipment were they using (radio, antenna, ect...)
5. Location at time of interference
6. Description of the interference

Over time, the information in a jamming report can help determine the source of the interference, and help guide decisions regarding radio and frequency use in the future.

Jamming reports should not be sent over air, unless crucial for an operation. If one must be sent, it MUST be fully encrypted. If an adversary has jamming capabilities, intercepting a jamming report will help them determine their own effectiveness, and allow them to adjust to be even more effective.

A blank example form is included in appendix C.

XV. Conclusion

While the amount of information may seem a little overwhelming to someone just starting out, it doesn't have to be implemented all at once. Start with getting a good equipment set up. It doesn't have to be expensive, just done properly. A cheap radio, mounted well with the proper accessories can be ten times more useful than a super expensive radio that is difficult to access and use. The next step is to start practicing good radio operating procedures. Use prowords. Use the NATO Phonetic alphabet, and modified number pronunciation properly. Keep transmissions short, and to the point.

Once the basics come naturally, and without effort, start implementing forms and reports. Run training exercises where the sending and receiving of reports are practiced. Then start adding in COMPLANS, and SOI's. Start simple, and work up to more comprehensive implementations.

Once that is solid, then add in the encryption, codebooks, and advanced authentications.

There is nothing magic about these procedures, and practice does make perfect.
Good communication can be a force multiplier, and conserves effort, so get started!

Romeo Bravo, Out!

XVI. Appendices

Appendix A:
Handheld Radio Types

This is just a brief introduction to the different types of radios.... whole books can be written on each category, I am just trying to keep it distilled to the basics.

Typically, in the U.S. we can categorize radios by the FCC licensing/ part that regulates the radio.

Category's:
Citizens Band Radio aka: CB: no license required, 40 channels around 27Mhz (am)... 4 watt output limit (12 watt SSB)
Pros: inexpensive, available at any truckstop in the U.S. Lots of accessories, The low frequency, and AM characteristics give it some of the longest range of handhelds in rural terrain. Some vehicle units also do SSB, which allows even longer ranges
Cons: efficient antennas tend to be on the long side for handhelds, and because they are ubiquitous, lots of potential for others to snoop on your comms

Cobra handheld CB radio

FRS/GMRS: The ubiquitous bubble pack radio, can be found at Wal-Mart, Radio Shack, Best-Buy, and many other places
FRS refers to the "family radio service", and GMRS refers to the "general mobile radio service".... most of the new radios include both FRS and GMRS frequencies, however there are slightly different specs and requirements to use the different radio services
FRS: no license required, limited to 1/2 watt from a permanently attached antenna. 462-467Mhz(fm)
GMRS: FCC License required... $85 for 5 years, good for all of your immediate family. GMRS shares some of the same frequencies as FRS, and when operated from a FRS/GMRS radio, has the same 1/2 watt, fixed antenna restrictions as FRS. When used on GMRS only equipment, GMRS is limited to 50 watts, and repeaters can also be used.
Pros: Small, ubiquitous, inexpensive
Cons: Limited range (1 mile at best despite what the label on the box says), and again, because they are ubiquitous, it is easy for others to snoop on your comms.
Some frequencies are not legal to use along the U.S. Canadian border.

The “privacy codes” many of these radios use do not add “channels”, but instead use a form of tone squelch. Realistically, they really don't add any privacy, since a radio set to the base channel, with no privacy code, will hear anything on that channel regardless of privacy code setting.

Motorola FRS/GMRS radio

Multi Use Radio Service aka MURS: No License required. Originally set up as a set of frequencies for drive way intercoms systems. Only FCC accepted Type 95 radios are legal for use on these 5 frequencies starting at 151mhz fm (Technically type 90 radios certified before 2002, with a 2 watt limit can also be used)
Pros: Not common, so some security through obscurity. Many drive way motion sensors also transmit on these frequencies, so you can use those motion sensors as intrusion detection, and not need another piece of hardware to monitor.

Cons: Only 5 channels, not a lot of gear choices

Marine VHF Radio: License required... Legally, only boat to boat, or boat to licensed land station allowed. Some folks do use marine VHF for backwoods comms, but it can be heavily monitored by the coast guard. And getting caught can mean fines and having your equipment confiscated.
156-162Mhz.
Pros: Lots of choices and availability
Cons: because generally not legal, can be difficult to test and practice with systems.
(I personally recommend staying from Marine VHF for team comms)

ICOM VHF Marine radio

Amateur Radio: License required, test is usually about $15, different levels of license, good for 10 years, renewal free. Many frequencies/bands/modes available
Anyone using the amateur bands must be licensed. FCC callsigns must be used regularly, no encryption allowed. For small team comms, the VHF, and UHF handhelds, and vehicle units excel. Handheld typically 1-5 watts, vehicle 50-100 watts.... limited to 1500 watts (but much over 100w is usually a waste of money and electricity)
Pros: Greatest variety of equipment available, also the most powerful and flexible
Cons: legal I.D.'s and a large self policing community make coded/encrypted comms difficult. Having your call tied to a searchable database means anyone that hears you can locate your mailing address.

Yaesu VX-6 & VX-170 Ham radios

Business band radio/Public safety: All requires FCC licensing, high variances in cost based on number of transmitters, frequencies, number of frequencies, region, ect. These radios are used in everything from hospitals to hotels, large warehouses, public safety departments, movie sets, taxi cabs, ect. While the most difficult to license, these radios have the largest variety of equipment and options available. Encryption is sometimes an option, as well as digital.
Pros: often heavy duty radios, with lots of choice.... digital or encryption can improve comsec
Cons: expensive, resource intensive to get started.

Baofeng Business band radio

Milsurp radios: You can find tons of military surplus radios on sites like Ebay... Generally these suck for modern team coms.
Pre SINGCARS radios are usually 30mhz-80mhz, which means you only have 5 frequencies on the 6m amateur band to legally use them (assuming you have an amateur license) PRC-6, PRC-8, PRC-9,

PRC-10, PRC-25, PRC-77 ect... These radios are heavy and limited for what they do. SINGCARS radios... if you find one that is functioning, you are still limited to the few 6m frequencies in SINGCARS single channel mode. The frequency hopping functions are not legal for frequencies you could legally use the radio for, and for the most part, civilian possession of the equipment required to generate, copy, and load the frequency hopping tables, is illegal (those are CCI: Controled Cryptographic Items)
In short... expensive, limited, and heavy. Not very good team radios

Other: ISM, SMR:
There are other categories of radios that fall under specific rule sets. ISM: Industrial, Scientific, Medical. SMR: Specialized Mobile Radio.
Typically radios in these classes do not require a license, and are limited to 1 watt. ISM has lots of "stuff" sharing its frequencies. WiFi, wireless security cameras, cordless phones, baby monitors, ect. A few companies have built dedicated radios that fall under the ISM band, notably the now defunct TriSquare eXRS radios, and Motorola DTR. Because there are few requirements for the type of transmissions in the ISM band, each mfg came up with their own format.... most radios are spread spectrum (kind of like frequency hopping), digital, and thus very hard to snoop on. The Nextel Direct Connect phones, while on the SMR band, are functionally like most ISM radio systems.
Pros: very secure
Cons: can be expensive, only work with equipment from same mfg.

NextTel I355 DirecTalk phone

Appendix B:
Training Forms

1. Dryad “Apple”
2. Dryad “Banana”
3. Codebook “Cherry”
5. OTP 901-904
6. OTP page of 20

For Training Use Only						UID:	APPLE			
Start DTG:					End DTG:					
Distribution:										
	ABCD	**EFG**	**HIJ**	**KL**	**MN**	**OPQ**	**RS**	**TUV**	**WX**	**YZ**
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
A	AUZM	KJE	WRY	CB	HT	PXD	QI	SFG	LO	VN
B	SABV	ILR	HQD	ZF	TJ	CYM	PE	UKO	XG	WN
C	SGRB	HAU	DWQ	LN	OI	TEK	YP	JZF	MV	XC
D	NYSO	QJK	MAV	RH	WT	ZXE	UP	IFL	BG	CD
E	GZHV	XMI	AJK	UQ	RS	YCE	PB	DLT	FO	WN
F	VTYJ	BRS	LMH	WD	ZI	QKX	AU	OGF	NE	PC
	ABCD	**EFG**	**HIJ**	**KL**	**MN**	**OPQ**	**RS**	**TUV**	**WX**	**YZ**
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
G	XSIJ	PGD	ZTL	RY	KE	BQV	OM	CNU	HF	AW
H	QAJU	VYR	ILF	MZ	WT	PBX	NO	DKC	SH	EG
I	JVPX	CQH	SIU	KE	WO	RML	AY	DGT	FZ	NB
J	LDSW	GBI	ECU	QH	YN	ROK	FP	JXV	ZA	TM
K	LGWI	UXZ	QRM	PT	YJ	SOV	FA	CBD	EK	NH
L	HGQE	JSY	CRN	BM	PO	DAU	KZ	FTL	IX	WV
	ABCD	**EFG**	**HIJ**	**KL**	**MN**	**OPQ**	**RS**	**TUV**	**WX**	**YZ**
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
M	ZTRP	BEH	GVQ	UI	KN	JDY	SM	WFA	OX	CL
N	RVAE	PWT	KCQ	OJ	IF	SZD	UG	MBH	YL	NX
O	CKBI	OEQ	HAL	GM	WU	DRS	YF	PVX	NZ	JT
P	PDTN	XVW	GHE	AL	UR	CYI	OZ	JSM	KQ	BF
Q	QEZB	CSH	LJX	YV	TW	RFI	KA	PUG	NO	DM
R	LIEZ	BNR	VFJ	YU	KH	OPM	DA	MCG	SQ	TX
	ABCD	**EFG**	**HIJ**	**KL**	**MN**	**OPQ**	**RS**	**TUV**	**WX**	**YZ**
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
S	HANP	TQE	FGB	SW	CY	VDU	ZK	JXI	OR	LM
T	XNZR	COI	FTG	AY	PB	KVS	DH	JQW	UM	LE
U	MCFR	YKZ	DBT	PS	EA	XIQ	WU	HLG	VN	OJ
V	BEYC	HUJ	XPL	IM	VQ	NKD	TW	GAR	OS	ZF
W	ZXWA	TED	LMJ	RU	SF	ONB	HP	IQK	YC	VG
X	IVBD	YSN	RPC	FW	KM	AOZ	JX	HLU	QG	ET
Y	SVXM	BDU	WTG	JN	ZO	HFQ	IA	PKL	CR	YE
Z	HXFB	NYP	DCU	MG	SE	OIW	VT	QRZ	LJ	AK

For Training Use Only						UID:	BANANA			
Start DTG:					End DTG:					
Distribution:										
	ABCD	**EFG**	**HIJ**	**KL**	**MN**	**OPQ**	**RS**	**TUV**	**WX**	**YZ**
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
A	ZPAQ	MVN	CFT	UD	JY	WKI	BR	ESH	XG	OL
B	KQTW	SLY	JCA	GB	PR	EZU	IF	VND	OM	XH
C	SCPK	NYF	QRL	AE	JW	XID	UT	GMZ	BV	OH
D	BXUH	SMW	KCO	EF	ZQ	DIR	LV	ATN	JG	PY
E	SFBU	YHI	ZJK	XO	DW	MAP	RQ	VGN	ET	CL
F	SQMP	FGN	YKU	RE	DB	JCA	VI	HLX	TW	OZ
	ABCD	**EFG**	**HIJ**	**KL**	**MN**	**OPQ**	**RS**	**TUV**	**WX**	**YZ**
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
G	BMJP	XRN	KGF	AQ	LU	TIW	VD	SOZ	CH	YE
H	SFJY	ECO	IUL	BQ	AN	HRW	VX	MDP	TK	GZ
I	PKDN	OUA	CJW	LH	MQ	YZI	SB	ETV	XF	RG
J	MNHY	OSB	ZIL	VR	XG	WCT	FD	UJP	EK	QA
K	CVHM	UPF	AQK	DY	EG	ZTO	WR	JBX	IN	LS
L	IFVO	TPR	ZCS	QM	UD	NHG	LX	BYJ	KE	AW
	ABCD	**EFG**	**HIJ**	**KL**	**MN**	**OPQ**	**RS**	**TUV**	**WX**	**YZ**
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
M	CVAG	MXI	ZUY	TH	ES	DKW	LJ	QFO	NB	PR
N	FCBT	LMA	URI	VZ	HK	POW	YJ	GES	ND	ZQ
O	CKZF	XHD	TJR	IP	UW	YML	GA	QNB	VS	OE
P	ZRIT	VKE	QMN	DL	UO	CAY	GF	BJP	WS	XH
Q	QONK	CFG	INM	JS	XU	HTL	AV	WYE	PB	RD
R	XRJD	LZI	CKH	WF	OT	QYN	EM	UAS	PV	GB
	ABCD	**EFG**	**HIJ**	**KL**	**MN**	**OPQ**	**RS**	**TUV**	**WX**	**YZ**
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
S	VCFI	KNJ	EBD	TM	AO	XZR	WS	HPU	QY	LG
T	NZQV	FEA	SKW	HJ	LC	UXM	GT	RBY	IO	PD
U	QYVX	ASC	GFN	RP	KD	ZEM	HW	UTO	BJ	IL
V	OUSA	WTJ	LXY	RB	VD	EIC	GN	HMQ	PK	ZF
W	JULN	YSX	ETV	QF	PK	CZH	MI	GWR	AO	BD
X	OMJA	YCK	PHG	US	BF	IQW	LN	RDZ	XT	EV
Y	LPIA	GOR	EMD	TK	UC	HBZ	VS	JYN	QX	WF
Z	MFWP	QZN	UVH	DO	IE	CBX	SA	YRT	KG	JL

Codebook:	CHERRY	Effective DTG:	
OPCODE	**NUMcode**	**Term(s)**	**Data to Follow**
ABC	000	Abort	
ADE	007	Address	
AEF	013	Advance	
AGH	019	Affirmative	
AIJ	028	Afternoon	
AKL	037	Aircraft (fixed wing)	2 digit qty
AMN	046	Aircraft (large unmanned)	2 digit qty
AOP	055	Aircraft (rotary winged)	2 digit qty
AQR	064	Aircraft (small unmanned)	2 digit qty
AST	073	Armed Men	2 digit qty or "00" plus 3rd digit for hundreds
AUV	082	Artillery	2 digit qty
AWX	091	Attack	
AYZ	109	Bearing (Magnetic)	3 digit compass bearing
BBD	118	Bearing (true)	3 digit compass bearing
BDF	125	Between	
BEG	127	Boat/Ship	2 digit qty
BFH	136	Border	
BGI	145	Building	
BHJ	154	Car	2 digit qty
BIK	163	Casualities	2 digit qty
BJL	172	Cave	
BKM	181	Certaintity	
BLN	190	Checkpoint	
BMO	209	Civilian	2 digit qty or "00" plus 3rd digit for hundreds
BNP	218	Clearing	
BOQ	227	Compromise	
BPR	232	Coordinate	
BQS	236	Creek	
BRT	245	Danger	
BSU	254	Day	
BTV	263	Distance	
BUW	272	Do Not Answer	
BVX	281	Dog	
BWY	290	Door	
BXZ	304	East	
BZA	313	Evening	
CAD	322	Execute	
CBE	331	Farm	
CCF	340	Fence	
CDG	349	Figures	Use "99" to indicate end of figures
CEH	359	Flash	
CFI	368	Forward this message to:	
CGJ	377	Frequency	7 digits: xxx.xxxxMhz
CHK	386	Friendly	
CIL	395	Gate	
CJM	401	Grid	6 8 or 10 digit grid should be predetermined
CKN	410	Harbor	
CLO	429	Hill	
CMP	438	Home Base	
CNQ	447	I see	
COR	451	Immediate	
CPS	456	Impossible	
CQT	465	Instruction	
CRU	474	Light Armor	2 digit qty

OPCODE	NUMcode	Term(s)	Data to Follow
CGX	483	Livestock	2 digit qty
CSV	492	Locate	
CTW	498	Location	
CUX	501	Machine guns	
CVY	510	Medevac	
CWZ	529	Message Readibility	
CXA	538	Morning	
CYB	547	Mountain	
CZC	556	Moving Away From	
DAE	562	Moving Towards	
DBF	565	My Location	
DCG	574	Negative	
DDH	583	Night	
DEI	592	Night Vision	
DFJ	608	North	
DGK	617	North East	
DHL	620	North West	
DIM	626	Observe (ed)	
DJN	635	of our locatiom	
DKO	644	Out Building	
DLP	653	Pistols	
DMQ	662	Possible	
DNR	671	Priority	
DOS	677	Probable	
DPT	680	Radio	
DQU	699	Rally Point	
DRV	700	Range	
DSW	719	Remain in place	
DTX	728	Return to base	
DUY	737	Rifles	
DVZ	746	River	
DWA	755	Road	
DXB	764	Routine	
DYC	773	Sattellite Dish	
EAE	782	Signal Strength	
EBF	785	Soldiers	2 digit qty
ECG	791	South	
EDH	800	South East	
EEI	819	South West	
EFJ	821	Street	
EGK	828	Sunrise	
EHL	837	Sunset	
EIM	846	Tanks	
EJN	855	Telephone	
EKO	864	Time	
ELP	873	Today	
EMQ	882	Tomorrow	
ENR	891	Train	
EOS	895	Train Tracks	
EPT	909	Transmit	
EQU	918	Travel	
ERV	927	Truck	2 digit qty
ESW	936	Unable to	
ETX	945	Unknown	
EUY	954	Unseen	

OPCODE	NUMcode	Term(s)	Data to Follow
EVZ	963	Valley	
EWA	972	We Are	
EXB	981	West	
EYC	990	Withdraw	
EZD	999	Within	

00901

88265 31416 11104 80868 66789
36783 52386 23053 88185 93175
94518 61094 29730 03669 09794
80266 26735 47249 85094 61967
24597 84354 29142 36645 10627
79456 71091 32395 36984 77902
51195 08089 58390 92642 57007
98555 90811 88925 08587 55604
84461 81143 61985 19704 30098
36421 42037 39103 43817 18912

DESTROY AFTER USE

00902

95650 72543 46505 09773 17559
13257 91436 05493 24492 40731
13138 66584 94864 39839 64641
32632 78906 44536 32884 68258
92590 64814 04922 41345 31826
35139 29113 83050 20693 24479
38394 98758 87755 78109 46328
42739 04040 24664 20575 82425
87901 46994 49964 62553 36595
76901 20279 78352 90077 11946

DESTROY AFTER USE

00903

90738 24783 36396 23003 54160
14132 09623 64075 85949 06759
29012 49776 60820 60306 73325
63068 33377 08454 10661 01936
02955 17801 50171 78875 56586
24295 28252 30112 79495 19095
95023 70687 76376 88242 39316
81445 99801 93994 97493 76070
47290 14876 25858 31594 11931
06241 63559 60288 52001 79414

DESTROY AFTER USE

00904

34743 00208 06412 96529 39238
98631 85315 55753 70472 69045
51981 93385 58606 44313 07557
20648 07454 43079 52774 67033
07946 86220 63707 45924 33983
14280 22311 80981 43947 30994
75371 02882 06729 77048 97408
29699 91778 71951 03458 37166
13279 28767 33201 54890 64521
26289 31870 90739 50305 23004

DESTROY AFTER USE

20 One Time Pads

25025 51061 00498 87190 39759 84779 94901 93909 75705 16467 08129 50803 77996 37833 71689 04447 62543 27466 66016 80066
63627 41886 33874 68703 28136 61603 77446 59659 51257 85234 45777 76102 79351 27073 00365 00163 05763 43331 28220 06671
97237 15975 88733 42472 72368 34519 11777 59628 53061 39012 40841 93889 07459 86447 80618 19539 97068 34036 00515 66046
15072 14043 38311 11731 46699 16877 56034 96547 95657 96444 14223 14502 59243 44396 44347 99362 48645 74275 76707 13280
13027 66491 24958 79537 15879 91819 60431 94580 70473 07193 56556 25824 17573 76875 60377 14051 83727 09988 65119 13983
18913 19709 93396 07961 45972 55376 70643 38466 69241 04741 70427 47929 99703 48884 03935 14380 44151 63413 05538 87298
73919 97081 74204 13159 65527 98952 63464 76734 50904 70329 12040 46000 50240 21199 92216 07013 80115 79968 75986 52586
70790 15709 78474 34455 94380 28608 04616 71298 26183 75679 04743 58436 90681 66707 47931 88858 59278 59449 80409 47805
20490 26730 13755 87609 74786 49364 37949 03230 91754 11626 41379 35394 19089 66899 52088 70378 75340 17426 68797 12345
41478 31021 00926 46559 80188 39186 46997 88288 82705 84132 71512 99703 19058 30888 69784 10210 86683 87584 87561 31263

03048 91467 61825 32599 26980 60487 79996 45623 07416 97621 94364 29687 37263 08650 41072 57933 88969 02322 39273 19319
21073 27188 93110 57858 79180 75497 76858 80783 51059 77702 57686 81001 75211 17610 06871 13128 61231 56160 43733 53253
75796 48452 19629 53391 27496 11948 89197 87723 49269 27475 37379 76521 69757 20632 29513 88583 70344 87483 96626 97104
34340 25286 36193 61437 21299 83637 76733 29199 43787 75681 05900 38208 53045 52431 27995 85477 63717 47835 17780 58543
83350 21862 21644 30313 13127 41072 01161 17683 87386 92194 26281 93567 01548 56883 93446 99862 70065 98854 24820 80351
68357 86071 78429 99613 68316 66006 65431 22710 60423 12989 52125 54248 81168 10360 37409 33468 89080 38785 58176 33599
65722 75935 02224 09152 29208 49765 72979 78499 63392 88868 25934 54351 80181 70870 47318 47813 58243 24831 19407 81347
11405 00791 52365 66069 51836 55247 44636 76135 16499 09327 84667 94186 66039 66072 77192 44641 14577 87015 65722 53315
69124 42302 54037 78612 55906 22143 37103 00753 41685 82441 71288 40497 84099 50895 70741 62528 50728 29961 59573 55241
03306 18435 50638 20326 43928 84102 35035 03643 04644 00282 37770 08896 81517 26166 06296 89489 46810 51862 86726 40717

24883 19547 38877 17068 06886 83158 98396 42124 24381 60536 12465 28409 79637 25290 08905 91932 85447 84319 36190 34354
62615 30069 89750 50731 84091 51397 98964 16693 69273 88728 00113 97943 62075 51854 70380 05408 91972 49784 72047 09684
40955 14122 45150 46595 72564 25609 38282 62263 64166 78196 64865 03120 18078 84113 57987 46967 01083 50877 75522 48286
49967 08642 68191 63028 39008 30070 57817 59548 53640 68558 58606 37399 70182 72106 10191 78616 12904 28369 20718 62478
46151 32738 95899 00821 62932 75348 80206 88282 39285 85103 91950 14540 79074 23012 15386 48088 27754 77511 06947 91216
69806 50221 02203 90959 04590 19600 47044 33956 91983 83008 07396 90138 72503 94590 95648 68060 75813 19399 64355 59984
04370 43927 22176 52248 33442 38998 35635 40044 07715 98361 82158 34816 51158 82716 45800 08658 34776 31081 26079 79111
51495 13167 22920 47867 67239 89515 30541 33216 26277 15972 27914 57170 00086 51478 51583 85668 02103 14425 10290 46050
46577 23255 12565 66765 28750 23069 96895 24651 92772 94207 98463 27903 07582 49623 54433 61233 65265 00517 42399 19157
29269 62725 97288 63747 81976 72184 52137 05752 00948 42813 69548 90461 70606 15569 68352 59959 33259 90616 19871 87725

56141 27825 83561 23725 02926 79000 89369 10503 34923 99081 19843 61179 55636 32728 84811 75697 80757 96350 11332 86434
64319 89043 51239 08968 95318 65926 85557 18931 58255 22816 17734 39122 44434 88934 83259 24453 24718 41291 09375 66012
35575 93176 18554 56061 55834 07503 18366 26036 93205 50620 07854 55028 17309 57438 72132 83857 38878 73354 02336 70369
86270 07018 62113 34299 71672 81207 35969 60366 17693 55413 25436 88049 45570 64601 44912 35671 08085 36308 52193 96942
45570 58237 67541 58147 35862 47873 45246 84633 63287 57874 66775 62709 75328 37663 31849 52790 03904 53259 76061 50124
27244 59821 16467 59346 83587 27329 44329 31017 42252 81395 41137 78004 97350 30785 74348 95762 45530 67545 56105 48924
78570 66960 62000 55014 21630 42345 19081 09931 07347 91440 12306 06547 12347 26459 55690 85023 45017 97246 37143 74527
36155 89827 94163 36012 52572 63736 96713 64017 90375 56094 64744 00123 92169 15358 57532 87796 34467 75542 84448 35259
74125 30823 05642 10919 54567 51004 73912 42107 84615 85796 91886 32777 02992 98079 19866 65684 72326 87031 49263 97684
94870 30683 05542 43273 38702 51479 30936 34921 65200 60435 43952 26885 63663 69379 11351 57425 76212 67727 56216 77761

93207 36286 05074 58074 47490 60867 67800 53283 95955 57266 44840 24569 36778 75639 01032 43804 79062 28353 43207 71760
74758 58956 50431 09671 78375 17955 23958 70642 23678 04483 47960 81081 30650 53863 77708 84004 19821 95656 52514 49050
89455 58047 58334 20821 50135 88305 60708 38097 13039 27860 62341 53147 20215 53656 09310 69808 78784 78294 98519 03667
89112 32039 54274 83139 14025 53520 16803 51781 40101 99475 70031 86759 59464 01089 51288 45612 62947 54499 22300 16777
11302 30582 46036 62036 36259 14864 60967 30605 91476 47937 48266 98540 31599 80350 67841 82274 89528 88325 69750 29395
65121 60248 37901 63957 32454 55783 66964 83050 61586 62224 79133 76811 56420 36877 18455 36923 51231 40292 06337 24845
40436 91364 20670 92303 31604 35569 15413 12108 17518 20545 40542 96751 75325 88872 92172 26262 61507 86367 56745 23032
48494 86232 85476 42337 76078 69296 56162 77737 58755 69664 09318 97917 85153 80379 35278 77664 57015 55015 93733 38765
28595 01362 83367 89076 30248 16778 85855 39204 57483 68882 71911 29537 07336 90524 73706 38477 76537 12491 87123 93974
79922 25994 13028 08516 85906 67850 53075 24810 49262 40429 85979 44319 28111 98985 34009 88281 91267 65422 52638 92131

Appendix C:
Blank Forms

1. One Time Pad Worksheet
2. Jamming/Interference Report
3. SITREP
4. SPOT Report (SALUTE)
5. 9-Line Air Medevac Request
6. 9-Line Ground Medevac Request
7. DRYAD
8. Blank Codebook
9. Blank 10-cycle SOI

1. One Time Pad worksheet

One Time Pad Worksheet			Destroy after use!!!		
To encrypt, work top to bottom, to decrypt, work bottom to top					
Unnncrypted	*This block should match key to verify proper key used.*				
Key					
Ciphertext					
Unnncrypted					
Key					
Ciphertext					
Unnncrypted					
Key					
Ciphertext					
Unnncrypted					
Key					
Ciphertext					
Unnncrypted					
Key					
Ciphertext					

code	A	B	C	D	E	F	G	H	I	J	K	L	M	N
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14
O	P	Q	R	S	T	U	V	W	X	Y	Z	?	!	_
15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
0	1	2	3	4	5	6	7	8	9	+	-	*	/	=
30	31	32	33	34	35	36	37	38	39	40	41	42	43	44

2. Jamming/Interference Report:

Jam/ Interference Report		DTG:	Unit:
1	Interference	(1)	
	Describe the intereference		
2	Location	(2)	
3	Start of interference	(3)	
4	End of interference	(4)	
5	Effects	(5)	
	What impact did the interference have on operations		
6	Frequency	(6)	
7	Equipment being used	(7)	
8	Narrative (8)		
9	Authentication	(9)	

Instructions:
Date and Time the report was made
Unit making report
Line 1: Describe the interference: Static? Tones? Music? Speach? Digital noise? Ect..
Line 2: The location that the detecting unit was when interference was detected. Use whatever common format used by the unit. Lat/Long, UTM, MRGS, or location descriptions.
Line 3: What time was the interference first detected
Line 4: What time did the interference stop, or the equipment being affected be turned off, or to another frequency
Line 5: What impact did the interference have on operations? I.E. Had to change channel, or could not communicate with another unit, ect...
Line 6: What frequency (or channel) was the interference detected
Line 7: What radio or equipment was being affected? (Make, model, brand, antenna, ect...)
Line 8: Narrative: Describe in a few normal sentences what happened
Line 9: Authentication: Who/what/how was this report verified as legitimate, and not a fake report from an inposter? I.E. was it authenticated by a radio IFF procedure and by whom?

3. SITREP

	SITREP	DTG:	Unit:
1	Current Location	(1)	
2	Activities of previous 24 hours	(2)	
3	Planned Activity for next 24 hours		
4	Casualties	(4)	
5	Ammo & Equipment Status	(5)	
6	Enemy contacts/KIA	(6)	
7	Intel (7)		
8	Notes (8)		
	In Notes, include Time it would take to go on the move, any compromise of COMSEC materials and sensitive items, ect...		
9	Authentication	(9)	

4. Spot Report (SALUTE)

Spot Report		DTG:	Unit:
1	Size of the enemy unit	(1)	
2	Activity of the enemy Unit	(2)	
	What were they doing when observed, how were they carrying themselves.		
3	Location of Enemy Unit	(3)	
4	Uniforms worn/Insignia	(4)	
5	Equipment being carried	(5)	
	What weapons, vehicles, and electronics were visible? How were they carried? What was in use?		
6	Narrative (6)		
7	Authentication	(7)	

5. COMPLAN

	COMPLAN		Effective Dates/times:		
	Plan Name:				
	Link	**Primary**	**Alternate**	**Contingency**	**Emergency**
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
	Use a second line if any links contain multiple Alternate/Contingency/Emergency methods				
	Scheduled Contacts:				
	Date (or recurring)	**Link**	**Primary Time**	**Alternate Time**	**Contingency Time**
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
	If a scheduled contact is at regular interval, use that instead of date i.e.: Every day, or every Sunday, etc. If it is an interval then specify the start, such as every third day starting 13Jan.				
	Mission Codewords:				
	Codeword	**Meaning**			
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					

6. Air Medevac 9-Line Request

	Air-Medevac 9-Line request			DTG:	Unit:
1	Location (UTM/Lat-Long)			(1)	
2	Callsign & Frequency			(2)	
3	Number of Patients/ Precedence			(3)	
	A- Urgent (less than 2 hours to save life)			B- Surgical Urgent	
	C- Priority		D- Routine	E-Convience	
4	Special Equipment Required			(4)	
	A- None	B- Hoist	C- Extraction	D-Ventilator	E- Jungle penetrator
5	Number of patients by Typr			(5)	
	L- Litter			A- Ambulatory (walking)	
6	Security at LZ			(6)	
	N- No enemy			E- Enemy in area	
	P- Possible enemy			X- Armed escort required	
7	LZ Marking Method			(7)	
	A-Panels	B- Pyro	C- Smoke	D- None	E- Other
8	Nationality/Status			(8)	
	A- Friendly Military	B- Friendly Civilian		C- Non Allied Military	
	D- Non Allied Civilian			E- Enemy POW	
9	Terrain/Obstacles			(9)	

Notes:

7. Ground Medevac 9-Line Request

	Ground Medevac Request			DTG:	Unit:
1	Location (UTM/Lat-Long)			(1)	
2	Callsign & Frequency			(2)	
3	Number of Patients/ Precedence			(3)	
	A- Urgent (less than 2 hours to save life)			B- Surgical Urgent	
	C- Priority		D- Routine	E-Convience	
4	Special Equipment Required			(4)	
	A- None	B- Hoist	C- Extraction	D-Ventilator	E- Jungle penetrator
5	Number of patients by Typr			(5)	
	L- Litter			A- Ambulatory (walking)	
6	Security at LZ			(6)	
	N- No enemy			E- Enemy in area	
	P- Possible enemy			X- Armed escort required	
7	LZ Marking Method			(7)	
	A-Panels	B- Pyro	C- Smoke	D- None	E- Other
8	Direction of recommended approach			(8)	
9	Terrain/Obstacles			(9)	

Notes:

For Official Use Only						UID:				
Start DTG:					End DTG:					
Distribution:										
	ABCD	**EFG**	**HIJ**	**KL**	**MN**	**OPQ**	**RS**	**TUV**	**WX**	**YZ**
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
A										
B										
C										
D										
E										
F										
	ABCD	**EFG**	**HIJ**	**KL**	**MN**	**OPQ**	**RS**	**TUV**	**WX**	**YZ**
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
G										
H										
I										
J										
K										
L										
	ABCD	**EFG**	**HIJ**	**KL**	**MN**	**OPQ**	**RS**	**TUV**	**WX**	**YZ**
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
M										
N										
O										
P										
Q										
R										
	ABCD	**EFG**	**HIJ**	**KL**	**MN**	**OPQ**	**RS**	**TUV**	**WX**	**YZ**
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
S										
T										
U										
V										
W										
X										
Y										
Z										

Codebook:		Effective DTG:	
OPCODE	**NUMcode**	**Term(s)**	**Data to Follow**
ABC	000		
ADE	007		
AEF	013		
AGH	019		
AIJ	028		
AKL	037		
AMN	046		
AOP	055		
AQR	064		
AST	073		
AUV	082		
AWX	091		
AYZ	109		
BBD	118		
BDF	125		
BEG	127		
BFH	136		
BGI	145		
BHJ	154		
BIK	163		
BJL	172		
BKM	181		
BLN	190		
BMO	209		
BNP	218		
BOQ	227		
BPR	232		
BQS	236		
BRT	245		
BSU	254		
BTV	263		
BUW	272		
BVX	281		
BWY	290		
BXZ	304		
BZA	313		
CAD	322		
CBE	331		
CCF	340		
CDG	349		
CEH	359		
CFI	368		
CGJ	377		
CHK	386		
CIL	395		
CJM	401		
CKN	410		
CLO	429		
CMP	438		
CNQ	447		
COR	451		
CPS	456		
CQT	465		
CRU	474		

OPCODE	NUMcode		
CGX	483		
CSV	492		
CTW	498		
CUX	501		
CVY	510		
CWZ	529		
CXA	538		
CYB	547		
CZC	556		
DAE	562		
DBF	565		
DCG	574		
DDH	583		
DEI	592		
DFJ	608		
DGK	617		
DHL	620		
DIM	626		
DJN	635		
DKO	644		
DLP	653		
DMQ	662		
DNR	671		
DOS	677		
DPT	680		
DQU	699		
DRV	700		
DSW	719		
DTX	728		
DUY	737		
DVZ	746		
DWA	755		
DXB	764		
DYC	773		
EAE	782		
EBF	785		
ECG	791		
EDH	800		
EEI	819		
EFJ	821		
EGK	828		
EHL	837		
EIM	846		
EJN	855		
EKO	864		
ELP	873		
EMQ	882		
ENR	891		
EOS	895		
EPT	909		
EQU	918		
ERV	927		
ESW	936		
ETX	945		
EUY	954		

OPCODE	NUMcode		
EVZ	963		
EWA	972		
EXB	981		
EYC	990		
EZD	999		

10 cycle SOI		Page 1	
Codename:	Start DTG:	End DTG:	Copy:

	ID		Put unit designators in column on left, put dates in row across the top, put callsigns/codenames in grid.								
	Unit/Dates										
1											
2											
3											
4											
5											
6											
7											
8											
9											
10											
11											
12											

Net Descriptions

Name	Description

Name	Description

	Net Frequency Assignments		Put net names in column on left, put dates in row across the top, put frequencies/channels in grid.								
	Net/Date										
1											
2											
3											
4											
5											
6											
7											
8											
9											
10											
11											
12											

IFF			Put dates in row across the top, put IFF in grid.								
Date:											
Radio Word											
DRYAD Sheet											
Challenge											
Response											
Duress											
Running											
Number											
Night											
Vehicle											
Vehicle/nite											
Concealed											

10 cycle SOI

Codename:	Start DTG:	End DTG:	Copy:

Com Codewords	Put dates in row across the top, put codewords in grid.									
Date:										
Goto Primary										
Goto Alt										
Goto Contingency										
Goto Guard										
Radio compromised										
Wiping radio										

Sound/Visual/Pyro signals

Name	Meaning

Name	Meaning

Phone Tagging

Color	Line

Appendix D: Index

Alphabetical Index

Appendix E:
Further reading links

FM 24-12 Communications in a come as you are war

FM 6 Signal Soldiers Guide

FM 21-60 Visual Signals

FM 24-18 Radio Operator

FM 31-20 ch 10 SF Commo

FM 6-02 Signal Support to Operations

UK Radio operations

Emergency destruction of documents

Partisan Tactical Communications on Mountain Guerrilla.com

Intra Team tactical communications on Mountain Guerrilla

Manual One Time Pads

Conversion Tables for One Time Pads

Wikipedia article on DRYAD

AMRRON: American Redoubt Radio Operators Network

3% Signal Corps /Sparks 31

Dan Morgans comms website