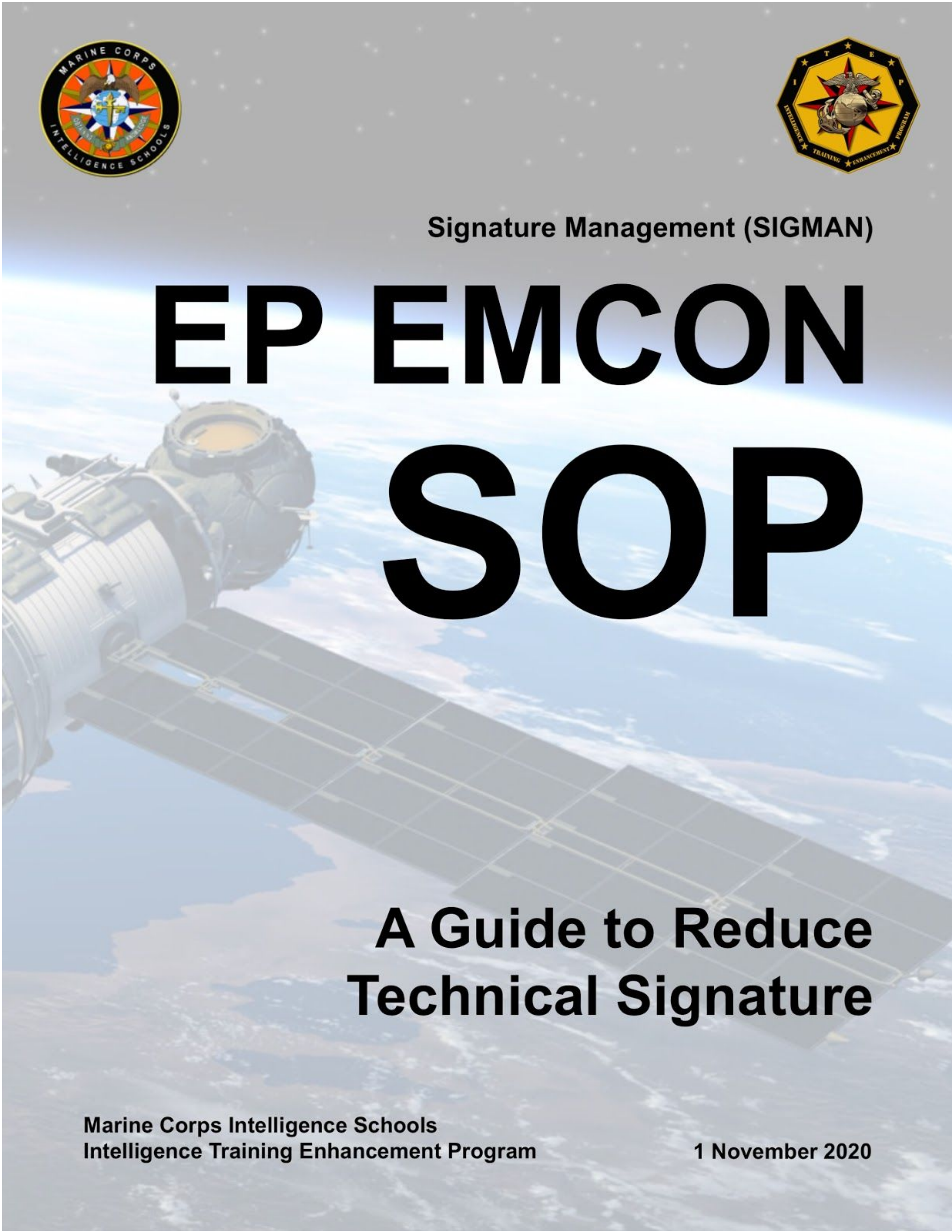


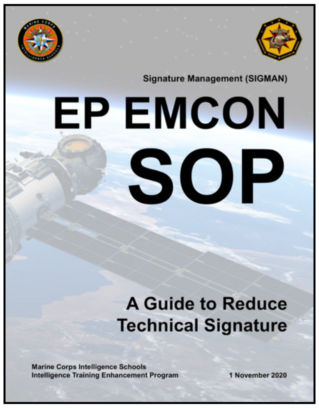
Signature Management (SIGMAN)

EP EMCON SOP

A Guide to Reduce Technical Signature

Marine Corps Intelligence Schools
Intelligence Training Enhancement Program

1 November 2020

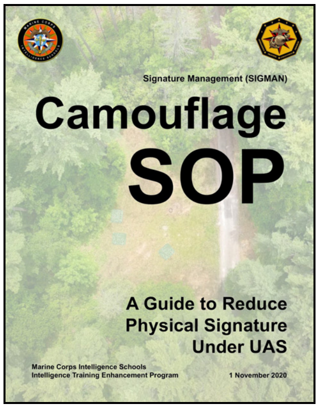


Signature Management (SIGMAN)

EP EMCON SOP

A Guide to Reduce Technical Signature

Marine Corps Intelligence Schools
Intelligence Training Enhancement Program
1 November 2020

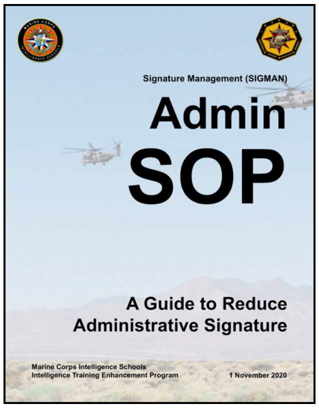


Signature Management (SIGMAN)

Camouflage SOP

A Guide to Reduce Physical Signature Under UAS

Marine Corps Intelligence Schools
Intelligence Training Enhancement Program
1 November 2020



Signature Management (SIGMAN)

Admin SOP

A Guide to Reduce Administrative Signature

Marine Corps Intelligence Schools
Intelligence Training Enhancement Program
1 November 2020

SIGMAN EP EMCON SOP:
A Guide to Reduce Technical Signature

Contributors:
Brian Alcorn
Garrett Boyce
Brian Walsh
Tom Haluska
Evan Kolodziejczak
Kent Johnson
Nick Pugh
Philip Burtt-Henderson
Nolan Sheahan
Brian Kerg

Reviewers: Nicolas Dilan, Doug McDonough, Kyle Wilmouth, Steven Grubbs, Jonathan George, Christian Andros, Joseph Livi, and Jason Sampson

Editor: **Brendan McBreen**
1 November 2020

Marine Corps Intelligence Schools (MCIS)
Intelligence Training Enhancement Program (ITEP)
2088 Regulus Avenue
Virginia Beach, Virginia 23461-2099

Purpose

Purpose

To REDUCE the technical signature of the infantry battalion.
To REDUCE electromagnetic emissions IOT AVOID being located and targeted by the adversary.

Process

1. UNDERSTAND adversary electromagnetic support (ES) collections.
2. UNDERSTAND friendly electromagnetic emissions signatures.
3. REDUCE friendly electromagnetic emissions:
   ESTABLISH standard EP EMCON operating procedures.

Premise

"To be detected is to be targeted is to be killed."

- *Marine Corps Operating Concept*, 2016
- *Marine Corps Concept of Employment for Signature Management*, 2019

Your radio can kill you. Our communications equipment squawks continuously and our adversaries can hear it. This is our challenge: Electromagnetic warfare (EW) is changing ground combat and we now need to change how we fight.

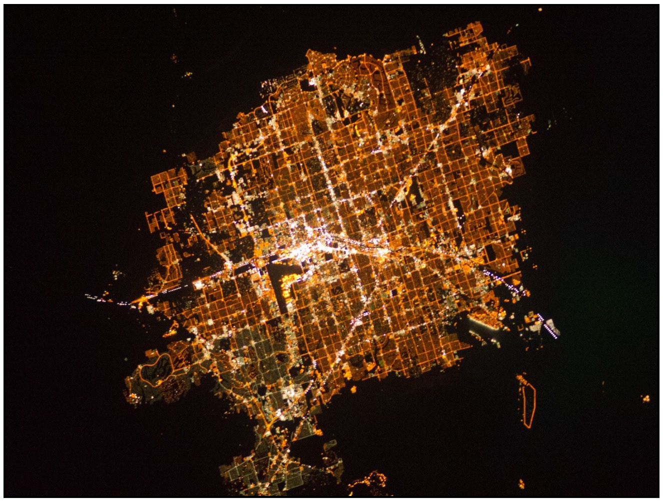
The threat has changed. Our adversaries can now find us with sophisticated electromagnetic reconnaissance—EW satellites, aircraft, UAS, and ground collections capabilities—and then target us with long-range precision fires.

Operations have changed. Our new concepts envision Marines seizing advanced bases under the arc of enemy missile fires. And even during traditional operations, Marines will face the threat of advanced EW collections cueing UAS and triggering long-range missile, rocket and artillery fires.

After two decades without a direct EW collection and detection threat, we are complacent about communications discipline, overly dependent on SATCOM, and addicted to excessive bandwidth and continuous talk. Every day, we acquire new equipment that *increases* our signature and ignores the

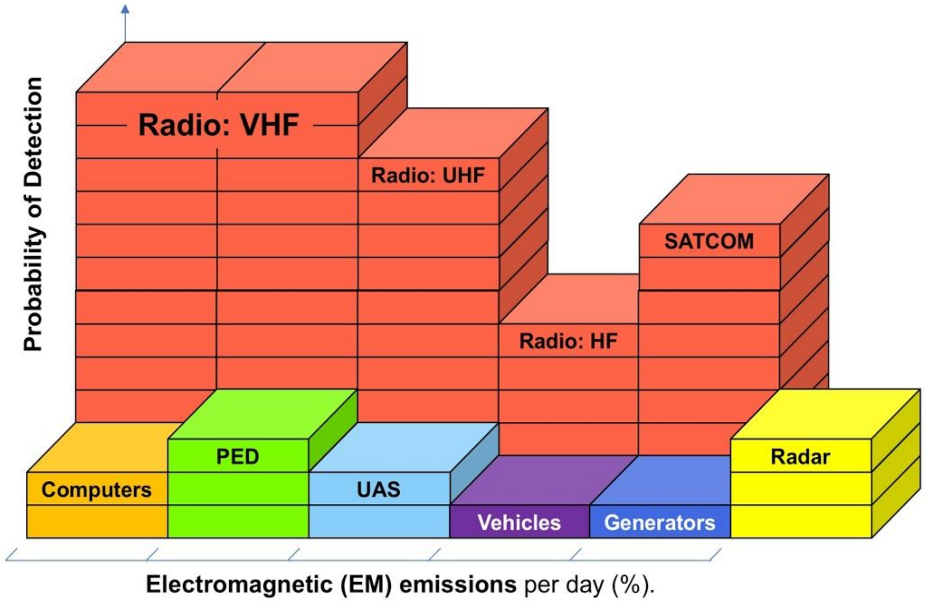
EW threat. Some of our systems are constantly emitting, which makes us much more vulnerable to enemy direction finding. Our assumptions of technological superiority are dangerously outdated.

Marine Corps communications equipment is especially bright and loud. To a sophisticated adversary, our units—especially our command posts in the field—look like Las Vegas from space.



Las Vegas, Nevada, from outer space.
Source: International Space Station, 2010.

Marine CP in Iraq.
Source: National Archives, 2003.



The vast majority of our infantry battalion emissions—notionally represented in the above illustration—are voice and data radio calls: VHF, UHF, HF, and SATCOM. Each of the different-colored stacks is a different signal. The height of each stack represents the probability of detection, which is a function of the number of daily calls multiplied by signal strength, propagation pattern, and waveform.

Our radio emissions, shown in red, are most likely to be detected by the enemy. But other communications equipment—computers, portable electronic devices (PED), and UAS—as well as our non-communications equipment—vehicles, generators, and radars—emit signals also. Any effort to reduce our signature, however, must address radio first.

The real signature management challenge for the Marine Corps is NOT the nets of the infantry battalion, but the signals emitted by our support units, aviation squadrons, and command posts.

Marines will soon operate in an electromagnetic environment under near-continuous adversary EW observation and possible attack. This requires new skills and precise communications procedures.

Our *Warfighting* doctrine expects competent leaders, enabled by commander's intent and mutual trust, to communicate implicitly without transmitting lengthy orders, reports, or requests. Operating in the chaos of combat with partial information is one of our strengths—*decentralization*. The goal of this SOP is to reduce our electromagnetic emissions. ***Well-trained units communicate less.***

Scope of this SOP

This SOP addresses only those non-technical **electromagnetic protection (EP)** measures known as **emission control (EMCON)**—steps to reduce emissions IOT avoid detection by the enemy.

The *Marine Corps Concept of Employment for Signature Management*, 2019, defines three types of signatures: physical, technical, and administrative. This SOP addresses ONLY technical signatures.

How do our adversaries collect SIGINT on our radios and ELINT on our non-communications devices? How do we know what enemy electromagnetic support (ES) assets are collecting on us? How do we reduce our signals? How do we communicate effectively?

The scope of this SOP is the infantry battalion—in the field, NOT in garrison. In urban, woodland, jungle, mountain, and desert environments. Supported, possibly, by civilian power, internet, and mobile telephone systems. Most of this SOP is focused on radios, but electromagnetic security and signature control (SIGCON) of non-communications equipment is also addressed.

Organization of this SOP

Chapter 1 is the actual **SOP** of EP EMCON procedures. Using these example templates, each unit should write their own SOP. Chapter 2 is **How To**, a collection of EP EMCON guidelines. Chapter 3 is **Train**, a guide to training units on EP EMCON. Chapter 4 is **Understand**, with sources that explain adversary and friendly capabilities. Chapter 5 is a **Reference** of additional materials.

If you do not already understand electromagnetic warfare (EW) terms and functions—especially the difference between EA, EP, and ES—read section 4.6. 'UNDERSTAND U.S. EW Doctrine' first. Use section 5.1 'EP EMCON Glossary' to clarify terms.

This *EMCON SOP* is a collective effort. If you can improve this document, send us your ideas or join the online GoogleDoc.

Brendan McBreen
bbmcbreen@gmail.com
1 November 2020

Information in this SOP

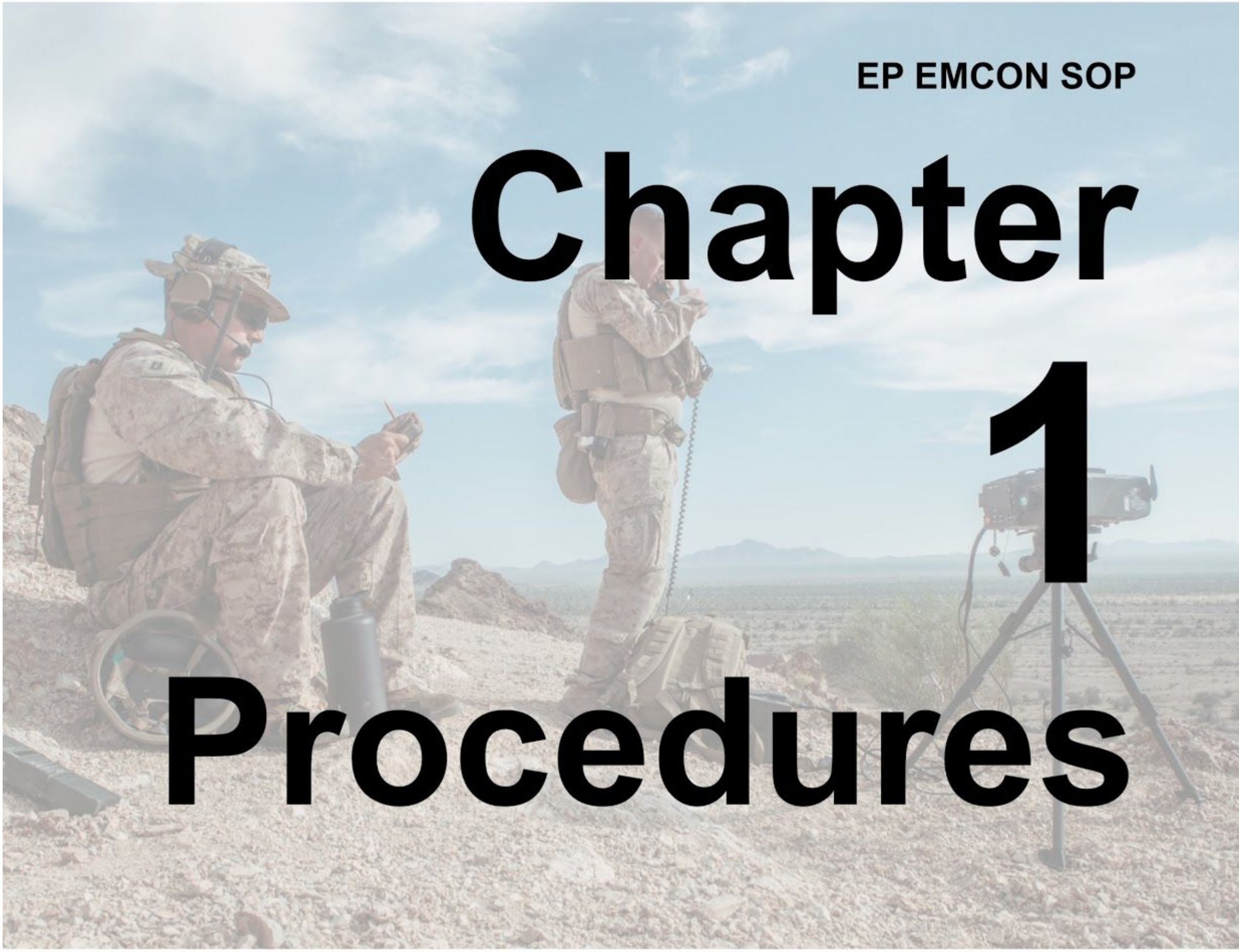
This *EP EMCON SOP* is UNCLASSIFIED and intended for wide distribution to all Marines. It contains **NO** technical information. **NO** countries are mentioned. **NO** specific adversary equipment or capabilities are discussed. When friendly equipment is discussed, **NO** specific vulnerabilities are mentioned that might imply adversary capability.

Out of Scope

EP EMCON is a small slice of a complex problem. The following EW areas are NOT addressed:

- Friendly electromagnetic protection (EP) measures that are technical in nature, communications security (COMSEC)—crypto equipment—and transmissions security (TRANSEC)—frequency modification technology—are OUT of scope. Evaluating, acquiring, or modifying comm equipment is OUT of scope.
- Friendly electromagnetic support (ES)—searching, intercepting, identifying, and locating adversary EM emissions—is OUT of scope. Electromagnetic reconnaissance to confirm IPB on the adversary's electromagnetic order of battle (EOB) is OUT of scope.
- Friendly electromagnetic attack (EA)—intrusion, jamming, or probing adversary emitters—is OUT of scope. Electromagnetic attack control authority (EACA) is OUT of scope.
- Friendly SIGINT is out of scope. Radio Battalion taskings—and SIGINT operational tasking authority (SOTA)—are OUT of scope. Sensing, targeting, warning, jamming, and exploiting adversary signals is OUT of scope. Conducting ELINT, COMINT, and FISINT on the adversary is OUT of scope.
- Friendly information operations are OUT of scope. The MEF Information Group (MIG)—its organization, units, and processes—is OUT of scope. Military deception (MILDEC) ISO EW is OUT of scope. The new electromagnetic warfare support team (EWST) is OUT of scope.
- Friendly communications planning and frequency management is OUT of scope. Electromagnetic compatibility (EMC)—making sure radios are compatible—is OUT of scope. Hazards of electromagnetic radiation to fuels, ordnance, and personnel (HERF, HERO, and HERP) are OUT of scope.
- Electromagnetic environmental effects (E3)—the impact of the natural environment on friendly comms—is OUT of scope. EM hardening—EP actions to shield equipment against EA—is OUT of scope.
- Friendly frequency deconfliction and electromagnetic spectrum (EMS) management is OUT of scope. The JRFL and other EMS control measures are OUT of scope. Electromagnetic battle management (EMBM) is OUT of scope.
- Computer network management and network security is OUT of scope.
- International treaties and HN laws and regulations that address frequency allocations for radio, TV, mobile phones, and wireless internet are OUT of scope.
- Adversary electromagnetic attacks (EA) to jam U.S. emitters are OUT of scope. Adversary computer attacks—denial of service, network penetration, and emplaced malware—are OUT of scope. Adversary missile, rocket, and artillery attacks on U.S. emitters are OUT of scope.
- Adversary attacks on satellites, or jamming or spoofing satellite signals are OUT of scope.

Table of Contents



EP EMCON SOP

Chapter 1 Procedures

In this Chapter

- EP EMCON SOPs
- EP EMCON Responsibilities

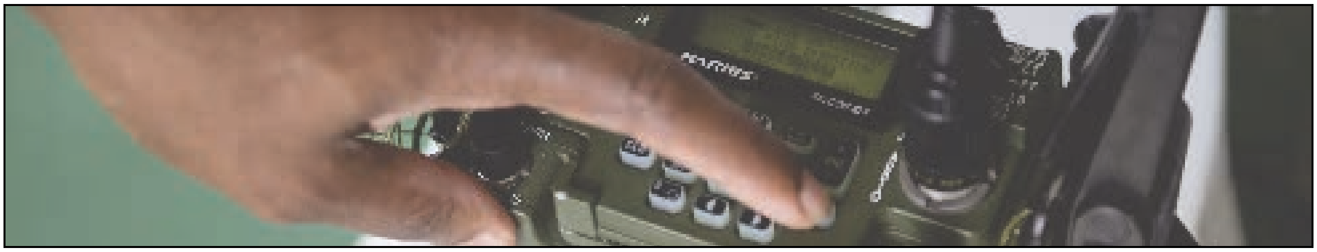
Marine Corps Intelligence Schools
Intelligence Training Enhancement Program

SIGMAN EP EMCON SOP:
Chapter 1: Procedures

Marine Corps Intelligence Schools (MCIS)
Intelligence Training Enhancement Program (ITEP)

EP EMCON Options SOP

Purpose. To REDUCE electromagnetic emissions IOT AVOID being located and targeted.



Process for commanders. ADJUST EMCON for each mission, each day, for each situation.

EMCON	Guidelines
1 **RADIO ROUTINE**	**Transmissions:** RADIO ROUTINE. Any and **all radio calls** are authorized. [1] **Emitters:** Any and all comm emitters are authorized. All non-comm emitters are authorized: PED, vehicles, generators, radars. **Adversary:** IMPROBABLE (45%) ES collections or EA. REMOTE (5%) threat of receiving fire (IDF). **Scenario:** Garrison or friendly country. Training, evaluations, and administrative movements. **Note:** Even during training, leaders should limit radio calls to mission-critical information.
2 **RADIO ESSENTIAL**	**Transmissions:** RADIO ESSENTIAL. **Mission-critical** and emergency **radio calls ONLY**. [2] [3] **Emitters:** Any and all comm emitters are authorized. All non-comm emitters are authorized. Emitters are SHUT OFF except when in use. Constant emitters (BFT / JBC-P, ALE / 3G ALE HF, and ANW2) are restricted or OFF. Non-essential PED is OFF. **Adversary:** PROBABLE (80%) ES collections or EA. IMPROBABLE (45%) threat of effective IDF. [4] **Scenario:** Friendly, neutral, or hostile country. Contingency operations or pre-hostilities. **Note: EMCON 2 is the desired standard for operations.**
3 **RADIO SILENCE**	**Transmissions:** RADIO SILENCE: **NO voice radio calls**. Text and burst data only. HF ideal. Wire. **Emitters:** Selected bands are restricted, receive-only, or OFF. Constant emitters (BFT / JBC-P, ALE / 3G ALE HF, and ANW2) are OFF. Unencrypted UHF black gear is OFF. Non-comm emitters are restricted or OFF. Passive receivers—GPS, GBS—are restricted or OFF. Voice CFF / CAS are OFF. **Adversary:** HIGHLY PROBABLE (95%) ES collections or EA. PROBABLE (80%) threat of IDF. **Scenario:** Conflict. Enemy is collecting and targeting. Precision IDF weapons are in range. **Note:** Some units, executing fast-moving operations without key equipment, cannot rely on chat.
4 **BLACKOUT**	**Transmissions:** BLACKOUT. **NO radio calls**—voice or data—**are authorized**. **Emitters:** ALL emitters are OFF. ALL radios, ALL PED are OFF. Batteries are OUT, generator power is off. ALL non-comm emitters are OFF. Vehicles are OFF. Lights are OFF. **Adversary:** NEARLY CERTAIN (99%) ES collections or EA. HIGHLY PROBABLE (95%) threat of IDF. **Scenario:** Conflict. Enemy is collecting and targeting. Precision IDF weapons are activated. **Note:** When missiles are inbound, units avoid being located, but cannot operate long at EMCON 4.

Notes: 1. Specific EMCON actions taken under each option are defined by each unit for each operation. Restrictions on calls, nets, bands, and equipment are clearly defined by unit SOP. 2. Unit PACE plans specify alternate comms. 3. For emergency radio calls, leaders violate EMCON for safety, enemy engagement, or CASEVAC. 4. Adversary descriptions are ICD 203 language on the *likelihood* of enemy action. An actual attack or EA may *not* yet have occurred.

1. SET EMCON for each operation.

   SPECIFY EMCON measures for each recurring radio call and each type of emitter.
   ADD an EMCOM matrix to every execution checklist for every mission in your SOP.

   ADJUST EMCON to reflect the adversary electromagnetic support collections capabilities in your AO. Adjacent units will have different EMCON for different missions.

   ENFORCE EMCON measures to protect your unit. CONTROL equipment.

2. CHANGE EMCON during an operation to reflect changes in the situation.
   If the adversary already knows where you are, the risk of emitting may be *less* important.

3. TRANSMIT EMCON directives on the radio IAW MCRP 3-30B.1 *Brevity: Multi-Service TTPs for Brevity Codes*, 28 May 2020.

ZIPLIP brevity code transmission	Notes
"2-3. ZIPLIP, OVER."	Shut up. ZIPLIP is a reminder to "limit transmissions to critical information only."

SNOOZE brevity code transmission	Notes
"All stations. As briefed, SNOOZE from sixteen-hundred to twenty-two hundred, OVER."	Set an EMCON block from 1600–2200. SNOOZE is "initiate EMCON procedures."

ALARM brevity code transmission	Notes
"2-3, 2-2. ALARM. Send log status report, OVER."	Wake up. ALARM is a directive to "terminate EMCON procedures."

Other EMCON brevity codes—CLAM, HUSH, and PUPPIES—are specific to NATO.

SILENCE proword transmission	Notes
"2-3, 2-2. SILENCE. BREAK. 2-7, 2-2. SAY AGAIN, ALL AFTER 'in the treeline,' OVER."	A directive to "cease transmission immediately." SILENCE is cancelled by SILENCE LIFTED.

SILENCE and SILENCE LIFTED are NOT EMCON prowords.

SILENCE directs one or more units to stay off the net so as not to interfere with another transmission. See ATP 6-02.53 *Techniques for Tactical Radio Operations*, 13 Feb 2020.

An emergency transmission—one operator transmitting one call for one emergency purpose—does not break EMCON. All other users remain in EMCON status.

Notes

Commanders balance the risk of detection—and unit vulnerability—against mission requirements. EMCON is a command decision. The CO authorizes emitters. The CO restricts emitters. EMCON is NOT ON or OFF. All units implement various EMCON measures, to different levels, at all times.

Extreme restrictions negatively affect mission accomplishment. Some EMCON measures reduce situational awareness, lessen control of subordinate units, and increase safety risks.

EMCON decisions are local. Each battalion, in each AO, faces different threats and has different mission requirements. A blanket MEF-level EMCON plan must be flexible.

All co-located units, organic, attached, and DS, must be controlled. Units with specialized equipment—UAS, GSP, RadBn, allies—implement their own procedures IAW the CO's direction.

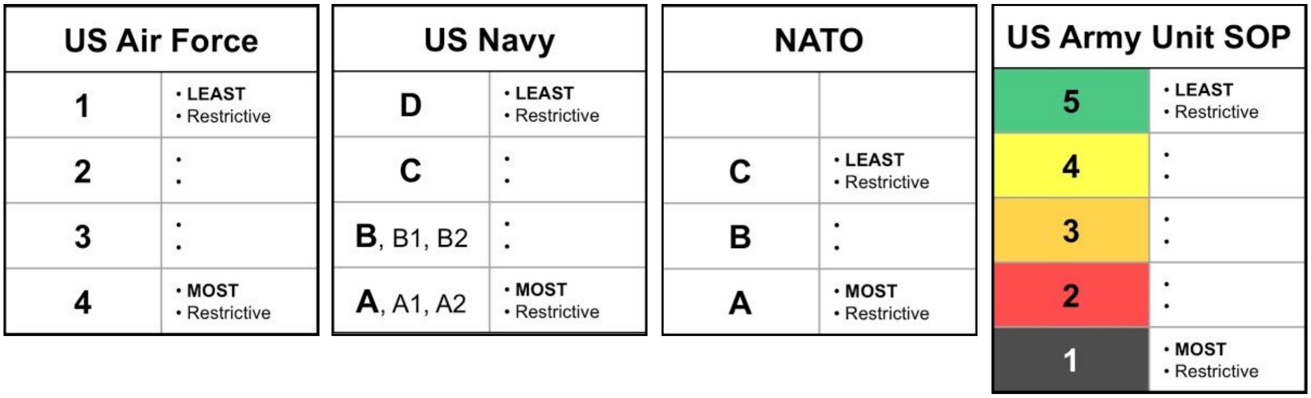
Battle captains must be alert to sudden, unscheduled EMCON changes and unexpected radio silence from higher, adjacent, subordinate, or supporting units.

EMCON (emission control) is "The selective and controlled use of electromagnetic, acoustic, or other emitters to optimize command and control capabilities while minimizing, for operations security: a. Detection by enemy sensors, b. Mutual interference among friendly systems, and/or c. enemy interference with the ability to execute a military deception plan." (*DOD Dictionary*, 1 Jun 2020)

EMCON Best Practices

There is no standard DOD EMCON protocol. There is no Marine Corps standard. Multiple standards are contradictory, labelled haphazardly by numbers or letters—with multiple conflicting categories and color codes—and either increasing or decreasing levels of restrictions.

EMCON Protocols defined by service doctrine



US Air Force	
1	• **LEAST** • Restrictive
2	:
3	:
4	• **MOST** • Restrictive

US Navy	
D	• **LEAST** • Restrictive
C	:
B, B1, B2	:
A, A1, A2	• **MOST** • Restrictive

NATO	
C	• **LEAST** • Restrictive
B	:
A	• **MOST** • Restrictive

US Army Unit SOP	
5	• **LEAST** • Restrictive
4	:
3	:
2	:
1	• **MOST** • Restrictive

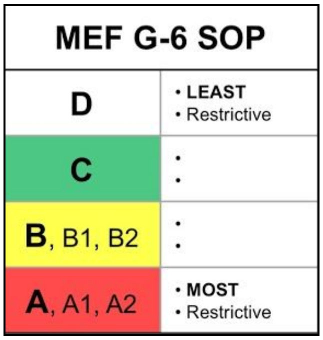
Sources: AFTTP 3-1. NWDC 3-51.1. ATP-1(D) V1. *EW Operator's Handbook*.

The US Air Force EMCON protocol is set by the AFTTP 3-1 series of manuals. Each aircraft type, in its own separate 3-1 manual, has the flexibility to set EMCON actions for each mission profile.

The US Navy EMCON protocol is set by NWDC 3-51.1. A separate NW OPTASK EW directs EMCON procedures across the fleet. US Navy **River City** procedures use a different model.

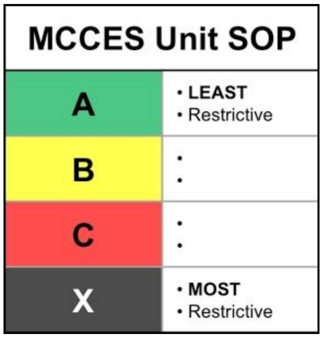
The NATO EMCON protocol is set by ATP-1(D), V1*,* which is near-aligned with the US Navy. The US Army directs units to set their own EMCON protocols. *The Electronic Warfare Operator's Handbook*, 1 May 2019, includes a unit example from the National Training Center (NTC).

EMCON Protocols defined by Marine Corps SOPs



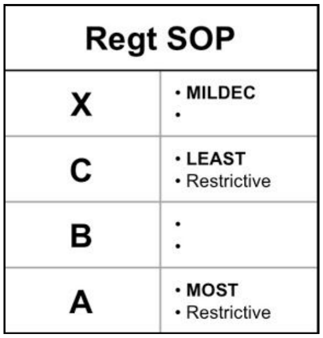
MEF G-6 SOP	
D	• LEAST • Restrictive
🟩 C	• •
🟨 B, B1, B2	• •
🟥 A, A1, A2	• MOST • Restrictive

Sources: *G-6 PACE Matrix*.



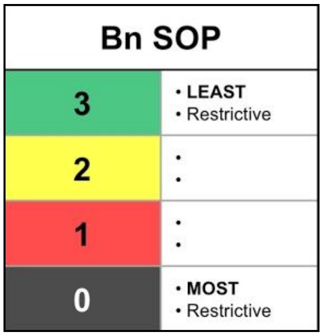
MCCES Unit SOP	
🟩 A	• LEAST • Restrictive
🟨 B	• •
🟥 C	• •
⬛ X	• MOST • Restrictive

C2 Planner's Guide.



Regt SOP	
X	• MILDEC •
C	• LEAST • Restrictive
B	• •
A	• MOST • Restrictive

Spectrum Warfare SOP.



Bn SOP	
🟩 3	• LEAST • Restrictive
🟨 2	• •
🟥 1	• •
⬛ 0	• MOST • Restrictive

Battalion Combat SOP.

A MEF EMCON SOP, specifically the *G-6 PACE Matri*x, 15 May 2020, is aligned with the overly complex and ship-specific US Navy protocol. Some paragraphs refer to "Level 1" through "Level 5."

The MCCES CTB *C2 Planner's Guide*, 18 Apr 2019, includes an example from a unit SOP. A regiment establishes a "deliberate emissions" level in their *Spectrum Warfare SOP*, 6 Feb 2019. An artillery battalion defines EMCON 0 as "radio silence," which is far from absolute.

Some of these schemes are better than others. **Less categories** is best. **Colors** are good. **Numbers**, increasing from least restrictive to most restrictive, are intuitive and better-understood.

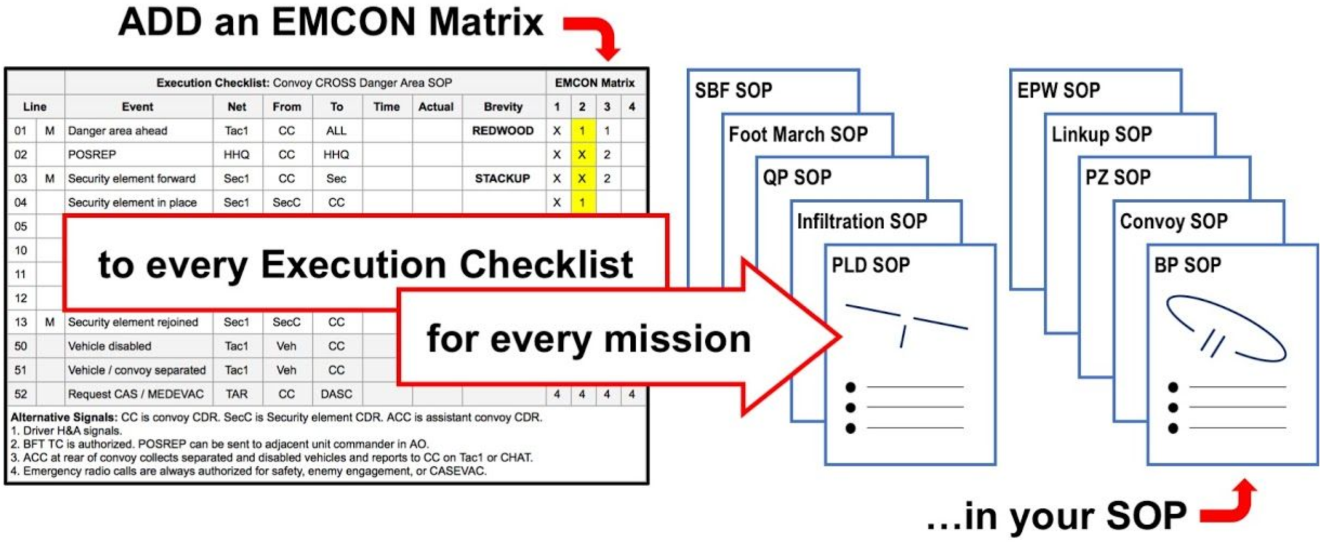
The **most important** aspect, however, is not the levels, but how the EMCON implementation guidance is applied at each level. Using this criteria, the Air Force model is the most flexible. Under a general service-wide guideline, each type of unit applies specific EMCON actions for each specific mission under different enemy situations. This is the model implemented by this SOP.

Contributors: **BBM**, 1 Nov 2020.

Procedures

EP EMCON Matrix SOP

Purpose. To REDUCE the number of radio calls IOT AVOID being located and targeted.



ADD an EMCON Matrix

to every Execution Checklist

for every mission

...in your SOP

		Execution Checklist: Convoy CROSS Danger Area SOP							**EMCON Matrix**			
Line		**Event**	**Net**	**From**	**To**	**Time**	**Actual**	**Brevity**	**1**	**2**	**3**	**4**
01	M	Danger area ahead	Tac1	CC	ALL			**REDWOOD**	X	1	1	
02		POSREP	HHQ	CC	HHQ				X	X	2	
03	M	Security element forward	Sec1	CC	Sec			**STACKUP**	X	X	2	
04		Security element in place	Sec1	SecC	CC				X	1		
05												
10												
11												
12												
13	M	Security element rejoined	Sec1	SecC	CC							
50		Vehicle disabled	Tac1	Veh	CC							
51		Vehicle / convoy separated	Tac1	Veh	CC							
52		Request CAS / MEDEVAC	TAR	CC	DASC				4	4	4	4

Alternative Signals: CC is convoy CDR. SecC is Security element CDR. ACC is assistant convoy CDR.
1. Driver H&A signals.
2. BFT TC is authorized. POSREP can be sent to adjacent unit commander in AO.
3. ACC at rear of convoy collects separated and disabled vehicles and reports to CC on Tac1 or CHAT.
4. Emergency radio calls are always authorized for safety, enemy engagement, or CASEVAC.

Process

1. CREATE an **Execution Checklist** for every tactical **mission** in your **SOP**.

   LIST the **radio calls** needed to execute the SOP. LIST the contingency radio calls.

   IDENTIFY mandatory, **mission-critical** calls: 'M' is 'mandatory.'

   For most units, this is a new level of detailed communications planning.

2. ADD an **EMCON Matrix** to every **Execution Checklist** for every **mission** in your **SOP**.

   Every tactical evolution must be executed at multiple EMCON levels.

   DEFINE the **authorized radio calls** at each EMCON level: 'X' is 'as required.'

   NOTE the **alternative signals** when radio calls are NOT authorized.

   EMCON 2 is the desired standard for operations.

Example Execution Checklist with **EMCON Matrix** for one specific SOP

		Execution Checklist: Convoy CROSS Danger Area SOP							**EMCON Matrix**			
Line		**Event**	**Net**	**From**	**To**	**Time**	**Actual**	**Brevity**	**1**	**2**	**3**	**4**
01	M	Danger area	Tac1(VHF)	CC	ALL			**REDWOOD**	X	1	1	
02		POSREP	Cmd1(HF)	CC	HHQ				X	X	2	
03	M	Security element forward	Sec(VHF)	CC	Sec			**STACKUP**	X	X	2	
04		Security element in place	Sec(VHF)	SecC	CC				X	1		
05		Security vehicle directives	Sec(VHF)	SecC	SecV				X			
10		First vehicle through area	Tac1(VHF)	Veh	CC				X			
11		Each vehicle through area	Tac1(VHF)	EachV	CC				X			
12		Last vehicle through area	Tac1(VHF)	ACC	CC				X	X	2	
13	M	Security element rejoined	Sec(VHF)	SecC	CC			**STACKBACK**	X	X	2	
50		Vehicle disabled	Tac1(VHF)	Veh	CC				X	3	3	
51		Vehicle / convoy separated	Tac1(VHF)	Veh	CC				X	3	3	
52		Request CAS / MEDEVAC	TAR(UHF)	CC	DASC				4	4	4	4

Alternative Signals: CC is convoy CDR. SecC is Security element CDR. ACC is assistant convoy CDR.
1. Driver H&A signals.
2. JBC-P/BFT TC is authorized. POSREP can be sent to adjacent unit commander in AO by VHF FH voice.
3. ACC at rear of convoy collects separated and disabled vehicles and reports to CC on Tac1 or CHAT.
4. Emergency radio calls on UHF or VHF FH are always authorized for safety, enemy engagement, or CASEVAC.

3. BRIEF EMCON during every mission brief.

BRIEF the **execution checklist** with the **EMCON matrix** of authorized radio calls.

Notes

PLAN each **EMCON matrix** with the S-6. READ the S-6 **list of authorized emitters** for guidance on net priorities, vulnerabilities, and options. See EP EMCON List of Authorized Emitters SOP.

ALIGN your **EMCON matrix** with the S-6 PACE plan and the S-6 CEOI special instructions (SPINS). There is no single “EMCON Plan.” There are combat plans, each adjusted for EW threats.

Leaders need to plan simple flexible operations that require less radio calls: less control measures, less “on-order” tasks, and less reporting requirements. This is NOT an S-6 task.

Well-executed tactical evolutions are a result of training. Well-trained units need less comm. A written SOP, with dozens of execution checklists and EMCON matrices, is useless unless it is trained and understood by Marines.

Execution Checklist Best Practices

LIST each **event** in rough chronological order. List the minimum number of events that need **radio calls** to execute the SOP. Some internal events do NOT need radio calls. NUMBER events in separate decades to indicate phases.

IDENTIFY **mandatory**, mission-critical radio calls: ‘M’ is ‘mandatory’ and ‘X’ is ‘as required.’ LIST contingency radio calls—safety, enemy engagement, or CASEVAC—in gray at the bottom of the execution checklist.

ASSIGN who is responsible for each radio call: **Net**, **From**, and **To**. Note the technology of each net: ‘TAD (UHF)’ or ‘Tac1 (VHF FH).’

Time only scheduled events: ‘H-15.’ Do NOT estimate timing for every event on a rigid schedule. **Actual** time is filled in during the mission.

GROUP **Brevity** codes by theme. Aviation calls can be girls’ names and ground calls can be football teams. Some events do NOT need a brevity code.

For ease of memorization, use the *same standard brevity code* for the *same event* across all missions, particularly contingencies. No one remembers fifty brevity codes. Aviators do this well.

AVOID assigning a single overall theme to each separate mission: ‘TRAP codes are all BASEBALL teams.’ Under this model, the standard event, ‘Security element in position,’ would have a *different* brevity code for each different mission. This is NOT a best practice.

ENSURE no brevity code duplicates existing control measures or callsigns. SYNCHRONIZE brevity codes with higher, subordinate, adjacent, and supporting units to avoid misunderstandings.

The best brevity code is a two-syllable word, with the accent the first syllable, that starts with a hard consonant sound: “KICKBACK” is better than “CAESAR” or “DEBRIS.” Avoid four-syllable words.

TITLE and DATE the execution checklist for a specific mission in one AO against a specific adversary.

During operations, do NOT state a brevity code unless it is TRUE. To inquire on the status of a given event, use the line number: “SAY AGAIN status of line eleven, OVER.”

Contributors: **BBM**, ELK, 1 Nov 2020.

Template: **Execution Checklist with EMCON Matrix**

		Execution Checklist:						**Date:**	**EMCON Matrix**			
Line		**Event**	**Net**	**From**	**To**	**Time**	**Actual**	**Brevity**	**1**	**2**	**3**	**4**
01												
02												
03												
04												
05												
11												
12												
13												
14												
15												
51												
52												
53												
54												

Alternative Signals:

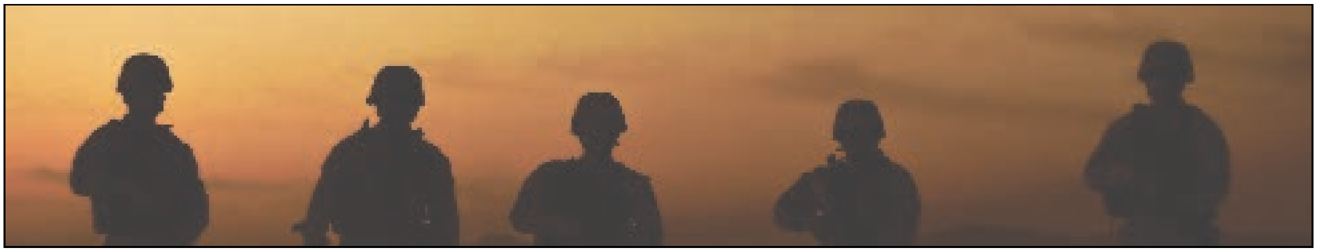
1.
2.
3.
4.
5.

Notes: Typeface is Arial narrow, black. Table header text is bold. Table borders are 0.75 point, 25% gray lines. Table headers and contingency rows are 5% gray fill. First column: Number events in separate decades to indicate phases. Contingencies are listed at the bottom in gray. Second column: 'M' is 'mandatory,' 'X' is 'as required.' Fourth column: Note the technology of each net: 'TAD(UHF).' Seventh column: Time only scheduled events: 'H-15.' Eighth column: Actual time is filled in during the mission. EMCON Matrix columns: 'X' is 'as required,' an authorized radio call. EMCON 2 is the desired standard for operations. Number each footnote and explain EMCON restrictions and alternative signals in the bottom section. Title and date the execution checklist for a specific mission in one AO against a specific adversary.

Procedures

EP EMCON List of Authorized Emitters SOP

Purpose. To REDUCE electromagnetic emissions IOT AVOID being located and targeted.



Process for the S-6

1. CREATE a **List of Authorized Emitters—**for a specific mission in one AO against a specific adversary. *The S-6 CONTROLS emissions by controlling categories of emitters:*

   "VHF FH Voice is OFF at EMCON 3."

   "All PED must be OFF, with batteries OUT, at EMCON 2."

   "Vehicle intercoms are SHUT OFF at EMCON 3."

   LIST only the equipment used by that specific mission. Because each operation is different—different equipment availability, task organization, distances, retrans, and comm requirements—there is *never* one standard **List of Authorized Emitters**.

   When specific **frequencies** and **power** levels are noted, the **List of Authorized Emitters** may require classification.

   Your **List of Authorized Emitters** is a planning tool for commanders. It should answer the question: "What radio nets are less vulnerable to adversary collections in our AO?"

2. PLAN communications in detail with mission commanders.

   REVIEW the commander's **Execution Checklist** with **EMCON Matrix**.
   See EP ECMON Matrix SOP.

   COMPARE the authorized radio calls listed in the commander's **Execution Checklist** to your S-6 **List of Authorized Emitters**, PACE Plan, and CEOI special instructions (SPINS).

   Provide guidance on net priorities, net vulnerabilities, and comm options.

   TRAIN commanders on EMCON:
   "The safest nets are HF chat > HF voice > VHF FH > VHF SC > UHF uncovered."

Example List of Authorized Emitters for one specific mission

	List of Authorized Emitters: Convoy Operations		**EMCON**			
	Equipment	**Freq/Power**	**1**	**2**	**3**	**4**
1	Radio: VHF FH Voice	All / 10W	ON 1	ON 1	Off 2	Off 2
2	Radio: PRC-150 HF ALE CHAT	All	ON + Voice	ON + Voice	ON	Off
3	Radio: PRC-117G UHF MUOS CHAT	All	ON 3	ON 3	ON 3	Off 3
4	Radio: UHF (PRC-113, PRC-117)	All	ON	ON	OFF 4	OFF 4
5	Radio: SATCOM	-	ON	ON	Off 2	Off 2
6	Computers (non-communications)	NA	ON	ON	Off	Off
7	PED	-	ON	Off GPS Auth	Off GPS Auth	Off GPS Auth
8	UAS	-	ON	ON	Off	Off
9	Vehicle: JBC-P / BFT / TC	-	ON 5	ON 5	Off 2	Off 2
10	Vehicle: C-IED / CREW UHF	-	As needed	As needed	As needed	Off
11	Vehicle: Intercom	-	ON	ON	Off 6	Off

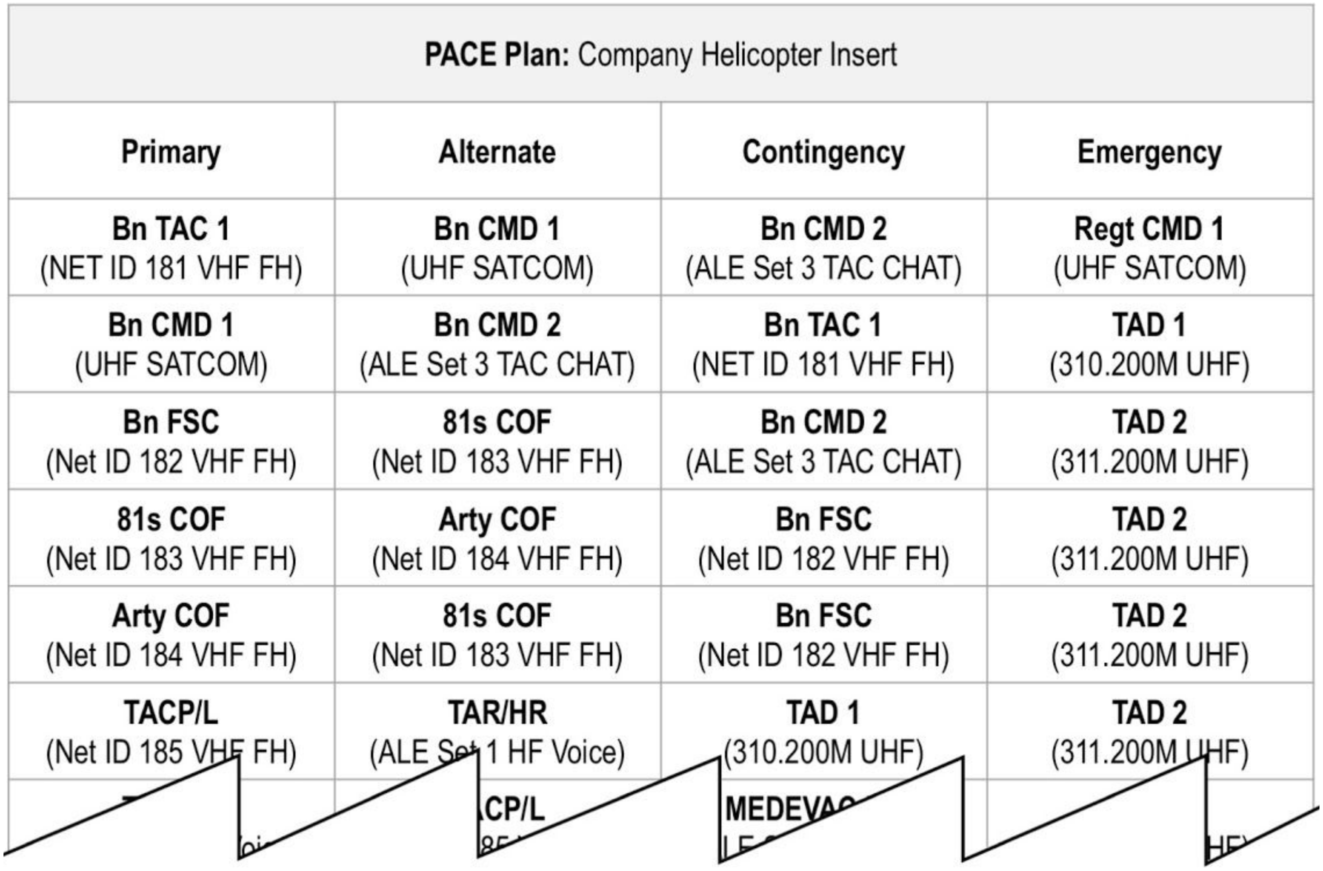
Notes: 1. Minimize calls in the assembly area. RP departure is particularly noisy and vulnerable. Restrict power to 10W.
2. NO voice at EMCON 3. Emergency calls are authorized only for safety, enemy contact, or CASEVAC.
3. All POSREPs are MUOS CHAT, except at EMCON 4. SEND only mission-essential reports.
4. NO voice at EMCON 3. Vulnerable UHF for emergency air coordination only: CAS, MEDEVAC.
5. JBC-P/BFT position reporting is Off. TC authorized to send text.
6. NO voice at EMCON 3. Convoy CDR can authorize intercom for specific elements, like security, for specific times.

3. CREATE a **PACE Plan** that addresses both: (1) adversary EA jamming, and (2) EP EMCON restrictions. Alternative comms should use alternative technology—***a list of four different VHF nets if NOT a PACE plan.***

   “The primary, alternate, contingency, and emergency (PACE) communications plan is a communication plan for a specific mission or task, **not a specific unit**.” ATP 6-02.53 *Techniques for Tactical Radio Operations*, 13 Feb 2020.

   Because each operation is different—different equipment availability, task organization, distances, retrans, and comm requirements—there is *never* one standard **PACE Plan**. For most units, this is a new level of detailed communications planning.

Example PACE Plan for one specific mission



PACE Plan: Company Helicopter Insert			
Primary	**Alternate**	**Contingency**	**Emergency**
Bn TAC 1 (NET ID 181 VHF FH)	**Bn CMD 1** (UHF SATCOM)	**Bn CMD 2** (ALE Set 3 TAC CHAT)	**Regt CMD 1** (UHF SATCOM)
Bn CMD 1 (UHF SATCOM)	**Bn CMD 2** (ALE Set 3 TAC CHAT)	**Bn TAC 1** (NET ID 181 VHF FH)	**TAD 1** (310.200M UHF)
Bn FSC (Net ID 182 VHF FH)	**81s COF** (Net ID 183 VHF FH)	**Bn CMD 2** (ALE Set 3 TAC CHAT)	**TAD 2** (311.200M UHF)
81s COF (Net ID 183 VHF FH)	**Arty COF** (Net ID 184 VHF FH)	**Bn FSC** (Net ID 182 VHF FH)	**TAD 2** (311.200M UHF)
Arty COF (Net ID 184 VHF FH)	**81s COF** (Net ID 183 VHF FH)	**Bn FSC** (Net ID 182 VHF FH)	**TAD 2** (311.200M UHF)
TACP/L (Net ID 185 VHF FH)	**TAR/HR** (ALE Set 1 HF Voice)	**TAD 1** (310.200M UHF)	**TAD 2** (311.200M UHF)
T oic	**ACP/L** 85	**MEDEVAC** LE	HF

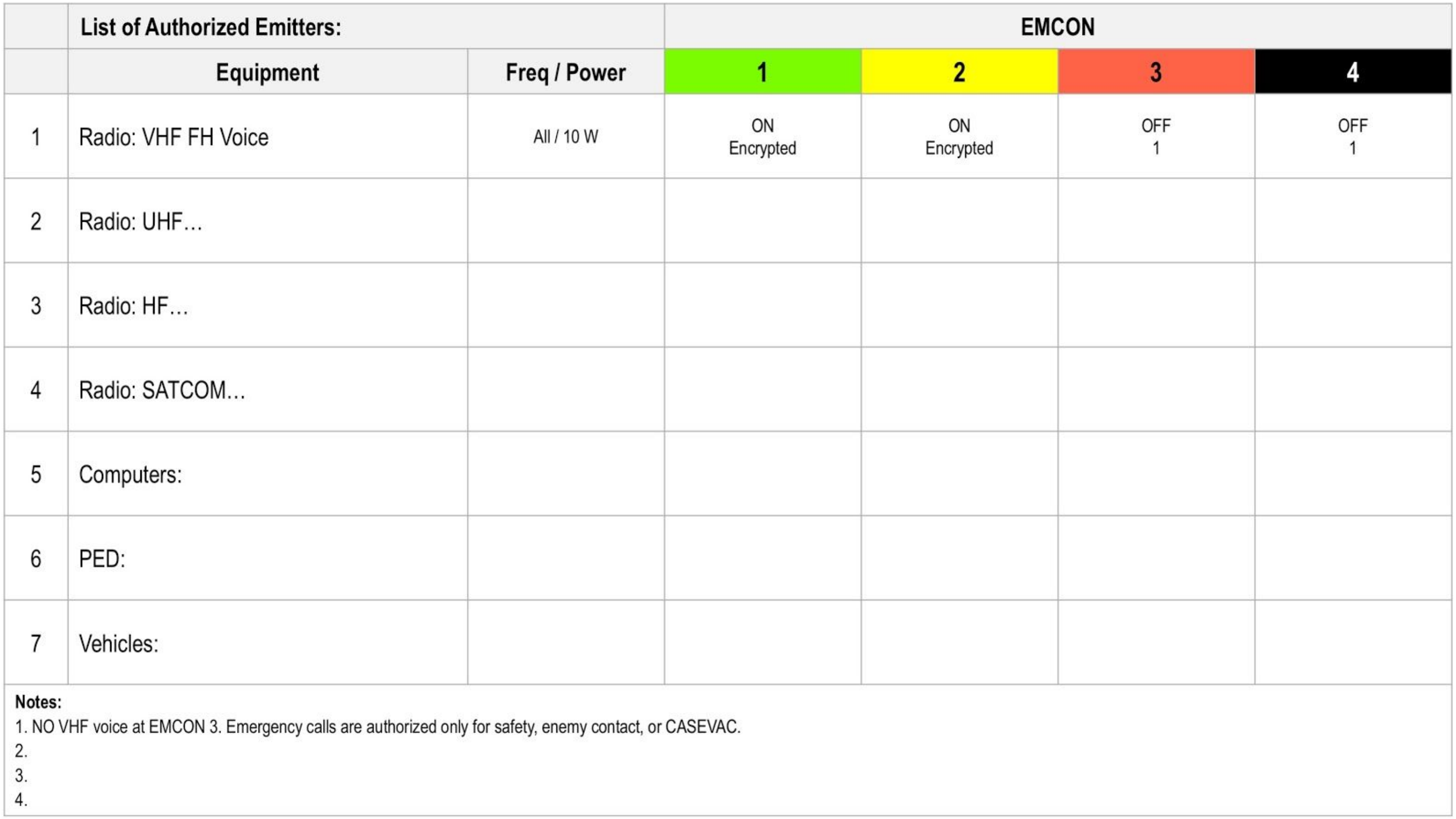
Notes on SATCOM

The S-6 should PLAN for a loss or degradation of SATCOM. Many units are overly-dependent on SATCOM for primary nets. Our headquarters, and all large C2 ground systems—BFT / JBC-P, CPOF, DCGS, AFATDS—rely on SATCOM-enabled local-area networks (LAN) for communications.

When we train to reduce our dependence on SATCOM, we may actually *increase* our vulnerability to adversary direction finding. Detailed communications planning must prepare for EMI and adversary EA jamming.

Contributors: **BBM**, ELK, 1 Nov 2020.

Template: **List of Authorized Emitters**



	List of Authorized Emitters:		**EMCON**			
	Equipment	**Freq / Power**	**1**	**2**	**3**	**4**
1	Radio: VHF FH Voice	All / 10 W	ON Encrypted	ON Encrypted	OFF 1	OFF 1
2	Radio: UHF…					
3	Radio: HF…					
4	Radio: SATCOM…					
5	Computers:					
6	PED:					
7	Vehicles:					

Notes:
1. NO VHF voice at EMCON 3. Emergency calls are authorized only for safety, enemy contact, or CASEVAC.
2.
3.
4.

Notes: Typeface is Arial narrow, black. Table header text is bold. Table borders are 0.75 point, 25% gray lines. Table headers are 5% gray fill. Second column: List technology, not specific nets. Third column: If specific frequencies and power levels are noted, the list may require classification. EMCON columns: Note ‘ON’ or ‘OFF’ with explanations. Number each footnote and explain EMCON restrictions in the bottom section. EMCON 2 is the desired standard for operations. Title and date the list for a specific mission in one AO against a specific adversary.

Procedures

EP EMCON Responsibilities

Purpose. To REDUCE electromagnetic emissions IOT AVOID being located and targeted.

Tasks for the Commander. Electromagnetic protection (EP) *must* be a command responsibility.

1. UNDERSTAND adversary electromagnetic support (ES) collections capabilities: electromagnetic reconnaissance, direction finding (DF), and SIGINT.

2. UNDERSTAND friendly electromagnetic emission signatures: radios, computers, portable electronic devices (PED), UAS, vehicles, generators, and radars.

3. TRAIN to operate with SOPs that require less electromagnetic communications. TASK the S-2 and S-6 to implement EP EMCON procedures against *specific* adversary capabilities.

4. TASK subordinate unit commanders to DEVELOP and TRAIN on SOPs that require less radio communications. Signal plans should merge EP EMCON procedures with visual signals. Well-trained units need less comm.

5. COMMAND combat operations under adversary EW threats. DIRECT EP EMCON measures that balance the risk of detection against communication requirements.

Tasks for the S-2

1. UNDERSTAND adversary electromagnetic support (ES) collection capabilities: electromagnetic reconnaissance, direction finding (DF), and SIGINT.

2. CONDUCT IPB. RESEARCH adversary electromagnetic order of battle (EOB) in the AOI: electromagnetic reconnaissance, direction finding (DF), SIGINT, COMINT, and ELINT.

3. REQUEST friendly ES to COLLECT on adversary EOB. DISSEMINATE adversary EOB updates. NOMINATE adversary ES collection systems for targeting.

4. REQUEST an electromagnetic survey from RadBn or MCIOC or a CI assessment from CI/HUMINT to UNDERSTAND friendly electromagnetic emission signatures: radios, computers, PED, UAS, vehicles, generators, and radars.

.

6. ADVISE the commander.

Tasks for the S-3

1. UNDERSTAND adversary electromagnetic support (ES) collection capabilities: electromagnetic reconnaissance, DF, and SIGINT.

2. UNDERSTAND friendly electromagnetic emission signatures: radios, computers, PED, UAS, vehicles, generators, and radars.

3. ADD an EMCON matrix to every execution checklist for every mission in your SOP.

   DEVELOP and TRAIN on SOPs that require less radio communications. Signal plans should merge EP EMCON procedures with visual signals. Well-trained units need less comm.

4. PLAN simple flexible operations. PLAN combat operations under adversary EW threats.

   PLAN operations that are less dependent on radio communications: less control measures, less link-ups, less “on-order” tasks, and less reporting. There is no EMCON plan. There are combat plans, adjusted for EW threats.

5. RUN the CP IAW EP EMCON SOPs. The CP is the largest EM emitter in the battalion.

6. ADVISE the commander.

Tasks for the S-6

1. UNDERSTAND adversary electromagnetic support (ES) collection capabilities: electromagnetic reconnaissance, DF, and SIGINT.

2. UNDERSTAND friendly electromagnetic emission signatures: radios, computers, PED, UAS, vehicles, generators, and radars.

3. ADD an **EMCON matrix** to every execution checklist for every mission in your SOP.

   CREATE a **list of authorized emitters** for every tactical mission in your SOP.

   CREATE a **PACE plan** for every recurring tactical mission in your SOP.

   DEVELOP and TRAIN on SOPs that require less radio communications. Signal plans should merge EP EMCON procedures with visual signals. Well-trained units need less comm.

4. PLAN communications under adversary EW threats. READ HHQ comm directives and EMSO guidance. RECOMMEND EMCON procedures by task and phase.

5. WRITE CEOI and Annex K with SPINS that implement EP EMCON measures and reinforce EP EMCON SOPs.

6. INSTALL CP communications. MASK and DISPERSE radio antennas, and REDUCE power IOT AVOID being located and targeted. PRIORITIZE LPD nets. REPORT EMI.

7. ENFORCE the comm plan and EP EMCON measures on subordinate units and attachments. ENFORCE radio procedures. Well-trained units need less comm.

8. CONTROL comm equipment. RESTRICT equipment to some users as an EP technique. MAINTAIN comm equipment. ENFORCE COMSEC and TRANSEC procedures.

9. MONITOR net transmissions. ENFORCE comm windows, comm procedures, and comm SOPs.

10. ADVISE the commander.

Tasks for Marines

1. UNDERSTAND adversary electromagnetic support (ES) collection capabilities: electromagnetic reconnaissance, DF, and SIGINT.

2. UNDERSTAND friendly electromagnetic emission signatures: radios, computers, PED, UAS, vehicles, generators, and radars.

3. TRAIN on SOPs that require less radio communications. Well-trained units need less comm.

4. CONDUCT combat operations under adversary EW threats.

Notes

EP EMCON SOPs are a leadership challenge. All leaders have to SUPERVISE their Marines and ENFORCE EP EMCON compliance.

For most units, this is a new level of detailed communications planning. Normal procedures are insufficient against the emerging threat. The typical guard chart below is **silent** on EMCON priorities, alternate nets (PACE plans), vulnerabilities to adversary detection, or guidance.

Contributors: **BBM**, TEH, 1 Nov 2020.

Notional **Guard Chart**

Radio Guard Chart: 1/1

Assigned Nets A As Required C Net Control M Monitor W When Directed X Guard * RTX		**E:** REGT CMD 1	REGT TAC 1	REGT INTEL 1	REGT CSS	**P:** BN TAC 1	**A:** BN CMD 1	BN FSC	81 COF	ARTY COF	BN TACP/L	TAR/HR	BN INTEL	BN TAC 2	**C:** BN CMD 2	CONVOY CONTROL	BN COMM COORD	TAD 1	TAD 2	TATC 1	TATC 2	LZ CONTROL
Equipment / Emissions V VHF SC VHF SINGLE CHANNEL FH VHF FREQUENCY HOP HF HF 3G HF 3G ALE U UHF VOICE S UHF SATCOM DEDICATED D UHF DAMA IW UHF SATCOM IW		IW (SAA)	FH (NET ID 210)	FH (NET ID 211)	HF (8.750/3.525M TAC CHAT)	FH (NET ID 181)*	IW (SAA)	FH (NET ID 182)*	FH (NET ID 183)	FH (NET ID 184)*	FH (NET ID 185)	HF (ALE SET 1, VOICE)	HF (ALE SET 5, VOICE)	FH (NET ID 186)*	HF (ALE SET 3, TAC CHAT)	FH (NET ID 187)	HF (ALE SET 4, TAC CHAT)	U (310.200M)	U (311.200M)	U (313.200M)	U (314.200M)	U (312.200M)
Units / Restoration		8	9	10	11	1	2	3	4	5	6	7	12	13	14	15	16	18	19	20	21	22
Regiment	*RIPPER*	C	C	C	C																	
Battalion MAIN	*SAVAGE*	X	X	X	X	C	C	C	X	X	C	A	C	C	C	C	C	A	A	A		A
Battalion TAC		X	X	X	X	W	W	W	W	W	W	A	W	W	W	A	A	A	A	A		A
A Co	*APEX*					X	W	X	A	A	A	A	W	W	W	A	A	A	A	A		A
B Co	*BAJA*					X	W	X	A	A	A	A	W	W	W	A	A	A	A	A		A
C Co	*CACTUS*					X	W	X	A	A	A	A	W	W	W	A	A	A	A	A		A
LAR Co	*BADGER*					X	W	X	A	A	A	A	X	W	W	A	A	A	A	A		A
81s	*MUSTANG*					X		X	C	A	A					A	A	A	A	A		A
Arty	*NOMAD*					X	W	X	A	C	A					A	A	A	A	A		A
Snipers	*PHANTOM*																					
DASC	*CHECKLIST*											C						A	A	C	C	A
MAG Flight	*BANTAM*																	C	C	X	X	C

Notes: A guard chart is INSUFFICIENT for EP EMCON guidance. NO EMCON information: **"Data / TAC CHAT, SATCOM, and HF are safer than VHF/UHF voice."** NO EMCON directives. NO comm windows. NO mobile phone or PED information. NO list of authorized emitters in the AO. NO PACE (primary, alternate, contingency, emergency) Plan—the 'Units / Restoration' row is only a prioritization scheme. NO recognition of adversary threats.

EP EMCON SOP

Chapter 2 How To

In this Chapter

- How to reduce electromagnetic (EM) emissions from:
  Radios, computers, PED, UAS, vehicles, generators, and radars
- How to request friendly ES and EA

Marine Corps Intelligence Schools
Intelligence Training Enhancement Program

SIGMAN EP EMCON SOP:
Chapter 2: How To

Marine Corps Intelligence Schools (MCIS)
Intelligence Training Enhancement Program (ITEP)

How To

REDUCE Radio EM Emissions

Purpose. To REDUCE electromagnetic emissions IOT AVOID being located and targeted.

Process. TRAIN to the *Ten Commandments* IOT REDUCE radio EM emissions.

The Ten Commandments

	Technique	Guidelines
1.	**TALK Less**	TALK **less**. TRANSMIT only **mission-critical** information. TALK **short**. TALK **correct**.
2.	**SCHEDULE Less**	MINIMIZE required **reports**. SCHEDULE comm **windows**.
3.	**MOVE**	MOVE **units**. MOVE **radios**. When in doubt, MOVE.
4.	**CHAT**	CHAT. Do NOT **call**. CHAT reports, requests, and brevity codes.
5.	**SIGNAL**	SIGNAL **movement**, **tactical action**, and **convoys** with one-arm hand and arm signals.
6.	**WIRE**	COMMUNICATE between stationary positions with **comm wire** and field phones.
7.	**MASK Antennas**	PLACE CP, vehicle, and manpack antennas behind **barriers**, **buildings**, **woods**, or **hills**.
8.	**REDUCE Power**	SHUT it OFF when not in **use**. SET radio to **low power**.
9.	**PRIORITIZE LPD Nets**	COMMUNICATE on **radio nets** that have LPD. KNOW which nets are more **vulnerable**.
10.	**PLAN Simple Flexible Ops**	PLAN operations that require **less radio calls.** PLAN **less nets**.

Notes

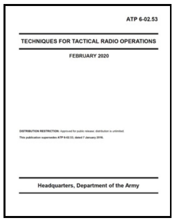
Marines and leaders need to TRAIN on proper radio procedures and ENFORCE disciplined EP EMCON practices. See TALK Less, SCHEDULE Less, MOVE, CHAT, SIGNAL, WIRE, MASK Antennas, REDUCE Power, PRIORITIZE LPD Nets, and PLAN Simple Flexible Ops.

The most important goal is to reduce radio calls. The technical signature of Marine infantry units is mostly radio emissions. The main effort is to **PLAN simple flexible operations** that require less radio calls. Well-trained units need less comm.

Marines need to understand that covered nets do NOT protect them from being located and targeted. Secure nets like SINCGARS VHF FH can be located. The *volume* of traffic—especially before stepping off on an operation—is an indicator to the enemy. The *origin* of the traffic is a target.

Marine command posts, a priority target for the enemy, emit large electromagnetic signals. Locate CPs in buildings or woods, and disperse tents, vehicles, antennas, and generators as far away as possible. Cover everything with camouflage netting. CPs are vulnerable to adversary DF collections and must enforce strict EP EMCON procedures.

References



ATP 6-02.53

TECHNIQUES FOR TACTICAL RADIO OPERATIONS

FEBRUARY 2020

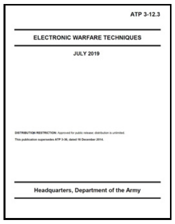
DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

This publication supersedes ATP 6-02.53, dated 7 January 2016.

Headquarters, Department of the Army

ATP 6-02.53 *Techniques for Tactical Radio Operations*, 13 Feb 2020. 218 pages.

Chapter 10 lists EP techniques for radios.



ATP 3-12.3

ELECTRONIC WARFARE TECHNIQUES

JULY 2019

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

This publication supersedes ATP 3-36, dated 16 December 2014.

Headquarters, Department of the Army

ATP 3-12.3 *Electronic Warfare Techniques*, 16 Jul 2019. 124 pages.

Chapter 7 lists EP techniques.

Contributors: **BBM**, 1 Nov 2020.

How To

TALK Less

Purpose. To REDUCE the length of radio calls IOT AVOID being located and targeted.

Procedures

1. TALK **less**.

TRANSMIT only **mission-critical** information. STOP and THINK before you TALK.

KILL extraneous radio checks. KILL extraneous radio calls and responses.

TALK only during comm windows.

2. TALK **short**.

TRANSMIT concise ten-second sentences. PAUSE. CUT sentences in half. DROP full callsigns. After the first call, DROP callsigns altogether. When possible, DROP “this is.” DROP “OVER.” AVOID repetition.

Long transmission	Short transmission
“TALON 2-3, TALON 2-3, this is TALON 2-2. Radio check, OVER.”	“2-3, 2-2. Radio check, OVER.”
“TALON 2-2, this is TALON 2-3. I have you loud and clear, OVER.”	“2-2, 2-3. ROGER, OVER.”

REDUCE combined conversation lengths between units.

USE **prowords**, **brevity codes**, and **execution checklists** to REDUCE the length of radio transmissions. See Prowords and Brevity Codes.

3. TALK **correct**.

USE proper radio procedure. Radio calls should TRANSMIT orders, ASK questions, or REPORT information.

Analyses show that many radio calls are explanations, corrections, discussions, repetitions, and reminders—NOT concise directives or reports. This is evidence of poor training and poor planning. Well-trained units need less comm.

Directive transmission	Notes
“2-3. Move to phase line AMBER, OVER.”	A directive transmission is preceded by one callsign, clearly identifying the recipient.

Interrogative transmission	Notes
“2-3, 2-2. What is your ETA? OVER.”	An interrogative is preceded by two callsigns: **you** this is **me**. Do NOT say “Interrogative.”

Descriptive transmission	Notes
“2-3, 2-2. SPOTREP. Three insurgent vehicles parked at traffic circle K-2. Time 1430. Machineguns mounted on each vehicle. OVER.”	A descriptive transmission is preceded by two callsigns: **you** this is **me**.

Relay transmission	Notes
“2-3, RELAY TO 2-9. Raid package is BUDWEISER. OVER.”	A relay is preceded by two callsigns: **you** and the **third party**, but NOT the sender.

USE proper operational terms (H-Hour, LD), tactical terms (fix, flank vs. envelop), terrain terms (road junction vs. intersection), distance terms (meters of distance, feet of elevation, feet of runway), and time terms (H+5 hours).

SPELL large numbers: 436 is “FOUR-THREE-SIX.”
SPELL decimals: 9.8 is “NINE DECIMAL EIGHT.”

4. TALK **formats**.

STANDARDIZE concise radio calls to REDUCE the length of radio transmissions.

STANDARDIZE report templates, especially personnel and logistics reports.

POSREP SOP	Notes
“2-3, 2-2. Send POSREP, OVER.”	Request position report.
“2, 3. POSREP. Grid 7-7-4, 2-4-2, OVER.” or	Grid.
“2, 3. POSREP. Checkpoint 1-4-ALPHA, OVER.” or	Checkpoint.
“2, 3. POSREP. 4-0-0 meters east of phase line RED, OVER.” or	Relative to a known point.
“2, 3. POSREP. Moving north on route TRUMAN, OVER.”	Moving, direction, and route.

SPOTREP SOP	Notes
“2-2, 2-3. SPOTREP. Three insurgent vehicles parked at traffic circle K-2. Time 1430. Machineguns mounted on each vehicle. OVER.” 1. Reporting unit and “SPOTREP” 2. Size	SPEAK in sentences. Skip lines that do not apply. Do NOT say, “Line one is… Line two is…” Do NOT say “BLANK” or “NEGAT.”

3. Activity 4. Location 5. Unit 6. Time 7. Equipment 8. Assessment	

5. TALK to **leaders**.

As far as possible, leaders should talk to leaders to avoid friction, misunderstandings, delays, and repeated transmissions.

A clear mission and **commander's intent** requires less radio calls. Simple flexible plans, with less centralized control and less "on order" tasks, require less radio calls

6. AVOID **garbage**.

KILL useless phrases that take up space, but add no value. SEEK concise terms.

Garbage transmission	**Short transmission**
"RAPTOR 2-3, RAPTOR 2-3, this is RAPTOR 2-2. Interrogative. Are all your vehicles ready? OVER." "Affirmative, RAPTOR 2-2. Be advised, we are fueled and standing by. Send your traffic, OVER." "ROGER, RAPTOR 2-3. You will initiate movement at this time. Report all checkpoints hourly. How copy my last? OVER." "RAPTOR 2-2, this is Raptor 2-3. Lima Charlie. ROGER your last. Copy all. Will report departing the Start Point shortly, OVER.	"2-3, move now. OVER." "2-2, 2-3. ROGER. OVER."

7. AVOID transmitting **essential elements of friendly information** (EEFI) on **uncovered** nets. PRC-153 (UHF) nets, although short-range, are the most vulnerable.

Strength	—	Number of personnel, size of unit.
Equipment	—	Type, quantity, condition.
Logistics	—	Procedure for resupply, depots.
Disposition	—	Where, what positions, map coordinates.
Organization	—	How, what, chain of command, force structure.
Movement	—	Where, how, when, and good or bad.
Unit	—	Type, designation.
Personalities	—	Who, where. **Names**, **ranks**.

See page 7-6 through 7-8 of MCRP 8-10B *Radio Operator's Handbook,* 4 Apr 2018.

8. MONITOR net **transmissions**. Any and all radio users have a responsibility to monitor the net IOT reduce talkative users.

TRANSMIT brevity code ‘ZIPLIP’ IAW MCRP 3-30B.1 *Brevity: Multi-Service TTPs for Brevity Codes*, 28 May 2020.

ZIPLIP brevity code transmission	Notes
“2-3. ZIPLIP, OVER.”	Shut up. ZIPLIP is a reminder to “limit transmissions to critical information only.”

Contributors: **BBM**, BMW, 1 Nov 2020.

How To

SCHEDULE Less

Purpose. To REDUCE the number of radio calls IOT AVOID being located and targeted.

Process

1. MINIMIZE required **reports**. MINIMIZE battle rhythm SOP reporting requirements.

   MINIMIZE hourly radio calls and daily reports.
   MINIMIZE radio checks, POSREPS, and SITREPS.
   Do NOT send empty NSTR reports.
   STANDARDIZE report formats. SEND concise personnel and logistic reports by text burst.
   DEVELOP tactical SOPs that require less reporting. See PLAN Simple Flexible Ops.

2. SCHEDULE comm **windows**: “REPORT between 1600–1800.”

   SCHEDULE multiple comm windows at different times daily to avoid creating a pattern. Except for emergencies—safety, enemy engagement, or CASEVAC—WAIT for comm windows to report. As far as possible, leaders should talk to leaders to avoid friction, misunderstandings, delays, and repeat transmissions. LEARN to live with EMCON.

   SET a separate net for each comm window: “1600-Tac1 (VHF FH). 2400-Cmd1 (HF Data).”
   SCHEDULE comm windows to blend behind “normal” background signal noise.
   See COLLECT Own-force EM Emissions Signature.

Notes

Most headquarters have a huge appetite for regular information. Report requirements—for text, data, PowerPoint graphics, and imagery—consume excessive bandwidth and generate large radio signals. Exhaustive demands for unit locations, activities, and situations produce near-continuous radio chatter. Constant emitters—BFT / JBC-P, ALE / 3G ALE HF, and ANW2—squawk hundreds of times per day on their own. These communications habits will prove deadly when we are faced with a sophisticated adversary who can integrate modern EW collection capabilities with precision fires.

Do comm windows reduce our signature? Or, after a quiet day, does a sudden surge of activity actually *increase* our signature and cue the enemy?

Contributors: **BBM**, BMW, 1 Nov 2020.

How To

MOVE

Purpose. To CHANGE the origin of radio calls IOT AVOID being located and targeted.

Process

1. MOVE **units**.

   Move CPs, antenna farms, equipment, assembly areas, bivouacs, patrol bases, and unit positions. SET SOP standards for time. TRAIN to rapidly set up and tear down the CP.

   MOVE after enemy jamming. *EA is a strong indicator of incoming enemy fires*.
   See REPORT Electromagnetic Interference (EMI).

   When in doubt, MOVE. The only way to AVOID being located and targeted is to MOVE. MINIMIZE transmissions sent from any one location.

2. MOVE **radios**.

   MOVE radio vehicles. TRANSMIT, then move. Or DRIVE away, TRANSMIT, and return.
   Do NOT transmit when parked at the CP.

   MOVE manpack radios. TRANSMIT, then move.

   MOVE after talking with aircraft. When uncovered UHF comms are complete, all prior EMCON efforts are ruined. MOVE. Although UHF HAVEQUICK is frequency hopping, most air units do NOT use it due to safety-of-flight concerns.

3. MOVE **UAS**. LAUNCH at one site, MOVE, and then recover at a separate site.
   Like artillery: “shoot and scoot.” See REDUCE UAS EM Emissions.

4. MOVE **vehicles**.

5. MOVE **generators**.

6. MOVE **radars** after each prolonged scanning period.

Contributors: **BBM**, 1 Nov 2020.

How To

CHAT

Purpose. To REDUCE the number of radio calls IOT AVOID being located and targeted.

Process for Marines

1. CHAT. Do NOT call.

   CHAT all standard **reports**: Logistics, personnel, administrative, and casualty reports.

   CHAT all standard **requests**.

   CHAT all **POSREPs**.

   CHAT all execution checklist **brevity codes**.

2. CHAT during scheduled comm windows. SHUT it OFF when the radio is not being used.
   PRC-117G: MUOS satellite connectivity "handshake" process requires constant emissions.

3. CHAT with a directional antenna. AVOID omnidirectional antennas.
   KNOW the position of your satellite in the sky.

4. Do NOT CHAT using mobile phone text. That will get you killed.

5. PICK UP the radio handset for immediate, tactically-demanding, leader-to-leader conversations:

   - Enemy contact,
   - Emergencies,
   - Contingencies, and
   - Time-sensitive events, such as call-for-fire, CAS, MEDEVAC, and helicopter coordination.

   Explanations, recommendations, conversations, and detailed descriptions are also better discussed using voice comms, but lengthy transmissions are dangerous.

Many units, especially aircraft, have limited CHAT capability, and must be contacted using voice comms.

Notes

The significant advantage of TACCHAT is that CHAT message data is sent in short, hard-to-detect packets. CHAT can reduce 95% of voice radio calls and prevent the enemy from locating or targeting you.

There are multiple CHAT equipment configurations:

- GETAC tablet or laptop connected to PRC-117G (MUOS).
- GETAC tablet or laptop connected to PRC-150 (HF) or the new PRC-160 (HF).
- NOTM (network on the move) and NOTM vehicle variants.
- BFT / JBC-P chat function. BFT / JBC-P are constant emitters. Position reporting should be disabled and the CHAT function should be SHUT OFF when NOT being used.
- TACCHAT IP is CHAT between networked computers.
- There is NO VHF radio CHAT capability.

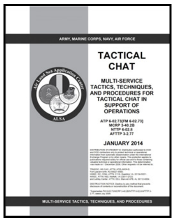
MATCH your equipment to your mission. It is difficult to move on foot with a GETAC laptop, but platoons can maneuver and CHAT with a tablet.

PLAN for power usage. Battery life is short on small devices.

ESTABLISH clear reporting requirements and execution checklists. See EP EMCON Matrix SOP.

USE the same CHAT application as your HHQ. Multiple applications—Mako, MIRC, Adobe Connect, Transverse Chat—exist on multiple platforms.

References



ARMY, MARINE CORPS, NAVY, AIR FORCE

TACTICAL CHAT

MULTI-SERVICE TACTICS, TECHNIQUES, AND PROCEDURES FOR TACTICAL CHAT IN SUPPORT OF OPERATIONS

ATP 6-02.73[FM 6-02.73]
MCRP 3-40.2B
NTTP 6-02.8
AFTTP 3-2.77

JANUARY 2014

[illegible]

MULTI-SERVICE TACTICS, TECHNIQUES, AND PROCEDURES

MCRP 3-40.2B *Tactical Chat: Multi-Service TTP for Tactical Chat in Support of Operations*, 1 Jan 2014. 80 pages.

Contributors: **BLA**, 1 Nov 2020.

How To

SIGNAL

Purpose. To REDUCE the number of radio calls IOT AVOID being located and targeted.

Process

1. SIGNAL unit **movement** with one-arm hand and arm signals IOT REDUCE radio calls.

   SIGNAL **tactical actions**, formations, halts, warnings, and immediate action drills.

   SIGNAL **fire commands** such as OPEN FIRE, SHIFT FIRE, and CEASE FIRE. USE whistles or pyro as back-up. STANDARDIZE one-arm hand and arm signals for patrols.

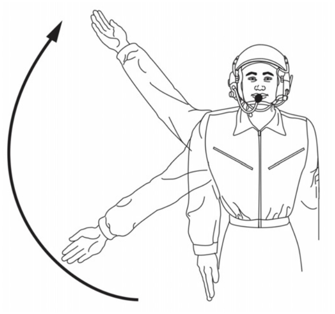
   At night, SIGNAL **link-ups** with IR recognition signals. TRAIN on SOP signals.

   Use a physical signal, such as a flag on a radio antenna, to initiate a pre-planned order.

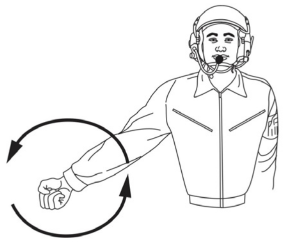
2. SIGNAL **convoys** with one-arm hand and arm signals IOT REDUCE radio calls.

   SIGNAL formations, halts, warnings, and immediate actions drill such as MOUNT, START ENGINES, HALT, SPREAD OUT, and DANGER AREA. Ground GUIDE vehicles with hand and arm signals. USE flags, lights, or horns as back-up. See TC 3-21.60 *Visual Signals.*

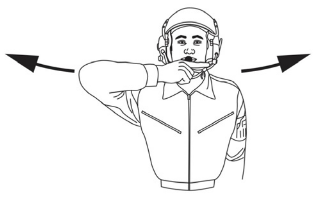
   Convoys—with radios in every vehicle—emit excessive radio signals. TRAIN SOP signals.



MOUNT



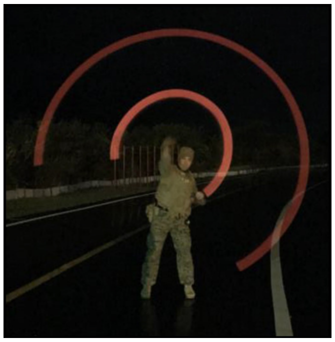
START ENGINES



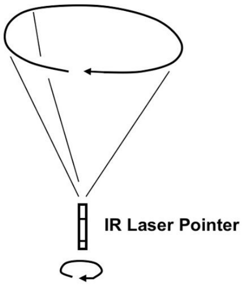
CUT ENGINES

3. SIGNAL your position to **helicopters** with a signal mirror or pyro IOT REDUCE radio calls.

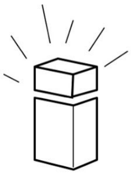
At night, SIGNAL friendly positions to helicopters using BUZZSAW, ROPE, or IR strobe.



BUZZSAW

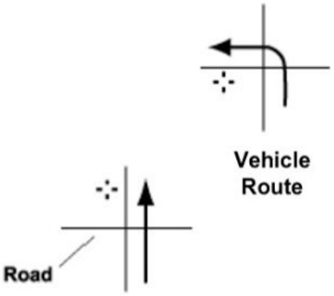


ROPE

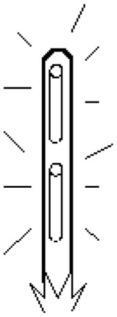


IR strobe

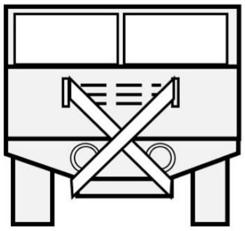
4. MARK convoy routes IOT REDUCE radio calls. MARK intersections and checkpoints. MARK vehicle roles such as convoy commander, security team, or last vehicle with engineer tape.



Mark routes

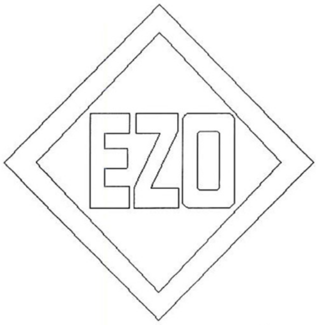


Mark checkpoints

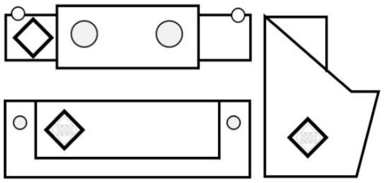


Mark last vehicle

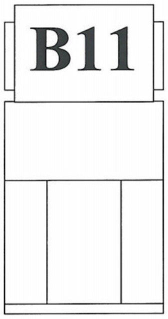
5. MARK vehicles IOT REDUCE radio calls. MARK hoods for aircraft recognition. Visual ID of vehicles increases situational awareness and speeds comms. ESTABLISH SOP markings.



Unit ID



Mark bumpers

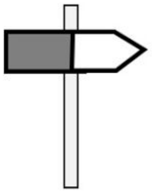


Mark hoods

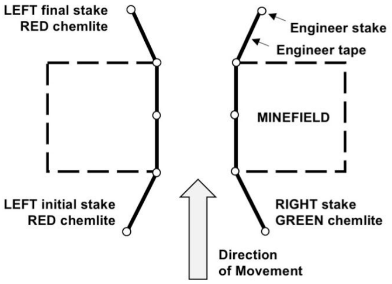
6. MARK vehicle tactical assembly areas (TAA) IOT REDUCE radio calls. Mark entry and exit points, unit parking and bivouac areas, CP, BAS, and RRPs. MARK guides to direct traffic.

MARK unit areas, packs, equipment, weapons, and supplies with company color codes IOT INCREASE situational awareness and speeds execution. ESTABLISH SOP markings.

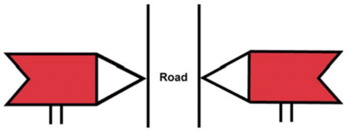
7. MARK traffic lanes IOT REDUCE radio calls. MARK minefields and passage lanes.



NATO Marker

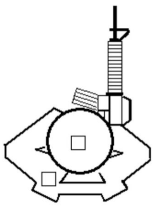


Mark cleared minefield

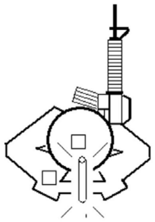


Mark passage lane

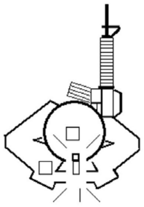
8. MARK key Marines IOT REDUCE radio calls. Visual ID of leaders increases situational awareness, especially at night. ESTABLISH SOP markings.



Glint tape

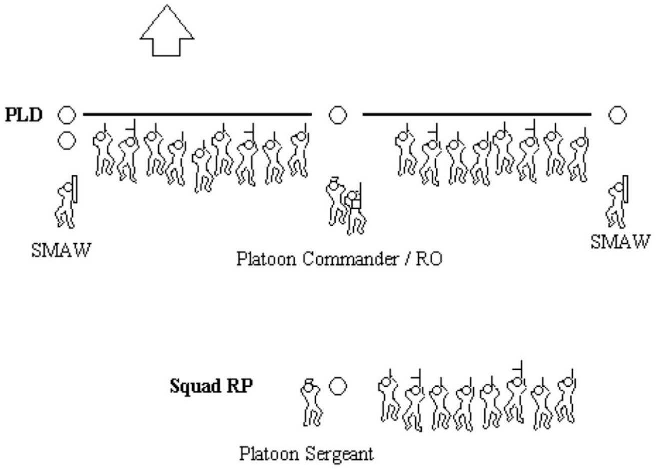


IR chemlite

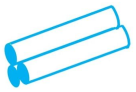


IR beacon

9. MARK friendly unit positions IOT REDUCE radio calls. Mark BP, unit boundaries, and sectors of fire with chemlite bundles. Mark assembly area, ORP, and assault position PLD. Mark ambush positions. Marked cleared buildings, rooms, and trenches. ESTABLISH SOPs.



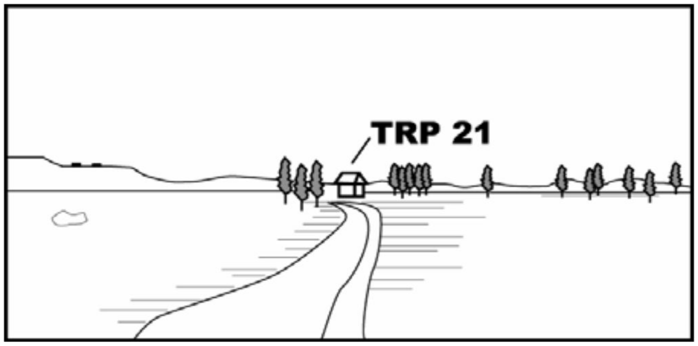
Mark assault position PLD



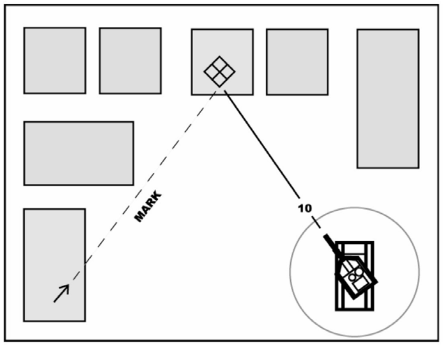
Chemlite bundle

10. MARK targets for aircraft IOT REDUCE radio calls. MARK targets with artillery or mortar marking rounds or smoke. At night, MARK targets with IR SNAKE or tracer rounds.

MARK targets to control ground fires IOT REDUCE radio calls. MARK targets with tracers, smoke, or pyro. At night, MARK targets with IR SNAKE or tracer rounds.



Night: IR Laser SNAKE on TRP 21



Day: MG tracer mark

11. MARK LZs IOT REDUCE radio calls. Every LZ needs four signals: one method of far ITG and one method of near ITG for both day and night. COORDINATE SOP with ACE.

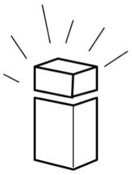
Day ITG:

Far: signal mirror or pyro

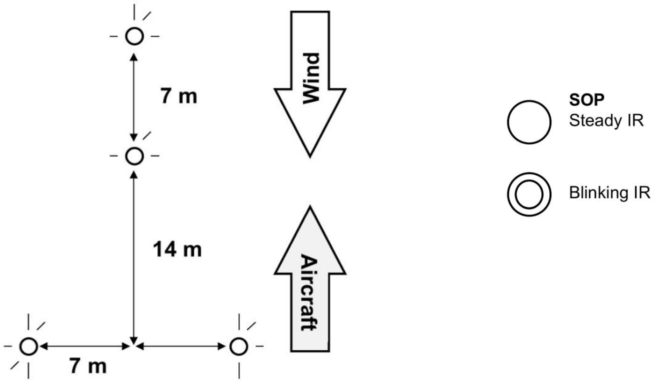
Near: VS-17 air panel

or smoke

Night ITG:



Far: BUZZSAW, ROPE or IR strobe



Near: NATO Y with IR or NATO Y with chemlites

Signal conventions

Two of anything—thumbs, lights, IR flashes, chemlites, clicks, or two dots in TAC CHAT—means YES. Three of anything means WARNING, DANGER, or STOP. One is NO.

GREEN of anything is good, first, FIRE, or GO! RED is danger, last, or STOP! YELLOW is caution. Any pyro signals that require a combination of specific colors should be avoided.

Notes

SIGNAL IOT REDUCE radio calls. **Every signal passed is one less radio transmission.**

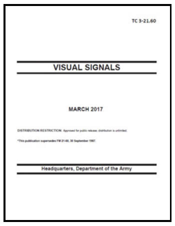
ASSIGN specific signals to every tactical evolution. See EP EMCON Matrix SOP. Signal plans cannot be improvised during the mission brief. Signals must be SOP.

MARK. Marking increases situational awareness and speeds execution. Every marked unit, position, or target reduces confusion and saves multiple radio transmissions. Note that IR marks are ***more*** visible to an adversary with NVGs than ordinary white light or colored chemlites.

BUILD a signal SOP.

TRAIN on SOP signals.

References



TC 3-21.60

VISUAL SIGNALS

MARCH 2017

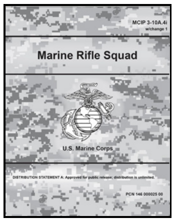
DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

*This publication supersedes FM 21-60, 30 September 1987.

Headquarters, Department of the Army

TC 3-21.60 *Visual Signals*, 17 Mar 2017.
96 pages.

Defines hundreds of hand-and-arm, flag, and light signals for ground, vehicle, and ground-to-aircraft operations.



MCIP 3-10A.4i
w/change 1

Marine Rifle Squad

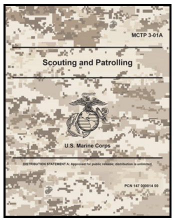
U.S. Marine Corps

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

PCN 146 000025 00

MCIP 3-10A.4i *Marine Rifle Squad*, 15 May 2020.
296 pages.

Appendix B includes sixteen pages of hand-and-arm signals for ground, vehicle, and ground-to-aircraft operations.



MCTP 3-01A

Scouting and Patrolling

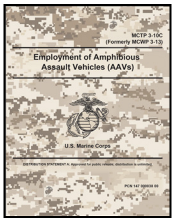
U.S. Marine Corps

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

PCN 147 000014 00

MCTP 3-01A *Scouting and Patrolling*, 24 July 2020.
319 pages.

The new MCTP 3-01A is missing an appendix for patrolling-specific hand and arm signals, but tracking hand and arm signals are included in Chapter 9.



MCTP 3-10C
(Formerly MCWP 3-13)

Employment of Amphibious Assault Vehicles (AAVs)

U.S. Marine Corps

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

PCN 147 000038 00

MCTP 3-10C *Employment of Amphibious Assault Vehicles (AAVs)*, 4 Apr 2018.
264 pages.

Appendix J lists standard flag, light, and marker signals. Appendix K lists hand and arm signals.

Contributors: **BBM**, 1 Nov 2020.

How To

WIRE

Purpose. To REDUCE the number of radio calls IOT AVOID being located and targeted.

Process

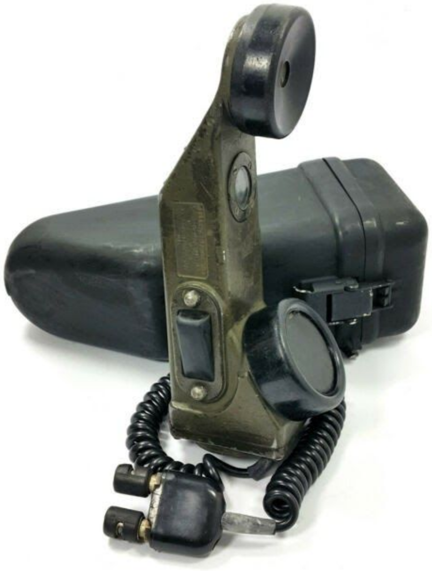
1. COMMUNICATE between stationary positions with **comm wire** and field phones.

2. COMMUNICATE between separate elements of a field HQ using **comm wire** and field phones. COMMUNICATE with remote antenna sites, OPs, and security posts.

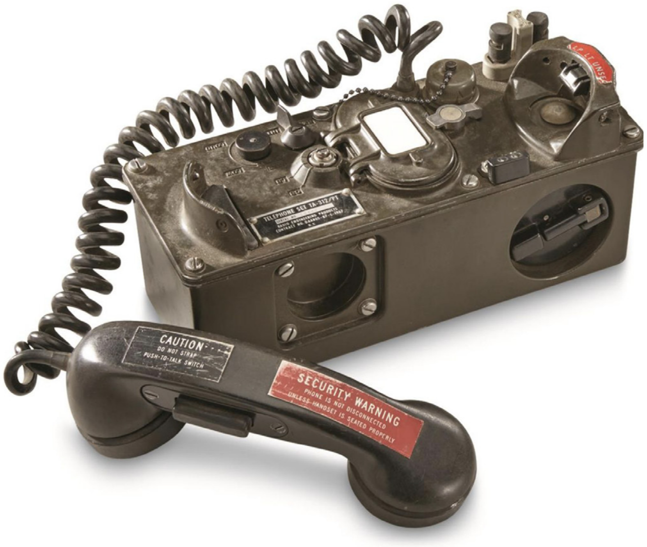
Notes

Ukrainian forces, under intense and near-continuous Russian EA jamming, have learned to depend on wire communications in stationary positions.

Field telephones have been removed from the equipment lists of most Marine units.



TA-1 Field telephone



TA-312 Field telephone

Contributors: **BBM**, 1 Nov 2020.

How To

MASK Antennas

Purpose. To REDUCE the direction of radio calls IOT AVOID being located and targeted.

Process for CPs

1. PLACE antennas behind barriers, buildings, woods, or hills IOT MASK friendly electromagnetic emissions. PARK behind a berm for antenna defilade.

2. DISPERSE antennas as far away from the CP as possible.

   DISPERSE antennas as far away from each other as possible.

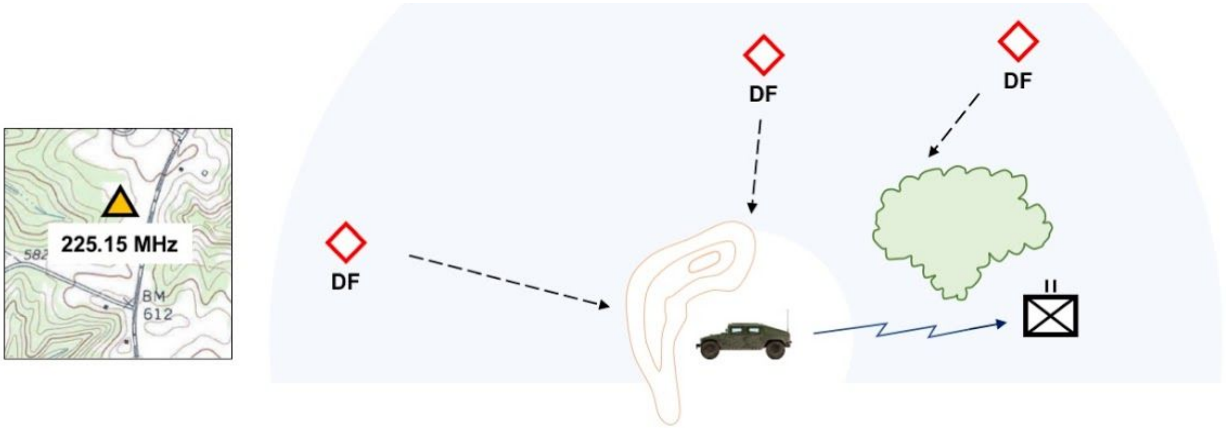
3. CONSTRUCT field expedient antennas IOT direct signals away from adversary DF units.

Process for vehicle-mounted radios

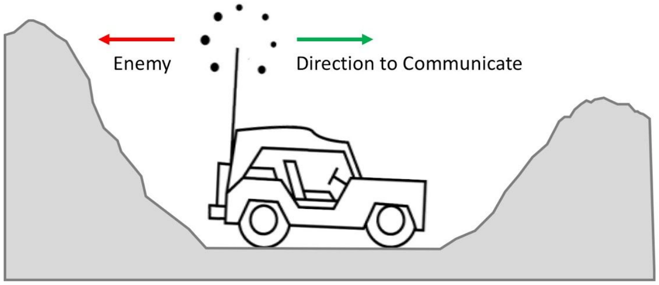
1. PLACE vehicle antennas behind barriers, buildings, woods, or hills IOT MASK friendly electromagnetic emissions. PARK behind a berm for antenna defilade.

2. DISPERSE vehicle antennas as far away from each other as possible.

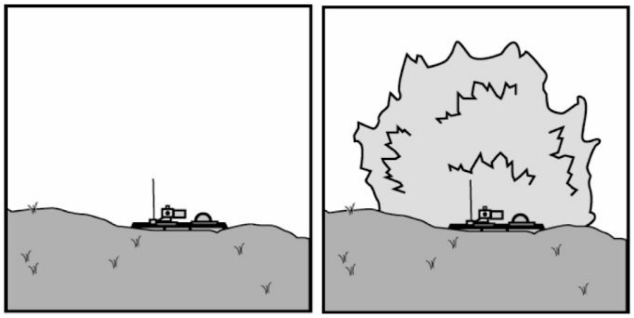
3. KEY handsets only when antennas are masked.



MASK signals from adversary DF units.



Antenna defilade.



Front view. Background vegetation avoids skylining.

Process for manpack radios

1. PLACE manpack antennas behind barriers, buildings, woods, or hills IOT MASK friendly electromagnetic emissions. POSITION behind a berm for antenna defilade.

2. DISPERSE manpack antennas as far away from each other as possible during movements and security halts.

3. KEY handsets only when antennas are masked.

Notes

Marine Corps-issue antennas such as the OE-254, TRC-209, and AS-2259 are *omnidirectional* —they emit signals in all directions—which makes them *more* susceptible to enemy DF capabilities.

Erect antennas to the lowest height needed.

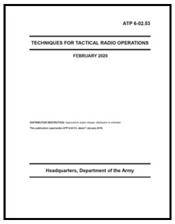
Masking antennas behind terrain adds to camouflage, but does NOT mask signals from overhead—satellite, aircraft, and UAS—collections platforms.

Dispersing antennas avoids dense clusters of signals, but slows tear-down and displacement times.

Construct field expedient antennas to direct electromagnetic energy away from adversary forces.

Use the Systems Planning Engineering and Evaluation Device (SPEED)—a communications planning tool—to find the best locations for antennas.

References



ATP 6-02.53

TECHNIQUES FOR TACTICAL RADIO OPERATIONS

FEBRUARY 2020

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

This publication supersedes ATP 6-02.53, dated 7 January 2016.

Headquarters, Department of the Army

ATP 6-02.53 *Techniques for Tactical Radio Operations*, 13 Feb 2020.
218 pages.

Chapter 8 is "Antenna Techniques." Appendix C is "Antenna Selection."

ARMY, MARINE CORPS, NAVY, AIR FORCE

TAC RADIOS

MULTI-SERVICE TACTICS, TECHNIQUES, AND PROCEDURES FOR TACTICAL RADIOS

ATP 6-02.72
MCRP 3-30B.3 [MCRP 3-40.3A]
NTTP 6-02.2
AFTTP 3-2.18

MAY 2017

DISTRIBUTION STATEMENT D: Distribution authorized to DOD and DOD contractors only to protect information and technical data that may be observed by adversary intelligence systems and determine what indicators hostile intelligence systems may obtain that could be interpreted or assembled to derive critical information in time to be useful to adversaries. This determination was made on 15 March 2017. Other requests will be referred to:

[illegible]

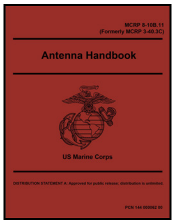
DESTRUCTION NOTICE: Destroy by any method that prevents disclosure of contents or reconstruction of the document.

*Supersedes ATP 6-02.72/MCRP 3-40.3A/NTTP 6-02.2/AFTTP 3-2.18, dated 5 November 2013.

MULTI-SERVICE TACTICS, TECHNIQUES, AND PROCEDURES

MCRP 3-30B.3 *Tac Radios: Multi-Service TTPs for Tactical Radios*, 19 May 2017.
200 pages.

Table 11 lists recommended antenna separation distances for co-located radios.



MCRP 8-10B.11
(Formerly MCRP 3-40.3C)

Antenna Handbook

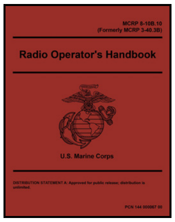
US Marine Corps

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

PCN 144 000062 00

MCRP 8-10B.11 *Antenna Handbook*, 2 May 2016.
193 pages.

Out-of-date ***1999*** *publication. Re-numbered in 2001 and 2016.
Chapter 8 discusses antenna siting.*



MCRP 8-10B.10
(Formerly MCRP 3-40.3B)

Radio Operator's Handbook

U.S. Marine Corps

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

PCN 144 000067 00

MCRP 8-10B.10 *Radio Operator's Handbook*, 4 Apr 2018.
152 pages.

Out-of-date ***1999*** *publication. Re-numbered in 2001 and 2016. Gender-neutralized in 2018. Chapter 3 is siting. Chapter 4 is antennas.*

Contributors: **TEH**, 1 Nov 2020.

How To

REDUCE Power

Purpose. To REDUCE the strength of radio calls IOT AVOID being located and targeted.

Process

1. SHUT it OFF. Radios are OFF when NOT being **used**.

2. SET radio to **low power**. SET to high power only if needed to communicate.

   Most tactical radios have only two power settings: low and high. LEARN how to set power.

Notes

Strong signals travel farther—all the way to the adversary's DF receivers. Generally, manpack radio battery power is low, vehicle radio power is stronger, and generator-equipped command post radio power is strongest. CP signals are more vulnerable *and* more valuable to the adversary.

When we increase radio power in response to attempted enemy jamming, we increase our vulnerability to adversary DF units. This is an adversary TTP.

Contributors: **BBM**, 1 Nov 2020.

How To

PRIORITIZE LPD Nets

Purpose. To REDUCE electromagnetic emissions IOT AVOID being located and targeted.

Process

1. COMMUNICATE on **radio nets** that have low probability of detection (LPD).

   Data / TAC Chat, SATCOM, and HF are safer than VHF/UHF voice.

2. ASK the S-2 and the S-6, “What radio nets are *less* vulnerable to adversary collections in our AO?”

   There is NO standard list of LPD nets. Adversary ES collections capabilities are different in every AO, every month. Friendly equipment availability, task organization, distances, retrans, and comm requirements change for each mission.

   The S-6 will list LPD nets for a *specific* adversary in a *specific* AO for a *specific* time. See EP EMCON List of Authorized Emitters SOP.

3. KNOW which nets are more **vulnerable**.

   MEMORIZE CEOI SPINS. MEMORIZE the PACE plan and the EMCON matrix.

   “**Safest nets:** HF chat > HF voice > VHF FH > VHF SC > UHF uncovered.”

   or

   “**Communicate in order:** Multi-channel LOS, SATCOM, HF, VHF FH, then VHF SC.”

4. LEARN EP EMCON best practices. LEARN the *terms* and the *technology*.

   “Always use VHF FH. Avoid VHF SC.”

   “UHF uncovered black gear is vulnerable.”

   “SATCOM data exceeds HF data capability.”

> “SHF and EHF directional antenna on single-channel TACSAT makes DF difficult.”
>
> All leaders need to UNDERSTAND adversary electromagnetic support (ES) collections capabilities, UNDERSTAND friendly electromagnetic (EM) emissions signatures, and REDUCE friendly electromagnetic emissions by using the right equipment.
>
> Leaders need to protect their unit by enforcing good EP EMCON practices.

Notes for the S-6

LPD decisions require a number of tradeoffs: Constant emitters—BFT / JBC-P, ALE / 3G ALE HF, and ANW2—have a low probability of intercept (LPI), but they emit signals continuously.

Using LOS systems to reduce SATCOM dependency may *increase* our vulnerability to adversary DF. UHF HAVEQUICK is safer, but most aviation units rarely use it due to safety-of-flight considerations.

LPD guidelines must be shaped by equipment availability. “USE HF data” is meaningless to units without HF radios. Some units need more HF radios.

The S-6 should enforce EP EMCON standards by controlling equipment. For certain missions, do NOT issue radios, antennas, or batteries for vulnerable nets.

LPD guidance must be simple and memorable. Nets and equipment that your Marines do NOT use are irrelevant. A long, complex, coded list of technology, like the one below, is NOT helpful:

LPD Nets: AO MAPLE, 1 Nov 2020					
Tac 1 (VHF FH)	3	UHF LOS	4	SATCOM	1
Tac 2 (VHF SC)	4	UHF HAVEQUICK	3	GBS (RCV)	1
TAD (UHF)	4	HF 3G ALE voice	2	DTCS (L-Band)	2
Intel (HF data)	1	HF ALE data	1	SHF DSCS	1
Cmd (HF voice)	1	HF	2	BFT / JBC-P	3
FD1 (ANW2)	2	CHAT	1	Iridium (L-Band)	2

Contributors: **BBM**, 1 Nov 2020.

How To

PLAN Simple Flexible Ops

Purpose. To REDUCE the number of radio calls IOT AVOID being located and targeted.

Process

1. PLAN simple flexible operations that require **less radio calls**.

LESS restrictive control measures	=	LESS radio requests, LESS permissions
LESS “on order” tasks	=	LESS radio directives, LESS discussions
LESS cross-boundary fires coordination	=	LESS radio permissions, LESS positions
LESS movement directives	=	LESS radio reports, LESS confirmations

2. ASSIGN each unit a clear task and purpose that requires **less radio calls**.

TASK-ORGANIZE self-contained, autonomous units, under individual commanders in their own zones, with fewer restrictions on how to accomplish their missions. MINIMIZE the number of supporting DS units and external agencies: “HMG are *attached* to Alpha at 1700.”

LESS commanders with MORE authority	=	LESS radio coordination
LESS moving parts and LESS tasks	=	LESS radio coordination
LESS link-ups or passage of lines	=	LESS radio coordination
LESS changes to attachments or DS units	=	LESS radio coordination
LESS requests to supporting DS units	=	LESS radio coordination
LESS HHQ oversight, clearance, control	=	LESS radio coordination

3. ISSUE a clear mission and commander’s intent that require **less radio calls**.

Robust plans with less centralized control, and less “on order” tasks, mean that less decisions are reserved to the HHQ. Autonomous units, with less dependent linkages, can flex when the situation changes. Mission orders and trusted subordinates generate LESS delays, MORE initiative, MORE aggressive action, and MORE momentum.

4. PLAN **less nets**. REDUCE the number of nets to reduce the signature of the unit.

Notes

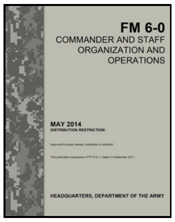
The single, most effective way to reduce the technical signature of the infantry battalion is to focus on how operations are planned and executed. Decentralized and autonomous operations are quieter operations because they require less radio chatter.

The primary EP EMCON effort should be planning operations that require less comm.

Excessive radio signatures occur when one headquarters attempts to tightly control the movement and tactical actions of multiple interdependent units in the same battlespace.

Excessive position reports, clearance of fires, and coordination calls with supporting units—that all have to be transmitted both to the HHQ and multiple adjacent units—increase the number of radio calls exponentially.

References



FM 6-0
COMMANDER AND STAFF
ORGANIZATION AND
OPERATIONS

MAY 2014
DISTRIBUTION RESTRICTION:

Approved for public release; distribution is unlimited.

This publication supersedes ATTP 5-01.1, dated 14 September 2011.

HEADQUARTERS, DEPARTMENT OF THE ARMY

FM 6-0 *Commander and Staff Organization and Operations*, 22 Apr 2016. 394 pages.

Appendix C “Plans and Orders Formats” discusses the advantages of simple, flexible plans.

Contributors: **BBM**, 1 Nov 2020.

How to

REDUCE Computer EM Emissions

Purpose. To REDUCE electromagnetic emissions IOT AVOID being located and targeted.

Process for Marines

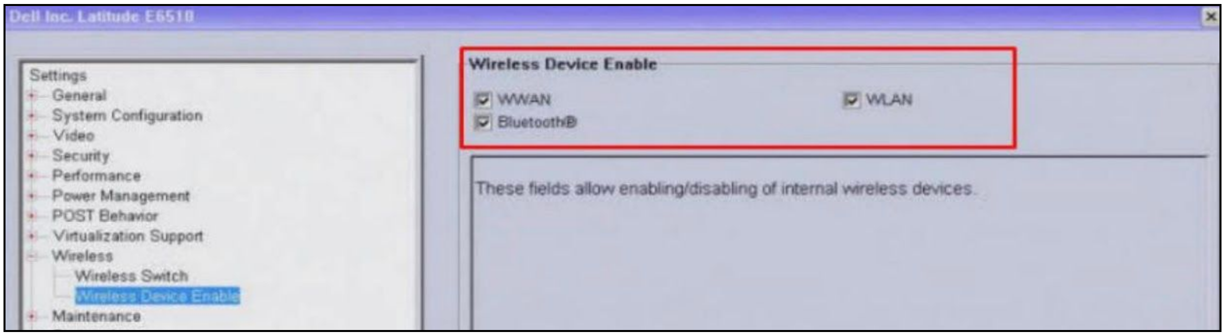
1. SHUT it OFF. Computers are OFF when not being **used**.

   All computers emit small amounts of EM signals for short distances.

2. UNPLUG all unnecessary peripheral devices.

Process for S-6

1. DISABLE wireless—WiFi and Bluetooth—on all computers. The only connections should be shielded wire. USE BIOS, not airplane mode, to ensure administrator control of wireless.



Wireless Device Enable

☑ WWAN ☑ WLAN

☑ Bluetooth®

These fields allow enabling/disabling of internal wireless devices.

Example BIOS (Basic Input/Output System) settings for wireless.

2. DISABLE all unnecessary ports, especially USB, to limit peripheral devices.

3. LIMIT the number of computers and CONTROL access to computers IOT reduce use.

4. MONITOR computer usage via remote console.

Notes

Computer emissions are small. Computer traffic, however, is huge, and significant when being transmitted by radio. **Control the radio to control the traffic**. See REDUCE Radio EM Emissions.

Computer tablets and hand-held devices also emit small amounts of EM noise.
See REDUCE PED Emissions.

References

USMC ECSM 005 *PEDs and WLAN Technologies*, 1 Jul 2016.

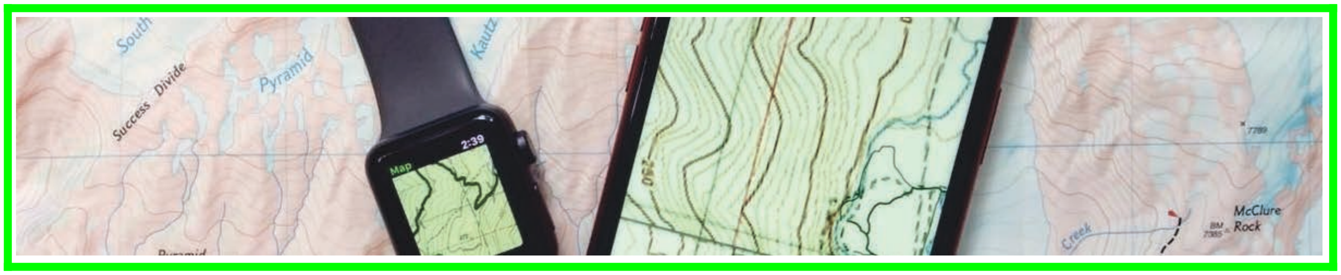
CJCSI 6211.02D *DISN Responsibilities*, 24 Jan 2012.

Contributors: **NMS**, 1 Nov 2020.

How to

REDUCE Portable Electronic Device Emissions

Purpose. To REDUCE electromagnetic emissions IOT AVOID being located and targeted.



Process for commanders

1. PROHIBIT all portable electronic devices (PED).

   EM emission risk is small compared to information leakage. The adversary can exploit vulnerabilities in applications, data storage, geo-located photographs, and internet traffic. Even when wireless is disabled, some devices save location and pattern of life information for later automatic upload, without the user's knowledge. Many PED have more than one transmission technology and are vulnerable even when not connected to the internet.

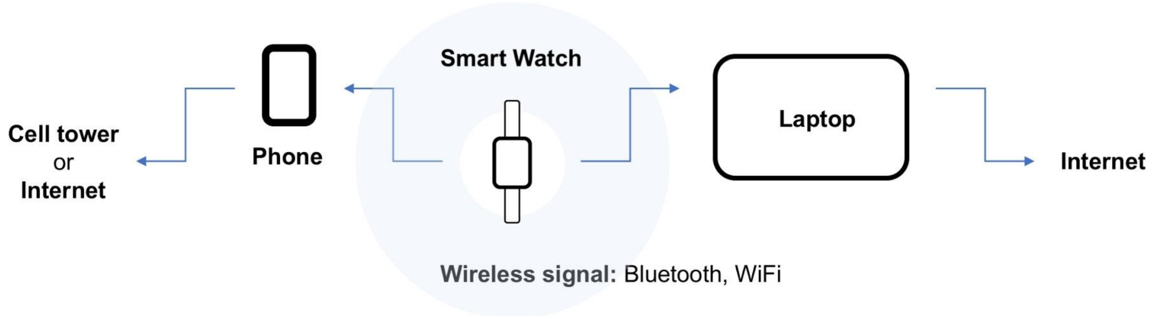
   or

2. COLLECT all PED. When deployed, CONTROL all PED use to specific locations and times.

   SET clear PED policy. NO connections to the Marine Corps network. NO wireless device-to-device information sharing. NO photographs of documents or computer screens. NO access to classified spaces or medical spaces. NO data storage of FOUO or PII.

   Mobile phones run applications, even games, that store GPS location information. Cellular phone connectivity and internet connectivity create global signatures and vulnerabilities. DISABLE geo-location on cameras. SHUT OFF wireless (WiFI, bluetooth) search emissions.

   Smart watches can store GPS location data and emit wireless signals. SHUT OFF wireless (WiFI, bluetooth) emissions. DISABLE watch apps on phones, tablets, or computers.



Fitness trackers. Most trackers CANNOT be SHUT OFF. Batteries CANNOT be removed. Wireless transmissions CANNOT be stopped. GPS and data storage CANNOT be disabled. DISABLE the associated fitness tracker apps on phones, tablets, or computers.

Computer tablets and e-readers. Different brands (iPad, Samsung Galaxy, Amazon Fire, NOOK, Kindle, Lenovo) have different capabilities. Some emit wireless signals. Some have cellular telephone connectivity. Some have camera, data storage, and internet capability.

Inventory scanners store and upload location data and emit wireless signals.

GPS devices or commercial GPS wrist watches—are usually receive-only. However, some commercial devices track and store location data for later wireless upload. This feature must be disabled. GPS receivers can be jammed or spoofed with incorrect grids.

Commercial GPS wrist watches are more vulnerable to spoofing. The DAGR, especially when loaded with crypto, is less vulnerable to jam or spoof.

Other PED. Two-way-radios, digital cameras, camcorders, pagers, personal digital assistants (PDAs), thumb drives and other storage devices, computer peripherals, and fax machines all pose some risk to deployed units.

Notes on training

Marines need training on PED vulnerabilities. Marines have a responsibility NOT to compromise their unit. Commanders authorize emissions. Commanders restrict emissions. Vulnerabilities exist in both official government-issued PED (OPED) and personal Marine-owned PED (PPED).

In 2018, adversaries pinpointed deployed unit locations through the *Strava* fitness tracking app. In 2019, *FaceApp* gave its creators permission to access user's photo galleries with photo locations. TikTok captures users' browsing behavior, locations, and search histories.

Contributors: **KSJ**, 1 Nov 2020.

How to

REDUCE UAS EM Emissions

Purpose. To REDUCE electromagnetic emissions IOT AVOID being located and targeted.

Process for organic or DS small UAS (SUAS), co-located with, and flying ISO Marine units

1. SHUT it off. UAS are OFF while NOT being **used**.

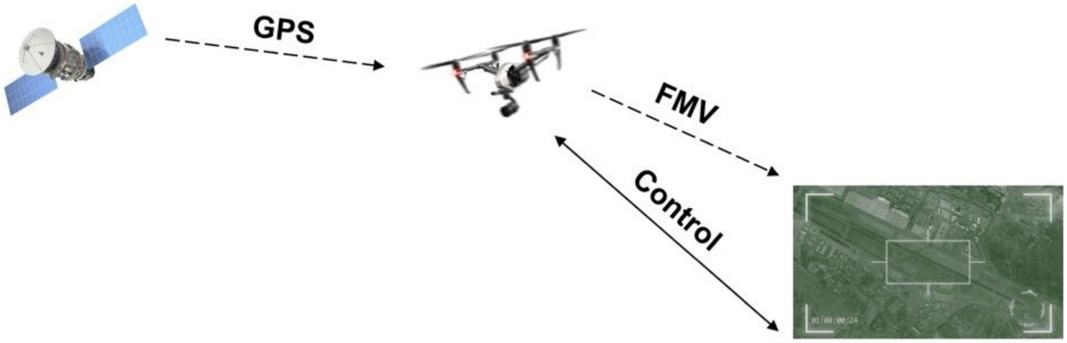
2. FLY to AVOID aircraft detection. If the enemy CANNOT hear or see the aircraft, he CANNOT cue ES DF units. The aircraft's omnidirectional RF signals CANNOT be reduced or masked without significant impacts to the operational capability of the system, but the aircraft's audio and visual signatures can.

3. LOCATE the ground controller behind buildings, woods, or hills IOT MASK EM emissions. Defilade, however, *increases* the risk of losing control of the aircraft.

   AVOID operating from cleared hilltops. Enemy DF units, tracking the omnidirectional signals from the aircraft, CANNOT determine the location of the ground controller, but they can guess the location by studying the terrain or following the aircraft back to its launch site.

   REDUCE the enemy's ability to find you. Complex urban terrain is best. AVOID flying from the CP. Alternatively, blend behind the background EM noise from the CP.

4. MOVE UAS. LAUNCH at one site, MOVE, and then recover at a separate site. Like artillery: "shoot and scoot." The ground controller can move to a new recovery site, or a patrol or adjacent unit can recover the unmanned aircraft.



SUAS have multiple send and receive emissions: GPS, control signals, and FMV, EO/IR, or other intel feeds.

Process for non-organic, Group 3, 4, and 5 UAS, operated by HHQ or supporting agencies

1. See REDUCE Radio EM Emissions.
   The complex networks that support global UAS require significant comm infrastructure, including SATCOM and SIPR CHAT links with pilots, PED, and UAS feeds. These EM emissions *increase* the risk of being located and targeted.

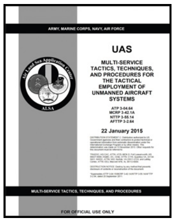
2. Fixed facilities—temporary SCIFs (T-SCIFs), SIPR networks, power grids, and concertina wire—produce EM and visual signatures that *increase* the risk of being located and targeted.

Notes

UAS GPS should always have crypto loaded to reduce vulnerability to GPS jamming. If control signals are jammed, the UAS will return to base, but if GPS is jammed, the UAS cannot return.

Temporary loss of UAS control or reception of video downlink may indicate UAS jamming.
See REPORT Electromagnetic Interference (EMI).

References



ARMY, MARINE CORPS, NAVY, AIR FORCE

UAS

MULTI-SERVICE TACTICS, TECHNIQUES, AND PROCEDURES FOR THE TACTICAL EMPLOYMENT OF UNMANNED AIRCRAFT SYSTEMS

ATP 3-04.64
MCRP 3-42.1A
NTTP 3-55.14
AFTTP 3-2.64

22 January 2015

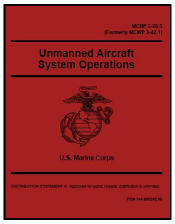
[illegible]

MULTI-SERVICE TACTICS, TECHNIQUES, AND PROCEDURES

FOR OFFICIAL USE ONLY

MCRP 3-42.1A *UAS: Multi-Service TTPs for the Tactical Employment of UAS*, 22 Jan 2015. 110 pages.

No discussion of EW, EP, or EMCON concerns or procedures for UAS.



MCRP 3-20.5
(Formerly MCWP 3-42.1)

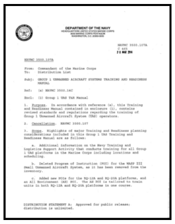
Unmanned Aircraft System Operations

U.S. Marine Corps

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

PCN 144 000242 00

MCRP 3-20.5 *Unmanned Aircraft System Operation*s, 2 May 2016.
61 pages.



DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
3000 MARINE CORPS PENTAGON
WASHINGTON, D.C. 20350-3000

NAVMC 3500.107A
C 465
26 MAR 2014

NAVMC 3500.107A

From: Commandant of the Marine Corps
To: Distribution List

Subj: GROUP 1 UNMANNED AIRCRAFT SYSTEMS TRAINING AND READINESS MANUAL

Ref: (a) NAVMC 3500.14C

Encl: (1) Group 1 UAS T&R Manual

1. Purpose. In accordance with reference (a), this Training and Readiness Manual contained in enclosure (1), contains revised standards and regulations regarding the training of Group 1 Unmanned Aircraft System (UAS) operators.

2. Cancellation. NAVMC 3500.107

3. Scope. Highlights of major Training and Readiness planning considerations included in this Group 1 UAS Training and Readiness Manual are as follows:

a. Additional information on the Navy Training and Logistics Support Activity that conducts training for all Group 1 UAS platforms in the Marine Corps including locations and scheduling.

b. Deleted Program of Instruction (POI) for the WASP III Small Unmanned Aircraft System, as it has been removed from the inventory.

c. Added new POIs for the RQ-12A and RQ-20A platforms, and an All Environment (AE) POI. The AE POI is tailored to train units in both RQ-12A and RQ-20A platforms in one course.

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

NAVMC 3500.107A *Group 1 UAS T&R Manua*l, 26 Mar 2014. 280 pages.

No discussion of EW, EP, or EMCON concerns or procedures for UAS.

Contributors: **ELK**, 1 Nov 2020.

How to

REDUCE Vehicle EM Emissions

Purpose. To REDUCE electromagnetic emissions IOT AVOID being located and targeted.

Process for Vehicles

1. SHUT it OFF. Vehicles are OFF when not being **used**.

   All vehicles emit EM signals from multiple components. When the vehicle is NOT running, the following emissions are OFF:

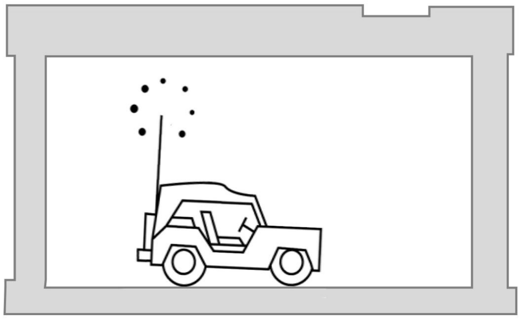
   - Starter, alternator, distributor, battery
   - Relay switches
   - Small electric motors: fans, A/C, pumps, windows, seats, windshield wipers, and others
   - Embedded vehicle computers
   - Embedded wireless (WiFi and Bluetooth) and cellular devices: car radios, keys, alarms

   Military vehicles may not have all these components, but commercial vehicles do.

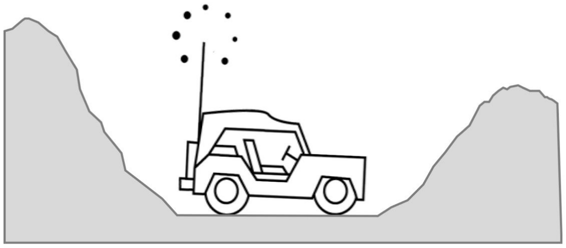
   Components that transmit even when the vehicle is OFF must be disabled or removed.

2. POSITION the vehicle behind barriers, buildings, woods, or hills IOT MASK friendly electromagnetic emissions.

   PARK behind a berm for defilade. When the vehicle is running, PARK under trees or inside buildings to mask overhead EM emissions. This also camouflages the vehicle from overhead visual and thermal observation.



Overhead masking.



Terrain masking.

3. DISPERSE into multiple small elements to AVOID creating a dense cluster of EM signals.

Process for Equipment Carried Inside the Vehicle

1. SHUT OFF Radios. See REDUCE Radio EM Emissions and MASK Antennas.

2. SHUT OFF Computers. See REDUCE Computer EM Emissions.

3. SHUT OFF Portable Electronic Devices. See REDUCE PED EM Emissions.

   Leaders must CONTROL what devices are ON and OFF inside each vehicle.

   LIMIT use of radios, computers, and PEDs only to mission-critical communications.

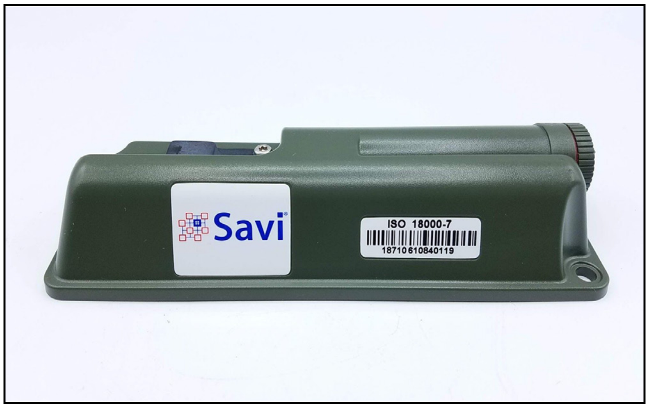
Process for RFID Tags

1. REMOVE the battery IOT SHUT it OFF.

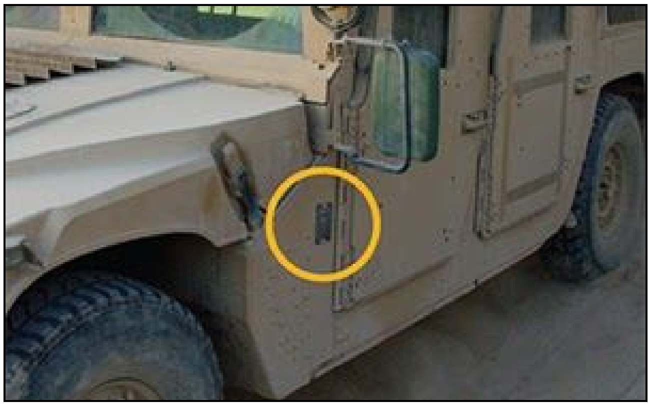
2. Or REMOVE the entire RFID tag. RFID tags emit extremely low-powered omnidirectional RF signals that may be detected and geo-located.

   Mounted on vehicles, weapons, equipment, conex boxes, pallets, and supplies, RFID tags enable logistics tracking, asset management, and maintenance programs.

   RFID tags are dormant until interrogated by a nearby powered transmitter/receiver. Realistically, it would be very difficult for an adversary to actuate an RFID tag.



RFID tag.



RFID tag mounted on a HMMWV.

Process for Blue Force Tracker (BFT), JBC-P, JCR, and Counter-IED (CREW) Systems

1. SHUT it OFF. Either adjust position reporting time (in TOOLS) to the maximums, or disable location updating completely. Turn systems ON only to manually input and transmit your location.

   Although chat messages can still be sent and received when the system is NOT reporting positions, NO messages are received when the system is completely OFF.

2. Turn CREW ON only where there is a RCIED (Radio-controlled improvised explosive device) threat. CREW jammers emit EM signals, a form of defensive EA.

Process for Electronic Logging Devices (ELD)

1. SHUT it OFF.

2. Or DISABLE or REMOVE the ELD. When contracting commercial vehicles—such as the trucks used to supply US bases, or the construction equipment used to build improvements —DISABLE or REMOVE embedded computers that transmit maintenance information to the manufacturer.

   One example is Trimble's PeopleNet, a commercial truck fleet ELD that transmits data on location, fuel consumption, stops, and driving hours.

IR Thermal Shield

A reflective mylar space blanket—stretched across the hood of a vehicle—will block IR thermal visibility. Some EM frequencies ***may*** be disrupted as well. Multiple layers of blankets create a more effective shield. Silver blankets need to be camouflaged and air must still flow to the engine.

Contributors: **GEB**, BAK, 1 Nov 2020

EP EMCON SOP

How To

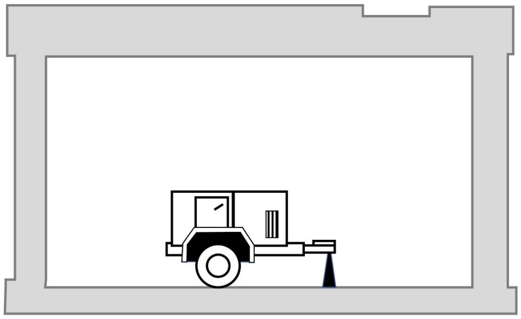
REDUCE Generator EM Emissions

Purpose. To REDUCE electromagnetic emissions IOT AVOID being located and targeted.

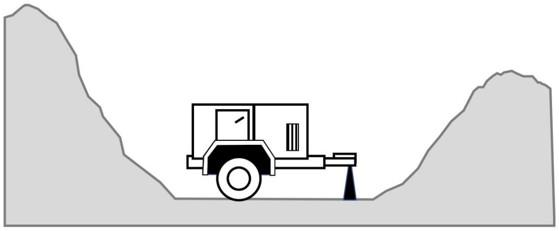
Process

1. SHUT it OFF. Generators are OFF when not being used.

2. POSITION generators behind barriers, buildings, woods, or hills IOT MASK friendly electromagnetic emissions. Or DIG a berm for generator defilade. Defilade masks EM as well as visual, audible, and IR emissions.



Overhead masking.



Terrain masking.

3. DISPERSE generators IOT AVOID creating a dense cluster of EM signals. Generators can be located 300 feet away, but dispersion makes it difficult to build a tactical microgrid.

4. COVER generators with camouflage netting to reduce some EM emissions. Netting is *multispectral*—masking generators from visual, IR thermal, and radar sensors.

5. LOAD generators to 80% capacity. This reduces EM emissions and increases life span.

6. MOVE generators.

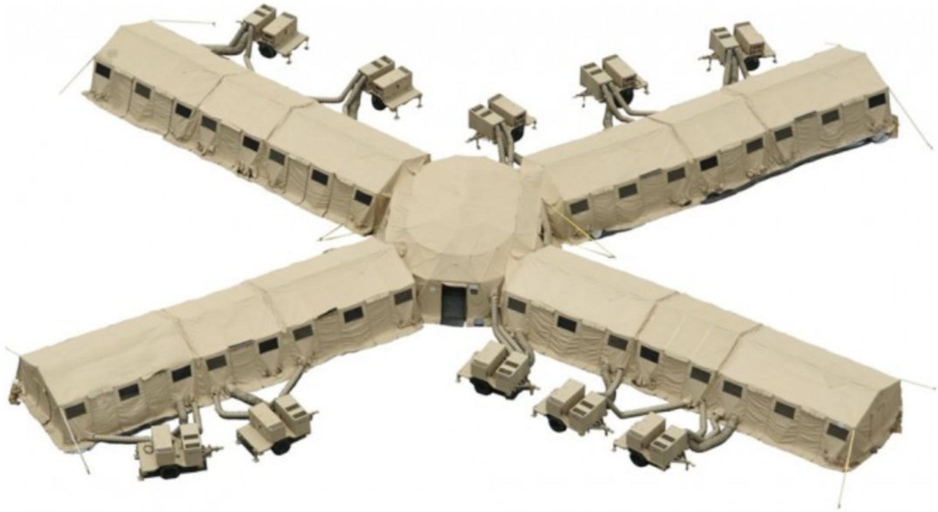
Notes

There are two methods of tactical power distribution: spot generation and microgrids. Spot generation is a single generator providing power to one or more loads. Microgrids are multiple, synchronized generators providing power to multiple loads. Tactical microgrids are more efficient, but a cluster of co-located generators emits a greater EM signature.

Try to establish power distribution centers near large pre-existing EM signatures. Urban areas, power stations, and power lines can provide EM camouflage for your electrical system. Generators are referenced by size: “a 30kW generator.”

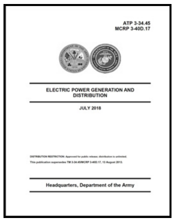
IR Thermal Shield

A reflective mylar space blanket—stretched over a generator—will block IR thermal visibility. Some EM frequencies ***may*** be disrupted as well. Multiple layers of blankets create a more effective shield. Silver blankets need to be camouflaged and air must still flow to the generator. Cardboard wrapped in tinfoil can be used over a generator as an EM shield.



Command Post of the Future (CPOF). Ten generators clustered in one location.
Source: General Dynamics.

References



ATP 3-34.45
MCRP 3-40D.17

ELECTRIC POWER GENERATION AND DISTRIBUTION

JULY 2018

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

This publication supersedes TM 3-34.45/MCRP 3-40D.17, 13 August 2013.

Headquarters, Department of the Army

MCRP 3-40D.17 *Electric Power Generation and Distribution*, 6 Jul 2018.
84 pages.

TM 3-34.46 (FM 5-424/25 June 1997)/MCRP 3-17.7K

THEATER OF OPERATIONS
ELECTRICAL SYSTEMS

May 2013

Publication of TM 3-34.46, 3 May 2013 supersedes FM 5-424, *Theater of Operations Electrical Systems*, 25 June 1997. This special conversion to the TM publishing medium/nomenclature has been accomplished to comply with TRADOC doctrine restructuring requirements. The title and content of TM 3-34.46 is identical to that of the superseded FM 5-424.

This special conversion does not integrate any changes in Army doctrine since 27 October 1997 and does not alter the publication's original references; therefore, some sources cited in this TM may no longer be current. For the status of official Department of the Army (DA) publications, consult DA Pam 25-30, *Consolidated Index of Army Publications and Blank Forms*, at http://armypubs.army.mil/2530.html. DA Pam 25-30 is updated as new and revised publications, as well as changes to publications are published. For the content/availability of specific subject matter, contact the appropriate proponent.

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

MCTP 3-17K *Theater of Operations Electrical Systems*, 3 May 2013.
268 pages.

Contributors: **GEB**, BAK, 1 Nov 2020.

How to

REDUCE Radar EM Emissions

Purpose. To REDUCE electromagnetic emissions IOT AVOID being located and targeted.

Process

1. SHUT it OFF. Radars are OFF when NOT being **used**.

2. VARY radar operation times. Radar systems that scan at the same period each day are easily detected by enemy sensors.

   For those systems with the capability, OPERATE in the ON/OFF cueing cycle, not continuously. Radars emit a great amount of power.

3. MOVE the radar system after each prolonged scanning period or when enemy aircraft have approached within 120 kilometers.

4. COORDINATE multiple radar systems to scan the same area to provide consistent, overlapping coverage, even when individual systems turn off or displace.

5. DISPERSE support vehicles, monitors, and personnel away from the radar. Antiradiation missiles (ARM) hone in on the source of radar emissions.

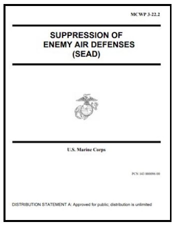
Notes

The greatest threat to radar systems are antiradiation missile missiles (ARM) from enemy aircraft. The Kh-3 missile has an operating range of 25–110 km. The YJ-91 has an operating range of 50–120 km. These missiles use GPS to guide the weapon to the last reported radar emission site, even after the radar has been turned off.

If an enemy aircraft is detected firing a missile, it must be assumed to be an ARM. Immediately shut OFF the radar and take cover. DO NOT turn the radar back on until after the radar has moved. Some missiles can loiter and then hone in again when the radar is reactivated.

AN/TPS-80 G/ATOR (Ground / Air Task-Oriented Radar).
Source: Northrop Grumman.

References



MCWP 3-22.2

SUPPRESSION OF
ENEMY AIR DEFENSES
(SEAD)

U.S. Marine Corps

PCN 143 000096 00

DISTRIBUTION STATEMENT A: Approved for public; distribution is unlimited

MCWP 3-22.2 *Suppression of Enemy Air Defenses (SEAD)*, 18 May 2001.
95 pages.

Contributors: **GEB**, 1 Nov 2020.

How To

COLLECT Own-force EM Emissions Signature

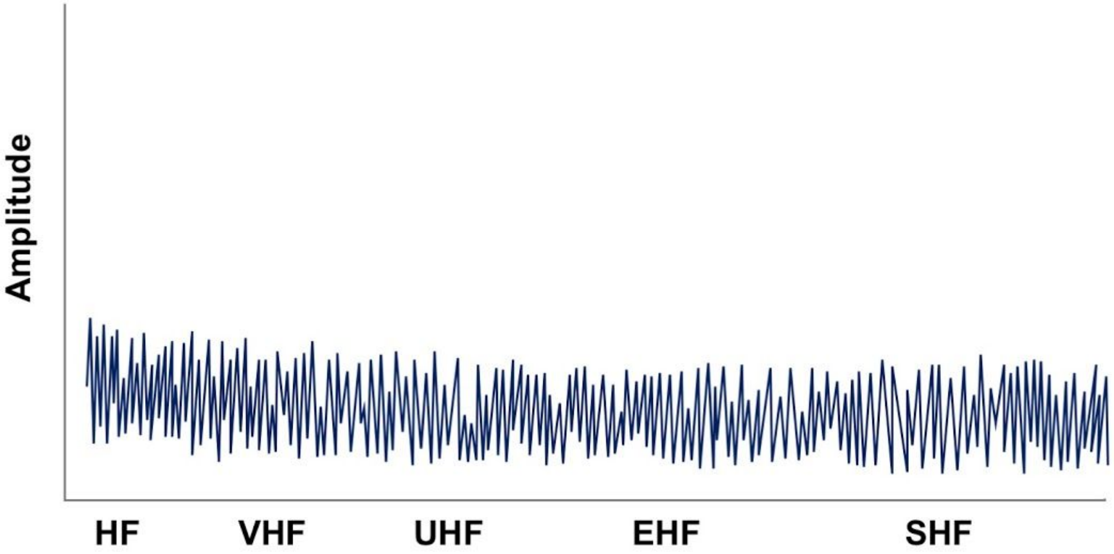
Purpose. To SEE what the adversary sees IOT IMPROVE our EP EMCON effectiveness.

Process

1. COLLECT your unit's own-force EM emissions **signature** from the adversary's point of view.

   With a spectrum analyzer, MEASURE the baseline signals in your AO.
   With a spectrum analyzer, MEASURE your unit's signals.
   Each unit S-6 needs organic own-force monitoring capability

   SCHEDULE comm windows to blend behind "normal" background signal noise.
   See SCHEDULE Less.



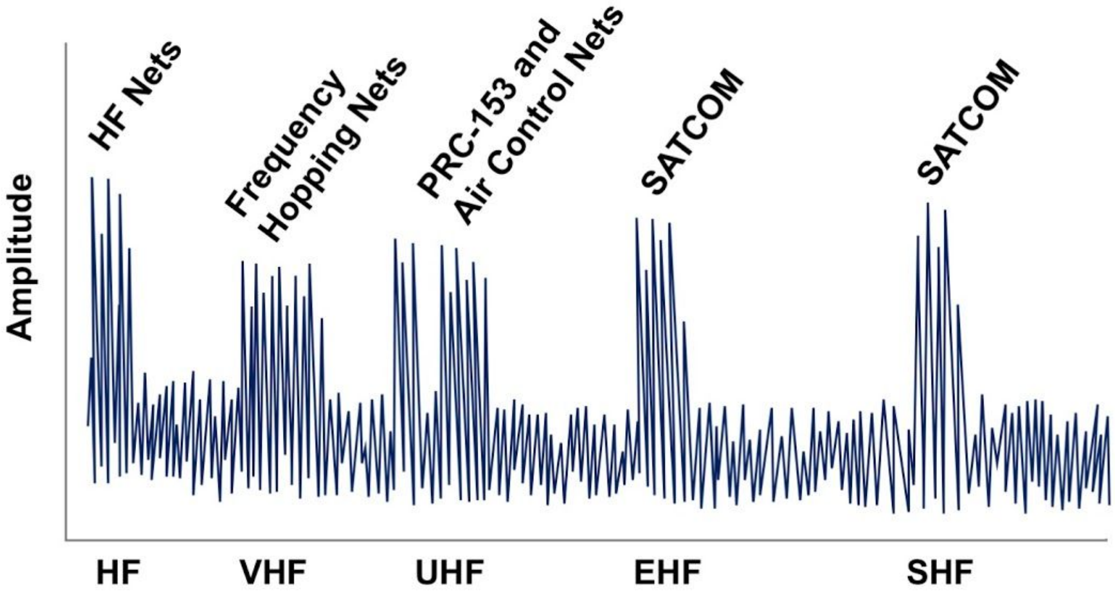
Notional EM signature with NO infantry battalion present.

2. REQUEST an EW threat vulnerability assessment from RadBn or MCIOC.

3. REQUEST a CI Threat Vulnerability Assessment (TVA) from CI/HUMINT Platoon.
   See MCRP 2-10A.2 *CI and HUMINT*.

4. ANALYZE your unit's electromagnetic signature. What are you emitting? When and why? ANALYZE your attachments' electromagnetic signatures. What are they emitting?

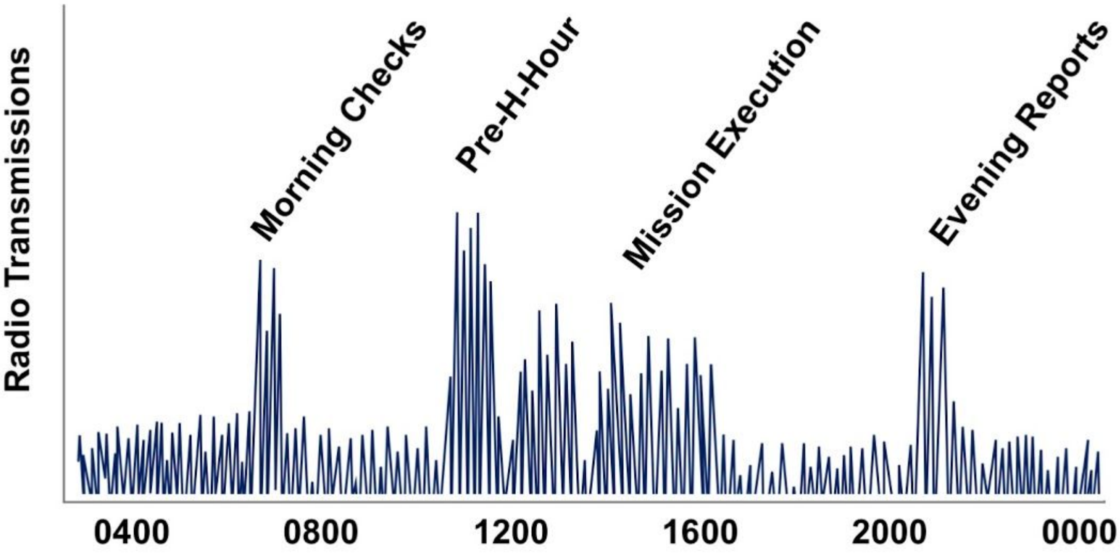
Every unit has a distinct electromagnetic signature that changes with the type of operation. An EM signature can be controlled by disciplined units.



Notional EM signature with infantry battalion present and communicating.

5. ADJUST your EP EMCON practices to REDUCE your signature. UNDERSTAND which leaders—organic and attached—control what equipment.

SCHEDULE multiple comm windows at different times daily to avoid creating a pattern. Comms usually spike just before H-hour.

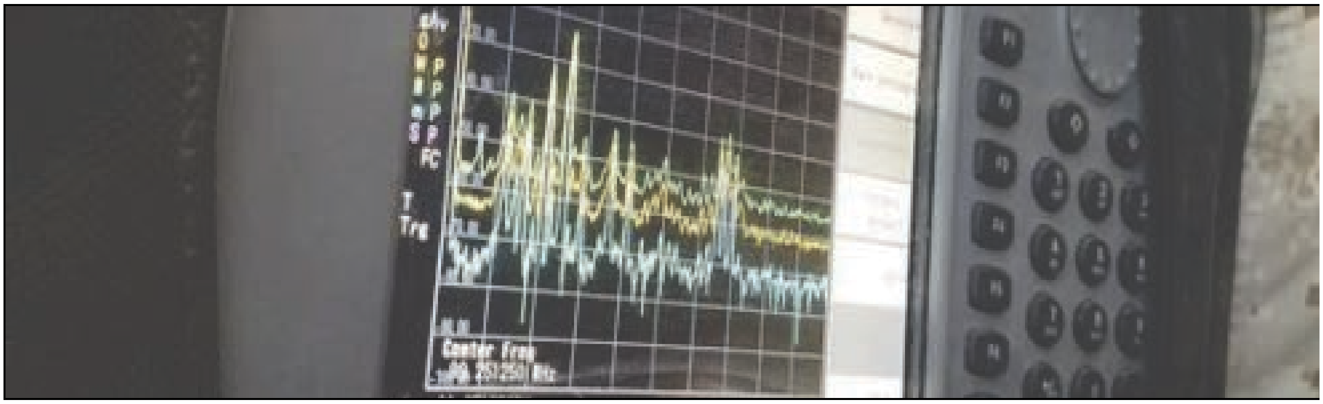


Number of notional radio transmissions throughout the day.

Notes

Units need organic own-force monitoring capability. Every battalion S-6 needs scanner capability.

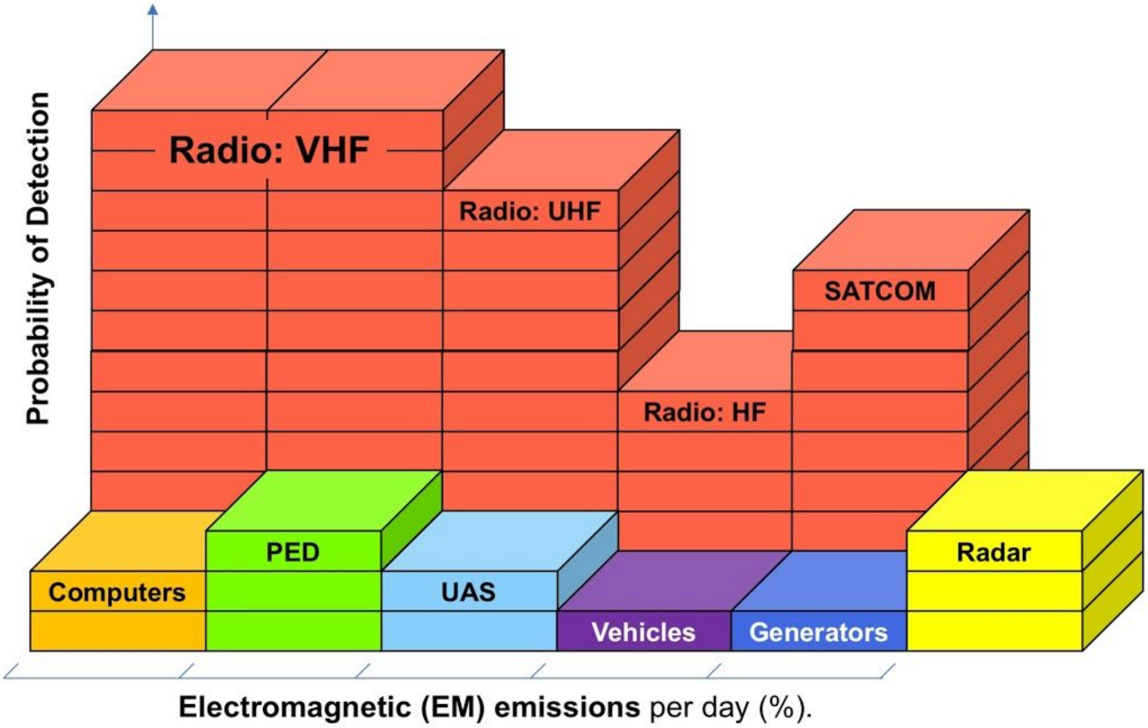
If you can't measure your own signature, you won't understand what you're emitting, and you will never improve your EMCON.



Spectrum Analyzer.

Leaders need to understand the details of their own-force EM emissions signature. In the notional infantry battalion illustration, below, each of the different-colored stacks is a different emission.

The height of each stack represents the probability of detection, a function of number of calls daily multiplied by signal strength, propagation pattern, and waveform.



EM emissions of a notional infantry battalion.

The vast majority of infantry battalion emissions are voice radio calls: VHF, UHF, HF, and SATCOM transmissions, shown in red. These are emissions most likely to be detected by the enemy. But other communications equipment—computers, portable electronic devices (PED), and UAS—as well as non-communications equipment—vehicles, generators, and radars—emit signals as well.

Commercial scanners, available on-line to Marine units as well as our adversaries, are an emerging weapon on the future battlefield.

AR-8200 Mark III Scanner.

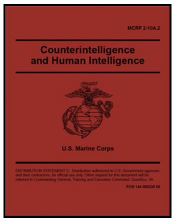
RTL-SDR.COM
QUICKSTART SETUP GUIDE: RTL-SDR.COM/QSG
DVB-T+DAB+FM+SDR
RTL2832U R820T2 TCXO+BIAS T+HF
V.3

RTL-SDR.

Sources

The notional signal illustrations re-created here were taken from an EW study conducted by MCAGCC TTECG S-2 at Twentynine Palms.

References


MCRP 2-10A.2

Counterintelligence and Human Intelligence

U.S. Marine Corps

MCRP 2-10A.2 *Counterintelligence and Human Intelligence*, 21 Nov 2019. 287 pages.

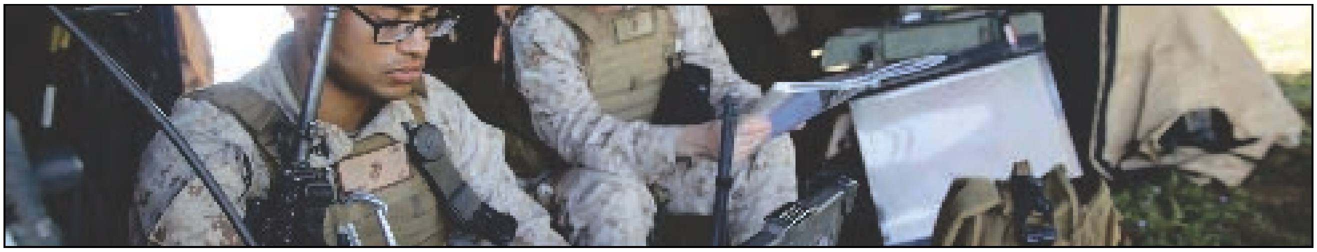
Marine CI has no history, experience, or capability to assess adversary electromagnetic reconnaissance.

Contributors: BBM, 1 Nov 2020.

How To

REPORT Electromagnetic Interference (EMI)

Purpose. To INFORM HHQ that you have been located and targeted.



Process

1. REPORT EMI to the commander. Electromagnetic interference (EMI) may be evidence of adversary ES collections and EA jamming. Your unit may have been located and targeted.

   REPORT GPS EMI.

   REPORT UAS EMI.

   REPORT SATCOM EMI.

   REPORT radio EMI affecting HF, VHF, or UHF radios.

2. REPORT EMI to HHQ. *EA is a form of enemy contact that must be reported.*
   SEND a MIJI (meaconing, intrusion, jamming, interference) report IAW SOP.

   If a radio system is being jammed, and reports cannot be sent on that net, use alternate communications means, including messengers, if necessary.

3. MOVE. EA is a strong indicator of incoming enemy fires.

4. REPORT EMI—if directed—on the (SIPR) *Joint Spectrum Interference Resolution Online* (JSIRO) system IAW CJCSM 3320.02D. Manual JSIR reports can be sent separately.

MIJI Report

1. DTG
2. UNIT
3. INTERFERENCE
4. LOCATION
5. ON TIME
6. OFF TIME
7. EFFECTS

JSIR Report

WHEN STARTED (ZULU)
AFFECTED FREQ (MHZ)
CHANNEL
LOCATION OF AFFECTED RECEIVER
COUNTRY OF AFFECTED RECEIVER
DESCRIPTION OF EMI EVENT
VICTIM POC NAME

8. FREQUENCY
9. NARRATIVE
10. AUTHENTICATION

MIJI Report Format.
Source: FM 6-99.2.

VICTIM UNIT
COCOM/SERVICE/AGENCY

JSIR Format.
Source: CJCSM 3320.02D.

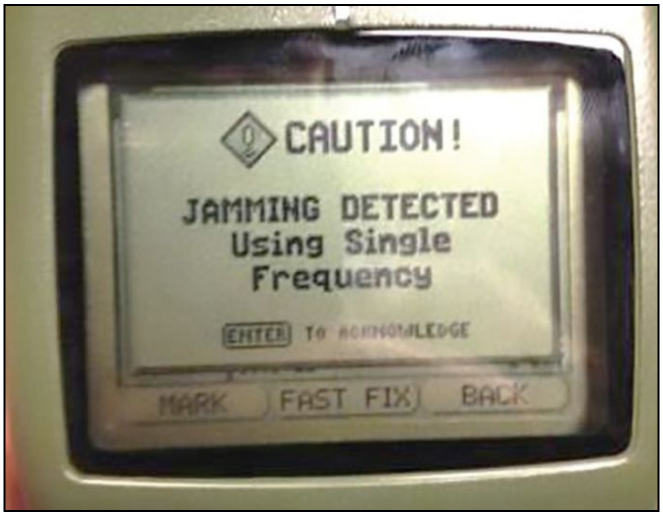
5. USE alternate equipment and nets IAW Annex K or CEOI PACE Plan.

Notes

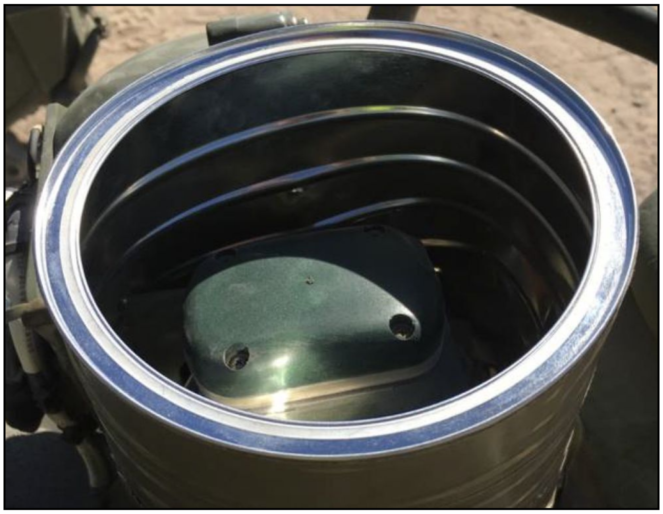
Joint Electromagnetic Spectrum Operations (JEMSO) protect and manage the electromagnetic environment. In order to act on adversary EMI, the JFC needs reporting from the field.

GPS is vulnerable to EMI. Fill DAGR with crypto to minimize this threat. The DAGR's internal software will detect and report the existence and direction of GPS EMI, even under IR scattering netting or inside buildings.

A metal can, or a hole in the ground, may be used as a shield to reduce GPS jamming.


CAUTION!
JAMMING DETECTED
Using Single
Frequency
ENTER TO ACKNOWLEDGE

DAGR EMI Message.



Field-expedient GPS shield.

UAS—which rely on GPS for PNT and rely on radio and SATCOM for communications and data relay—are particularly vulnerable to EMI.

EMI affecting satellite communications could affect the entire AOR and therefore requires a priority JSIR Report.

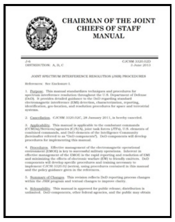
The Army Training Network (ATN) https://atn.army.mil (CAC) offers EMI training:

React to Electromagnetic Interference (EMI)	113-641-3008
React to SATCOM Electromagnetic Interference (EMI)	113-SI7E-0018
Recognize Electromagnetic Interference (EMI)	129-800-9000
Respond to Electromagnetic Interference	129-800-9001
React to Wideband Satellite EMI	11-CW-8050
React to Electromagnetic Interference	150-MC-5902

Real-World EMI

In 2016, Ukrainian forces and U.S. advisors were forced to rely on hard-wired field telephones. The frequency and effectiveness of adversary jamming prevented normal radio communications and left both their radios and cell phones unusable for hours at a time.

References



CHAIRMAN OF THE JOINT CHIEFS OF STAFF MANUAL

J-6
DISTRIBUTION: A, B, C

CJCSM 3320.02D
3 June 2013

JOINT SPECTRUM INTERFERENCE RESOLUTION (JSIR) PROCEDURES

References: See Enclosure I.

1. Purpose. This manual standardizes techniques and procedures for spectrum interference resolution throughout the U.S. Department of Defense (DoD). It provides detailed guidance to the DoD regarding standard electromagnetic interference (EMI) detection, characterization, reporting, identification, geo-location, and resolution procedures for space and terrestrial systems.

2. Cancellation. CJCSM 3320.02C, 28 January 2011, is hereby canceled.

3. Applicability. This manual is applicable to the combatant commands (CCMDs)/Services/agencies (C/S/A), joint task forces (JTFs), U.S. elements of combined commands, and DoD elements of the Intelligence Community (hereinafter referred to as "DoD components"). DoD components will develop procedures for implementing this manual.

4. Procedures. Effective management of the electromagnetic operational environment (EMOE) is key to successful military operations. Inherent in effective management of the EMOE is the rapid reporting and resolution of EMI and minimizing the effects of electronic warfare (EW) to friendly emitters. DoD components will develop specific procedures and training necessary to implement CJCSI 3320.02 (series), using procedures contained in this manual and the policy guidance given in the references.

5. Summary of Changes. This revision reflects DoD reporting process changes within the JSIR program and textual changes to improve clarity.

6. Releasability. This manual is approved for public release; distribution is unlimited. DoD components, other federal agencies, and the public may obtain

CJCSM 3320.02D *Joint Spectrum Interference Resolution (JSIR) Procedures*, 3 Jun 2013.

See also CJCSI 3320.02F *Joint Spectrum Interference Resolution*, 8 Mar 2013.

FM 6-99.2 (FM 101-5-2)

U.S. ARMY REPORT AND MESSAGE FORMATS

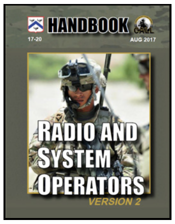
April 2007

DISTRIBUTION RESTRICTION: Approved for public release; distribution unlimited.

Headquarters Department of the Army

FM 6-99.2 *U.S. Army Report and Message Formats*, 30 Sep 2009.
288 pages.

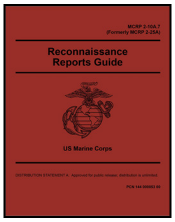
The MIJI Report format is on page 139.



HANDBOOK
17-20 AUG 2017
RADIO AND SYSTEM OPERATORS
VERSION 2

CALL 17-20 *Radio and System Operators Handbook V2*, 1 Aug 2017.
412 pages.

Appendix I includes MIJI and JSIR report formats that differ from the formats established by CJCSI 3320.02D and FM 6-99.2.



MCRP 2-10A.7
(Formerly MCRP 2-25A)

Reconnaissance Reports Guide

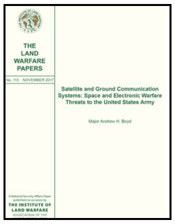
US Marine Corps

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

PCN 144 000053 00

MCRP 2-10A.7 *Reconnaissance Reports Guide*, 2 May 2016. 158 pages.

A different format for a MIJI report format is on page 103.



THE LAND WARFARE PAPERS

No. 115 NOVEMBER 2017

Satellite and Ground Communication Systems: Space and Electronic Warfare Threats to the United States Army

Major Andrew H. Boyd

A National Security Affairs Paper published on occasion by
THE INSTITUTE OF LAND WARFARE
ASSOCIATION OF THE

Andrew Boyd. *Satellite and Ground Communication Systems: Space and Electronic Warfare Threats to the United States Army.* Arlington, VA: AUSA, Nov 2017. 39 pages.

Page 17 and notes 113–115 discuss EMI and EA jamming in Ukraine.

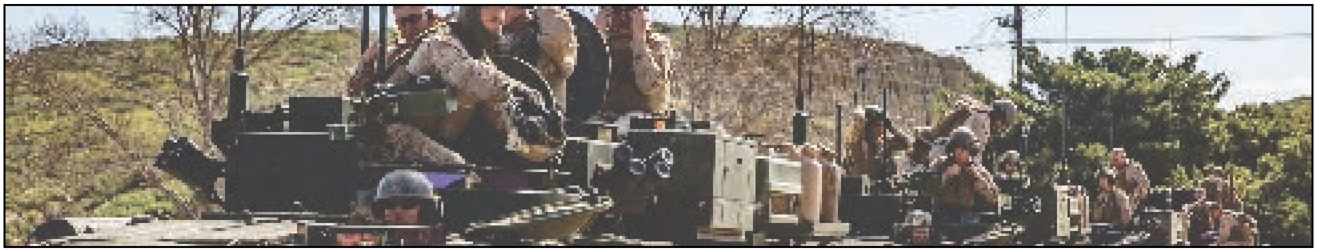
Contributors: **BBM**, 1 Nov 2020.

EP EMCON SOP

How To

REQUEST Friendly ES to FIND EN ES

Purpose. To UNDERSTAND adversary ES collections in the AO IOT take EP EMCON precautions.



Process

1. REQUEST friendly ES from HHQ.

   Friendly ES assets INTERCEPT, IDENTIFY, and LOCATE sources of electromagnetic energy. See page 1-2 of MCRP 2-10A.1 *SIGINT*, 4 Apr 2018. Historically, the infantry battalion had NO organic electromagnetic reconnaissance capability. The new Electromagnetic Warfare Support Team (EWST) may.

   The infantry battalion, with NO EA weapons, does NOT target or engage enemy emitters, but it must be aware of enemy ES collectors.

2. CONSUME HHQ intel reports of on-going adversary ES collections in the AO.

Notes

Radio reconnaissance teams build a picture of the adversary's electromagnetic order of battle (EOB) and situational awareness of the EMOE.

ES and SIGINT differ by purpose and context. Commanders task ES assets to search for local EM signals for immediate operational needs such as direction finding and targeting.

SOTA commanders task tactical SIGINT units to answer PIRs and fill intel gaps.

ES and SIGINT use the same assets and may be tasked simultaneously. See JP 3-85 *JESO*, 22 May 2020, and CJCSI 3320.01C *Joint Electromagnetic Spectrum Management Operations in the Electromagnetic Operational Environment*, 5 Feb 2019.

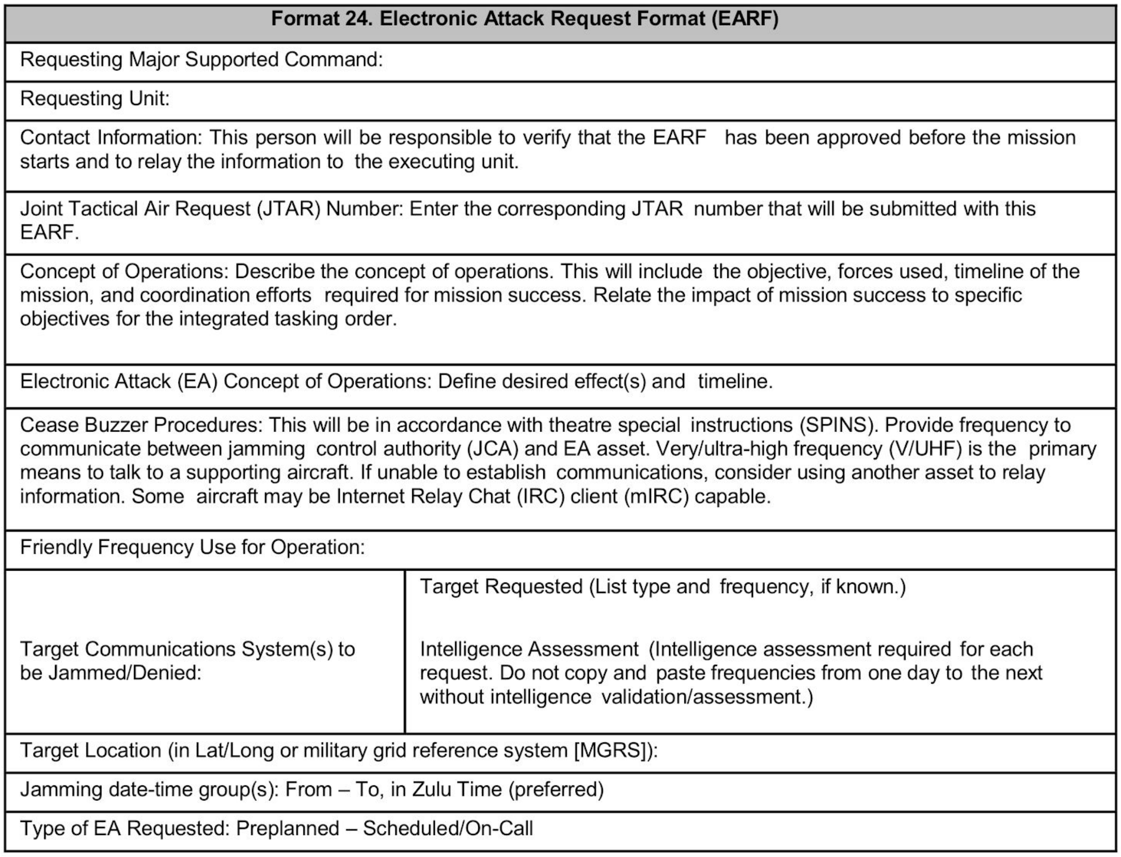
ES is primarily passive. Our ES units do NOT need to emit anything to detect the enemy. EA jamming is active and therefore can be detected by the enemy.

Contributors: TEH, BBM, 1 Nov 2020.

How To

REQUEST Friendly EA to ATTACK EN ES

Purpose. To ATTACK adversary ES collections in the AO IOT AVOID being located and targeted.



Format 24. Electronic Attack Request Format (EARF)	
Requesting Major Supported Command:	
Requesting Unit:	
Contact Information: This person will be responsible to verify that the EARF has been approved before the mission starts and to relay the information to the executing unit.	
Joint Tactical Air Request (JTAR) Number: Enter the corresponding JTAR number that will be submitted with this EARF.	
Concept of Operations: Describe the concept of operations. This will include the objective, forces used, timeline of the mission, and coordination efforts required for mission success. Relate the impact of mission success to specific objectives for the integrated tasking order.	
Electronic Attack (EA) Concept of Operations: Define desired effect(s) and timeline.	
Cease Buzzer Procedures: This will be in accordance with theatre special instructions (SPINS). Provide frequency to communicate between jamming control authority (JCA) and EA asset. Very/ultra-high frequency (V/UHF) is the primary means to talk to a supporting aircraft. If unable to establish communications, consider using another asset to relay information. Some aircraft may be Internet Relay Chat (IRC) client (mIRC) capable.	
Friendly Frequency Use for Operation:	
Target Communications System(s) to be Jammed/Denied:	Target Requested (List type and frequency, if known.) Intelligence Assessment (Intelligence assessment required for each request. Do not copy and paste frequencies from one day to the next without intelligence validation/assessment.)
Target Location (in Lat/Long or military grid reference system [MGRS]):	
Jamming date-time group(s): From – To, in Zulu Time (preferred)	
Type of EA Requested: Preplanned – Scheduled/On-Call	

EARF Format. **Source:** Table D-1 of FM 3-12 *Cyberspace and Electronic Warfare Operations*, 11 Apr 2017. Other EARF formats can be found on Table 50 of MCRP 3-31.6 *JFIRE: Multi-Service TTPs for Joint Application of Firepower*, 18 Oct 2018, and on pages 90–93 of FM 6-99.2 *U.S. Army Report and Message Formats*, 30 Sep 2009.

Process

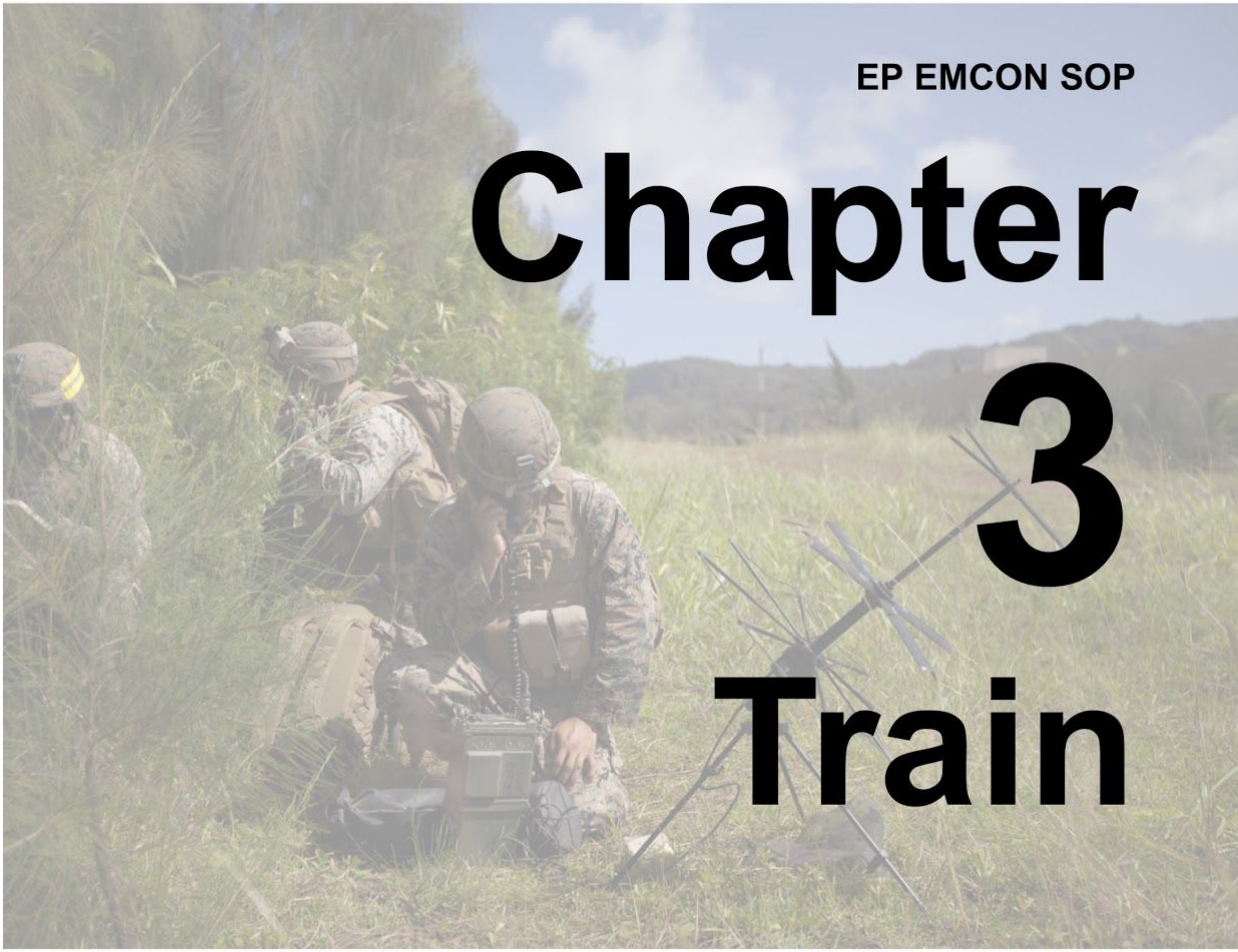
1. REQUEST friendly EA from HHQ IAW SOP. See Electronic Attack Request Format (EARF).

   Friendly EA units TARGET, ENGAGE, and ASSESS enemy EW. Historically, the infantry battalion has NO organic EA capability. The new EWST may.

2. PLAN operations to coincide with friendly EA windows. Coordinate with RadBn.

   Friendly EA is jamming or intruding on enemy nets to disrupt capabilities. In most cases, these effects are temporary. Defensive EA, which denies the enemy the ability to target, guide, or trigger weapons, is often mistakenly called EP. See JP 3-85 *JESO*, 22 May 2020.

Contributors: **BBM**, 1 Nov 2020.



EP EMCON SOP

Chapter 3 Train

In this Chapter

- EP EMCON training standards
- EP EMCON training

Marine Corps Intelligence Schools
Intelligence Training Enhancement Program

SIGMAN EP EMCON SOP:
Chapter 3: Train

Marine Corps Intelligence Schools (MCIS)
Intelligence Training Enhancement Program (ITEP)

Train

SET EP EMCON Training Standards

Purpose. To REDUCE electromagnetic emissions IOT AVOID being located and targeted.

Individual Training Standards

1. Individual training standards for communications equipment are published in the NAVMC 3500.56C *Communications T&R Manual*.

2. For training on comm equipment, see the *CTB Communications Handbook*, 7 Feb 2020.

Collective Training Standards

1. Collective training standards for EP EMCON procedures are defined by unit SOP.

   Other tasks, "MOVE the CP in less than two hours," support EP EMCON standards.

2. The overall collective task is "EP 1001: AVOID being located and targeted by the adversary."

EP-1001:	**AVOID being located and targeted by the adversary.**
SUPPORTED MET(S):	
EVALUATION-CODED:	YES
SUSTAINMENT INTERVAL:	6 months
DESCRIPTION:	The battalion operates in the field, transitioning from a defensive task to an offensive task, and directing all of its subordinate elements.
CONDITION:	In the field, given (2) day-long missions: "Establish a BP IOT block a corridor," and "ATK OBJ (village) IOT clear corridor for FOF," the battalion plans, moves, and executes under EMCON conditions.
STANDARD:	Adversary collections are unable to target battalion headquarters within 1000m. Adversary collections are unable to target company positions or convoys within 1000m. Adversary collection-to-engagement timeline is notionally assumed to be 120 minutes.

EVENT COMPONENTS:

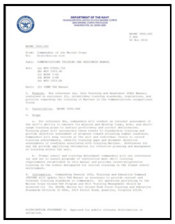
1. PLAN and BRIEF operations
2. ESTABLISH BP
3. PLAN (notional) fires, R&S, patrols, and passage of lines
4. CONDUCT movement to contact, deliberate ATK, and consolidation
5. PLAN (notional) fires, R&S, and MEDEVAC

REFERENCES: *EP EMCON SOP*

CHAINED EVENTS:

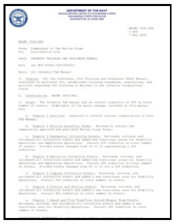
MISCELLANEOUS: Simulated adversary EW collections are needed to evaluate this task. Artillery, Engineer, LAR, or assault support increase unit signatures.

References



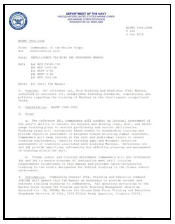
NAVMC 3500.56C *Communications T&R Manual*, 2 Nov 2016.
213 pages.

ZERO mention of EW, EP, or EMCON procedures.



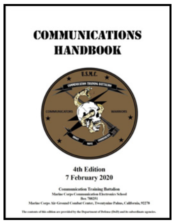
NAVMC 3500.44D *Infantry T&R Manual*, 7 May 2020.
768 pages.

ZERO mention of EMCON or radio procedures.
Just generic "Operate HF radio," "Operate VHF radio," and "Operate UHF radio."



NAVMC 3500.100B *Intelligence T&R Manual*, 6 Jun 2016.
601 pages.

ZERO mention of EMCON or radio procedures.
Just "Provide intel support to EW," which includes EP.



COMMUNICATIONS
HANDBOOK

4th Edition
7 February 2020

Communication Training Battalion
Marine Corps Communication Electronics School
Box 788251
Marine Corps Air-Ground Combat Center, Twentynine Palms, California, 92278

The contents of this edition are provided by the Department of Defense (DoD) and its subordinate agencies.

CTB Communications Handbook, 4th Edition. MCAGCC, CA: MCCES CTB,
7 Feb 2020. 232 pages.

Contributors: **BBM**, 1 Nov 2020.

Train

CONDUCT EP EMCON Training

Purpose. To REDUCE electromagnetic emissions IOT AVOID being located and targeted.

Process

1. CONDUCT individual **training**.

   Marines need to train on dozens of individual **skills**, especially radio equipment skills, chat, vehicle, and signal skills, to support EP EMCON SOPs.
   Marines need to train on radio **procedures** that support EP EMCON SOPs.

   Marines should UNDERSTAND adversary electromagnetic support (ES) collections.
   Marines should UNDERSTAND friendly electromagnetic emissions signatures.

2. CONDUCT team **training** on drills and tactical SOPs-—under EMCON restrictions.
   Every tactical evolution should be able to be executed at multiple EMCON levels.

   For each drill, TRAIN on the **authorized radio calls** at different EMCON levels.
   For each drill, TRAIN on the **alternative signals** when radio calls are NOT authorized.
   See EP EMCON Matrix SOP.

3. During a scheduled field exercise, exercise EMCON as an added task.

   SCHEDULE a six-hour block of time for the unit to move up one EMCON level. If EMCON 2 is the desired standard for operations, move up to EMCON 3.

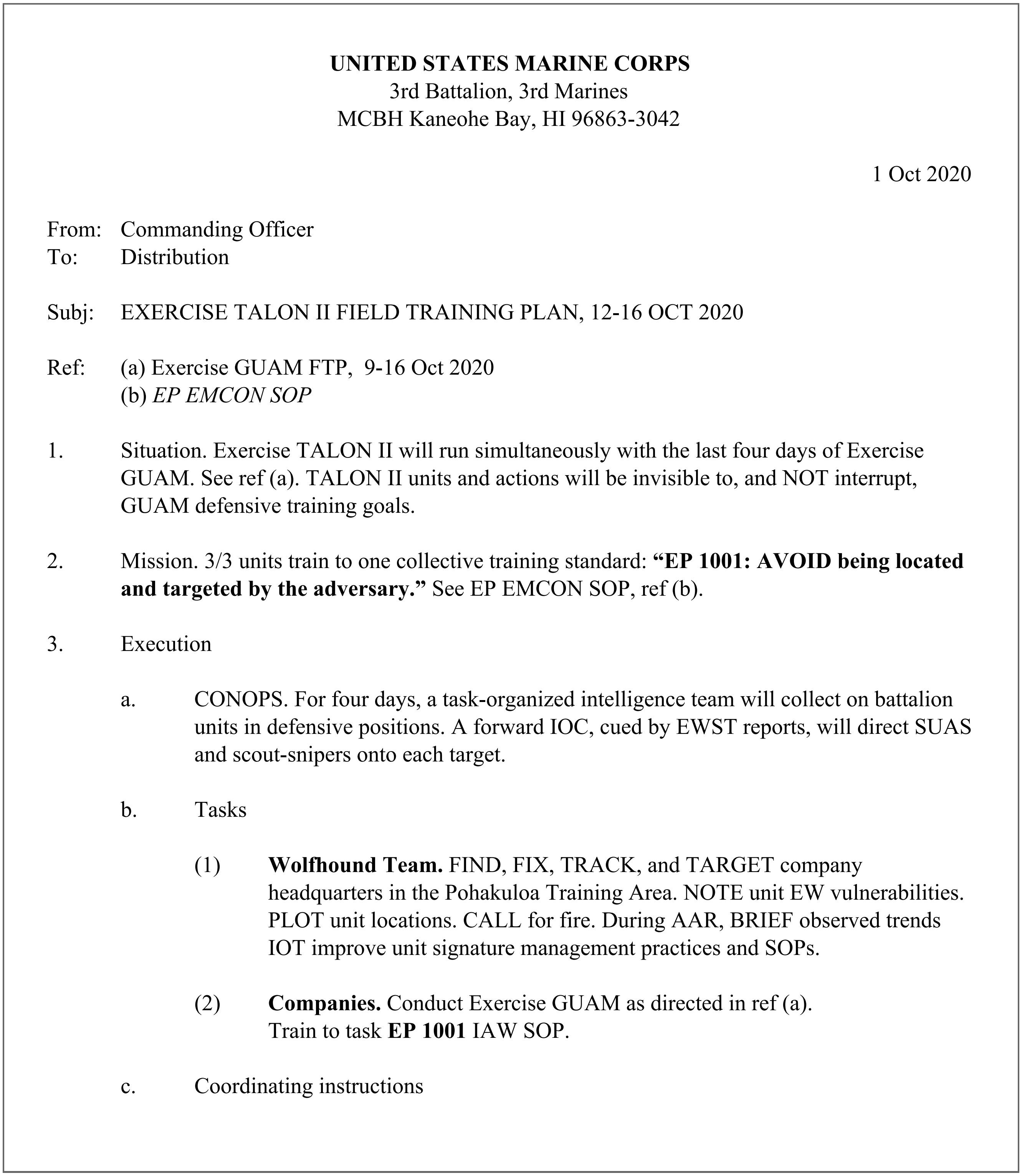
SNOOZE brevity code transmission	Notes
"All stations. As briefed, SNOOZE from sixteen-hundred to twenty-two hundred, OVER."	Set an EMCON block from 1600–2200. SNOOZE is "initiate EMCON procedures."

Limited radio checks, limited HHQ RFIs, and limited reports train a unit on EMCON SOPs and alternative comm options. ASSIGN someone to monitor nets for EMCON compliance:

ZIPLIP brevity code transmission	Notes
"2-3. ZIPLIP, OVER."	Shut up. ZIPLIP is a reminder to "limit transmissions to critical information only."

4. During a field exercise, COLLECT on your own units IOT EVALUATE EP EMCON practices.

   ASSIGN an intelligence team with EW collections capabilities to FIND, FIX, TRACK, and TARGET your units. Unit commanders need to know they are being watched and heard. See the field training plan below.



UNITED STATES MARINE CORPS
3rd Battalion, 3rd Marines
MCBH Kaneohe Bay, HI 96863-3042

1 Oct 2020

From: Commanding Officer
To: Distribution

Subj: EXERCISE TALON II FIELD TRAINING PLAN, 12-16 OCT 2020

Ref: (a) Exercise GUAM FTP, 9-16 Oct 2020
(b) *EP EMCON SOP*

1. Situation. Exercise TALON II will run simultaneously with the last four days of Exercise GUAM. See ref (a). TALON II units and actions will be invisible to, and NOT interrupt, GUAM defensive training goals.

2. Mission. 3/3 units train to one collective training standard: **“EP 1001: AVOID being located and targeted by the adversary.”** See EP EMCON SOP, ref (b).

3. Execution

   a. CONOPS. For four days, a task-organized intelligence team will collect on battalion units in defensive positions. A forward IOC, cued by EWST reports, will direct SUAS and scout-snipers onto each target.

   b. Tasks

      (1) **Wolfhound Team.** FIND, FIX, TRACK, and TARGET company headquarters in the Pohakuloa Training Area. NOTE unit EW vulnerabilities. PLOT unit locations. CALL for fire. During AAR, BRIEF observed trends IOT improve unit signature management practices and SOPs.

      (2) **Companies.** Conduct Exercise GUAM as directed in ref (a).
      Train to task **EP 1001** IAW SOP.

   c. Coordinating instructions

(1) Task Organization. Wolfhound Team, under the S-2, is activated at 0800 on 11 Oct 2020.

Marines (38): IOC (7), EWST (6), SUAS (7), and Scout-Sniper Platoon with SARC (18).

Equipment: (3) HMMWV, (1) CESAS HMMWV, (1) RQ-11B Raven, (1) RQ-20 Puma.

(2) Schedule. 11 Oct. 0800. Task-organize Wolfhound Team. Plan operations.

12-15 Oct. Collect on each company for approximately 30 hours each.

15 Oct. 2400. ENDEX for both Exercise GUAM and TALON II.

16 Oct. 1100. Exercise AAR.

(3) For realism, the Wolfhound Team cannot know Exercise GUAM unit sectors, positions, or details.

(4) RadBn will request FAA permission to jam friendly radios IOT increase collections vulnerabilities.

(5) SUAS are FMV only, NO EW capability. In addition to intelligence reporting, the Wolfhound team will submit actual SUAS and sniper calls for fire to exercise control for record-keeping purposes.

4. Command and Signal IAW Exercise GUAM CEOI. Wolfhound Team reports to XO on exercise control net.

5. Admin and Logistics. The Wolfhound Team will be supported by, and report to, battalion exercise control HQ.

Notes

Adversary collections threats should be integrating into ALL training. Without a threat, Marines learn noisy EM habits.

An EMCON drill can be scheduled at a set time each day while deployed. The number of hours can be increased as units gain experience.

Any use of EMCOM 4 must be carefully coordinated. Once units are blacked out, they cannot be contacted except by messenger. The planned end time for the blackout must be emphasized.

All EMCON training should include own-force monitoring. See COLLECT Own-force EM Emissions Signature.

Training without SATCOM is valuable, but when we reduce our dependence on SATCOM, we may actually *increase* our vulnerability to adversary DF.

Attachments are a challenge. When a new unit is attached, EMCON SOPs must be emphasized.

Contributors: **BBM**, 1 Nov 2020.

How to

TRAIN on Radios

Purpose. To REDUCE electromagnetic emissions IOT AVOID being located and targeted.

Process

1. TRAIN to MAXIMIZE the use and MINIMIZE the vulnerability of each radio.

   KNOW your tools. TRAIN to set power levels. TRAIN to use crypto. TRAIN to change nets. TRAIN to mask antennas. TRAIN to use vehicle-mounted radios.
   UNDERSTAND capabilities and vulnerabilities of each radio IOT make EMCON decisions.
   READ the manual. TRAIN on the *CTB Communications Handbook*, 7 Feb 2020.

2. TRAIN to chat on multiple platforms IOT REDUCE radio calls.

3. TRAIN to read the CEOI, PACE plan, and EMCON matrix. TRAIN on terms and technology.

4. TRAIN on EP EMCON procedures for radios. See REDUCE Radio EM Emissions, TALK Less, SCHEDULE Less, MOVE, CHAT, SIGNAL, WIRE, MASK Antennas, REDUCE Power, Prioritize LPD Nets, and PLAN Simple Flexible Ops.

PRC-117F

PRC-117G

PRC-150

PRC-152

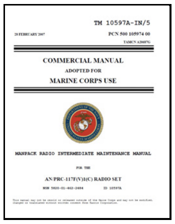
Notes on radio capabilities. *For Marine leaders, knowing the precise details of radio operations is more critical now than it has ever been.* Ask questions. Practice. READ the manual.

System	Frequency Band						Multi-Band Radio	Freq Range	Features
	HF 2-30 MHz	**VHF** 3-300 MHz		**UHF** 300-3000 MHz					
	LOS **BLOS**	**LOS**		**LOS**		**BLOS**			
		AM	FM	AM	FM	SATCOM			
PRC-113		○		○			YES	116.000-399.975 MHz	Voice: VHF/UHF AM mode used by FACs for LOS air to ground comm.
PRC-117F		○	○	○	○	○	YES	30.000-512.000 MHz	Voice and data: SINCGARS, VHF/UHF LOS in AM and FM, HQ II, and SATCOM.
PRC-117G		○	○	○	○	○	YES	30.000-2.000 GHz	Voice and data: SINCGARS, HQ II, VHF/UHF AM and FM, ANW2, and SATCOM.
PRC-148		○	○	○	○		YES	30.000-512.00 MHz	Voice and data: HQ I/II, SINCGARS ESIP in SC or FH, and analog.
PRC-150	○						NO	1.600-60.000 MHz	Voice and data: HF ALE.
PRC-152		○	○	○	○	○	YES	30.000-512.000 MHz and 762-870 MHz	Voice and data: SINCGARS, VHF/UHF in AM and FM, HQ II, and SATCOM.
PRC-153				○	○		NO	380.000-470.000 MHz	Voice radio: short distances. Primarily used by Marines.

Source: Table 47 of MCRP 3-30B.3 *Tac Radios*, 19 May 2017.

Radio Manuals

PRC-117F


TM 10597A-IN/5
28 FEBRUARY 2007
PCN 500 105974 00
[illegible]

COMMERCIAL MANUAL
ADOPTED FOR
MARINE CORPS USE

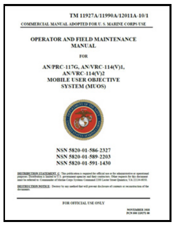
MANPACK RADIO INTERMEDIATE MAINTENANCE MANUAL
FOR THE
AN/PRC-117F(V)1(C) RADIO SET
NSN 5820-01-462-2484 ID 10597A

This manual may not be resold or released outside of the Marine Corps and may not be modified, changed or translated without written consent from Harris Corporation.

Marine: TM 10597A-IN/5 *Manpack Radio Intermediate* ***Maintenance Manual*** *for the AN/****PRC-117F****(V)1(C) Radio Set*, 28 Feb 2007. 138 pages.

Army: TM 11-5820-1407-13&P *Technical Manual* **Operator and Field Maintenance Manual** *Including Repair Parts and Special Tools List for Radio Sets AN/****PRC-117F****(V)2(C) (NSN 5820-01-580-2575)(EIC 6HP) AN/VRC-103(V)3 (NSN 5820-01-579-0420)(EIC 6HS), AN/TRC-223(C) (NSN 5820-01-579-0476)(EIC 6HU),* 15 Apr 2015.

PRC-117G


TM 11927A/11990A/12011A-10/1
COMMERCIAL MANUAL ADOPTED FOR U. S. MARINE CORPS USE

OPERATOR AND FIELD MAINTENANCE MANUAL
FOR
AN/PRC-117G, AN/VRC-114(V)1,
AN/VRC-114(V)2
MOBILE USER OBJECTIVE
SYSTEM (MUOS)

NSN 5820-01-586-2327
NSN 5820-01-589-2203
NSN 5820-01-591-1430

DISTRIBUTION STATEMENT C: This publication is required for official use or for administrative or operational purposes. Distribution is limited to U.S. government agencies and their contractors. Other requests for this document must be referred to: Commander of Marine Corps Systems Command 2200 Lester Street Quantico, VA 22134-6050.

DESTRUCTION NOTICE: Destroy by any method that will prevent disclosure of contents or reconstruction of the documents.

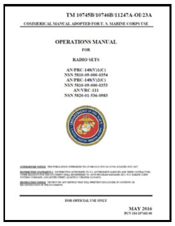
FOR OFFICIAL USE ONLY

NOVEMBER 2018
PCN [illegible]

Marine: TM 11927A/11990A/12011A-10/1 ***Operator and Field Manual*** *for AN/****PRC-117G****, AN/VRC-114(V)1, AN/VRC-114(V)2 Mobile User Objective System (MUOS),* 30 Nov 2018. 107 pages.

Army: TM 11-5820-1408-13&P *Technical Manual* **Operator and Field Maintenance Manual** *Including Repair Parts and Special Tools List for Multiband Manpack Radio AN/****PRC-117G****(V)4(C) (NSN 5820-01-579-0452)(EIC 7EA) Vehicular System AN/VRC-114(V)3 (NSN 5820-01-579-0432)(EIC 7EB) Transit Case System AN/TRC-227(V)1 (NSN 5820-01-579-0466)(EIC 7EH),* 15 Apr 2015*.*

PRC-148


TM 10745B/10746B/11247A-OI/23A
COMMERICAL MANUAL ADOPTED FOR U. S. MARINE CORPS USE

OPERATIONS MANUAL
FOR
RADIO SETS
AN/PRC-148(V)1(C)
NSN 5810-09-000-0354
AN/PRC-148(V)2(C)
NSN 5810-09-000-0353
AN/VRC-111
NSN 5820-01-536-0983

SUPERSEDURE NOTICE: [illegible]

DISTRIBUTION STATEMENT C: [illegible]

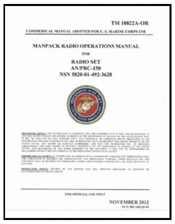
DESTRUCTION NOTICE: DESTROY BY ANY METHOD THAT WILL PREVENT DISCLOSURE OF CONTENTS OR RECONSTRUCTION OF THE DOCUMENTS.

FOR OFFICIAL USE ONLY

MAY 2016
PCN [illegible]

Marine: TM 10745B/10746B/11247A-OI/23A ***Operations Manual for Radio Sets*** *AN/****PRC-148****(V)1(C) (NSN 5810-09-000-0354), AN/PRC-148(V)2(C) (NSN 5810-09-000-0353), AN/VRC-111 (NSN 5820-01-536-0983)*, 31 May 2016. 300 pages.

PRC-150


TM 10822A-OR
COMMERICAL MANUAL ADOPTED FOR U. S. MARINE CORPS USE

MANPACK RADIO OPERATIONS MANUAL
FOR
RADIO SET
AN/PRC-150
NSN 5820-01-492-3628

DISCLOSURE NOTICE: [illegible]

DISTRIBUTION STATEMENT C: [illegible]

DESTRUCTION NOTICE: DESTROY BY ANY METHOD THAT WILL PREVENT DISCLOSURE OF CONTENTS OR RECONSTRUCTION OF THE DOCUMENTS.

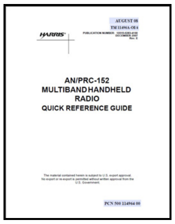
FOR OFFICIAL USE ONLY

NOVEMBER 2012
PCN [illegible]

Marine: TM 100822A-OR ***Manpack Radio Operations Manual for Radio Set*** *AN/****PRC-150*** *(NSN 5820-01-492-3628)*, 30 Nov 2012. 301 pages.

Army: TM 11-5820-1501-13&P ***Operator and Field Maintenance Manual*** *Including Repair Parts and Special Tools List* ***for Advanced Tactical HF Radio*** *AN/****PRC-150****A(C) (NSN: 5820-01-575-6358)(EIC: 6GK); 20-Watt Vehicular System AN/VRC-104(V)5 (NSN: 5820-01-575-9257)(EIC: 6GM); 150-Watt Vehicular System AN/VRC-104(V)6 (NSN: 5820-01-575-9305)(EIC: 6GN); 150-Watt Base Station System AN/TRC-209B(C) (NSN: 5820-01-575-9287)(EIC: 6GS); 400-Watt Base Station System AN/TRC-210(V)3 (NSN: 5820-01-575-9263)(EIC: 6GT),* 15 May 2013*.*

PRC-152


AUGUST 08
TM 11496A-OI/4
HARRIS
PUBLICATION NUMBER: [illegible]
DECEMBER 2007
Rev. E

AN/PRC-152
MULTIBAND HANDHELD
RADIO
QUICK REFERENCE GUIDE

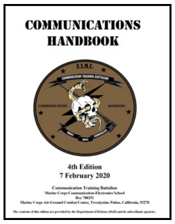
The material contained herein is subject to U.S. export approval. No export or re-export is permitted without written approval from the U.S. Government.

PCN 500 114964 00

Marine: TM 11496A-OI/4 *AN/****PRC-152*** *Multiband Handheld Radio* ***Quick Reference Guide***, 1 Aug 2008. 252 pages.

Army: TM 11-5820-1500-13&P *Technical Manual* **Operator and Field Maintenance Manual** *Including Repair Parts and Special Tools List for Radio Sets AN/****PRC-152****(V)1 (NSN 5820-01-566-0746)(EIC 6KD), AN/VRC-110(V)1 (NSN 5820-01-578-8805)(EIC 6LE) AN/VRC-110(V)2 (NSN 5820-01-579-4483)(EIC 6LF),* 15 Apr 2015*.*

Radio Handbooks



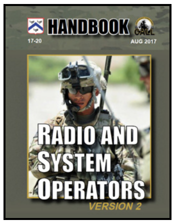
COMMUNICATIONS HANDBOOK

4th Edition
7 February 2020

Communication Training Battalion
Marine Corps Communication-Electronics School
Box 788251
Marine Corps Air-Ground Combat Center, Twentynine Palms, California, 92278

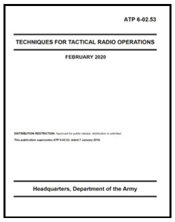
The contents of this edition are provided by the Department of Defense (DoD) and its subordinate agencies.

CTB Communications Handbook, 4th Edition. MCAGCC, CA: MCCES CTB, 7 Feb 2020. 232 pages.



HANDBOOK
17-20
AUG 2017
RADIO AND SYSTEM OPERATORS
VERSION 2

CALL 17-20 *Radio and System Operators Handbook V2*, 1 Aug 2017.
412 pages.



ATP 6-02.53

TECHNIQUES FOR TACTICAL RADIO OPERATIONS

FEBRUARY 2020

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

This publication supersedes ATP 6-02.53, dated 7 January 2016.

Headquarters, Department of the Army

ATP 6-02.53 *Techniques for Tactical Radio Operations*, 13 Feb 2020.
218 pages.

ARMY, MARINE CORPS, NAVY, AIR FORCE

TAC RADIOS

MULTI-SERVICE
TACTICS, TECHNIQUES,
AND PROCEDURES FOR
TACTICAL RADIOS

ATP 6-02.72
MCRP 3-30B.3 [MCRP 3-40.3A]
NTTP 6-02.2
AFTTP 3-2.18

MAY 2017

MULTI-SERVICE TACTICS, TECHNIQUES, AND PROCEDURES

MCRP 3-30B.3 *Tac Radios: Multi-Service TTPs for Tactical Radios*, 19 May 2017.
200 pages.

Notes on BFT / JBC-P / JCR

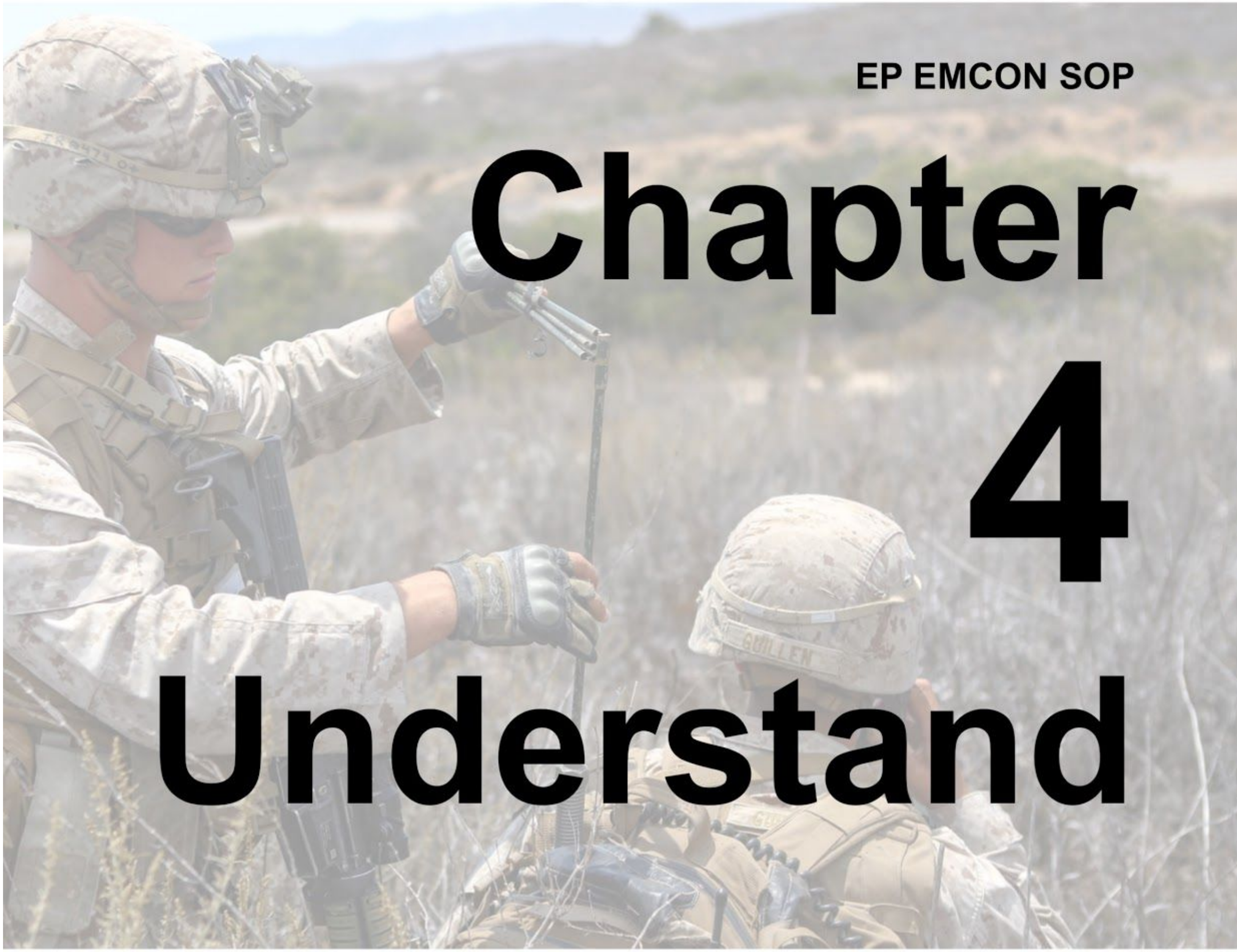
BFT / JBC-P / JCR position reporting systems are a significant vulnerability because they are *continuous emitters*. GPS satellites continuously transmit signals to a joint friendly force tracking (JFFT) device, which then transmits its position information—omni-directionaly—to an overhead communications satellite. The satellite downlink transmits position data to a ground station which collects all unit locations. The ground station then disseminates unit positions to all command posts through a distributed C2 system.

Notes on SATCOM

Understand SATCOM strengths and vulnerabilities. The signal from the ground to the satellite is the **uplink**. The signal from the satellite is the **downlink**. The downlink creates a footprint on the earth's surface. Satellite bands—L, S, C, X, Ku, K, Ka, and V—are grouped into three blocks:

- UHF narrowband: MUOS and UFO, INMARSAT, GPS and JBC-P, PSC-5 and Iridium.
- SHF wideband: WGS SATCOM and DSCS, WIN-T, TROJAN SPIRIT.
- EHF protected: AEHF and MILSTAR, GBS, SMART-T.

Contributors: **BBM,** 1 Nov 2020.



EP EMCON SOP

Chapter 4 Understand

In this Chapter

- Understanding adversary ES collections capabilities
- Understanding friendly EW doctrine

Marine Corps Intelligence Schools
Intelligence Training Enhancement Program

SIGMAN EP EMCON SOP:
Chapter 4: Understand

Marine Corps Intelligence Schools (MCIS)
Intelligence Training Enhancement Program (ITEP)

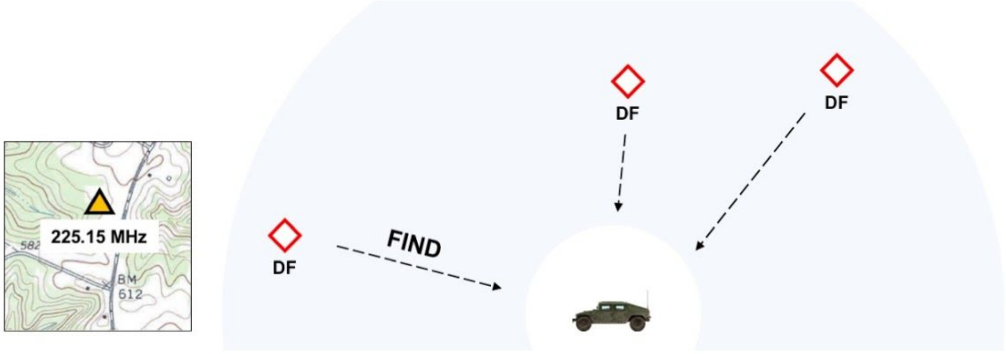
Understand

Adversary ES Collections Capabilities

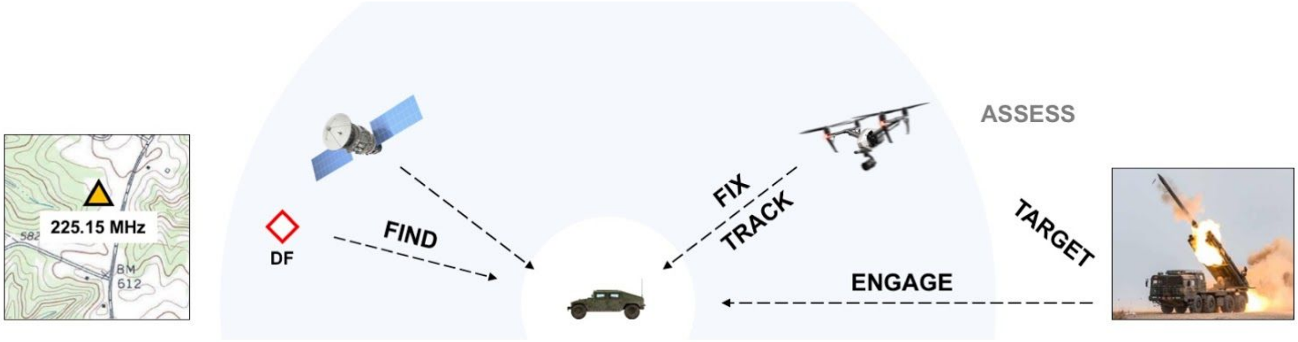
Purpose. To FIND information on adversary electromagnetic reconnaissance threats.

Process

1. ASK the **S-2**, "Which of our EM emissions can adversary ES units collect in our AO?" IOT UNDERSTAND adversary ES collections capabilities and UNDERSTAND friendly electromagnetic emissions signatures.



Conventional ES direction finding (DF): Friendly omnidirectional radio emissions are captured by adversary ground ES DF units. Three bearings are ideal for an accurate fix.



Modern integrated Fires Network: Satellite, aircraft, and UAS collectors augment adversary ground DF units to FIND, FIX, TRACK, TARGET, ENGAGE with precision fires and then ASSESS (F2T2EA).

Understanding how adversary collections initiate the adversary kill chain includes understanding the real-world delays that accrue at each step. Where does an ISR report go? How long does it take to be processed? When does targeting information reach a decision maker? When does targeting information reach a firing agency?

Simplified diagrams like the one above make the F2T2EA cycle seem simple and fast. We need to understand realistic timelines for our adversary's kill chain processes. Some foreign armies have a *five-day* turnaround for FMV intelligence.

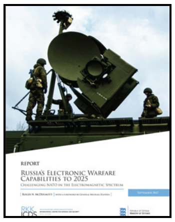
2. SEARCH the classified U.S. intelligence sites on **SIPR**:

NGIC (U.S. Army) provides intelligence on foreign ground forces.

NASIC (U.S. Air Force) provides intelligence on foreign air and space forces.

MIDB contains DIA information on foreign EOB.

3. SEARCH the web for evolving EW **capabilities**.



Russia's Electronic Warfare Capabilities to 2025.
Roger McDermott. Estonia: ICDS, Sep 2017. 48 pages.

Discusses Russian EW threats to NATO.

4. READ B: Annex B (**Intelligence**) of the OPORDER to understand adversary order of battle (OOB), electromagnetic order of battle (EOB) and electromagnetic reconnaissance units.

READ B12: Appendix 12 (**Intelligence Products**) to Annex B (Intelligence) for IPB products on adversary OOB, EOB, and electromagnetic reconnaissance units collecting EM signals.

Read B3B: Tab B (**Multidiscipline CI Threat Report**) to Appendix 3 (CI) to Annex B (Intelligence) for an assessment of adversary collection capabilities in the EM spectrum.

READ B2A: Tab A (**Communications Intelligence Collection Requirements**) to Appendix 2 (SIGINT) to Annex B (Intelligence) to understand how friendly SIGINT will target adversary collectors. Friendly electromagnetic reconnaissance is ES, a search for their collectors.

5. UNDERSTAND adversary ES **technology**, capabilities, terms, proliferation, and TTPs.

See UNDERSTAND Adversary Satellite ES Collections Capabilities.

See UNDERSTAND Adversary Aircraft ES Collections Capabilities.

See UNDERSTAND Adversary UAS ES Collections Capabilities.

See UNDERSTAND Adversary Ground ES Collections Capabilities.

6. ASK the **S-6**, “What U.S. signatures are vulnerable to adversary ES units?” and “What steps are we taking to REDUCE our EM vulnerabilities?” IOT UNDERSTAND friendly electromagnetic emissions vulnerabilities.

   READ K: Annex K (**Combat Information Systems**) of the OPORDER to understand the friendly communications plan and our electromagnetic protection (EP) procedures.

   READ K1: Appendix 1 (**Information Systems Security**) to Annex K (Combat Information Systems) to understand actions are being taken to REDUCE our EM vulnerabilities.

   READ the CEOI and SPINS for EP EMCON guidance.
   See EP EMCON CEOI SOP.

7. REQUEST a **Threat Vulnerability Assessment** (TVA)—if one has been conducted—which may include a survey of friendly EM vulnerabilities. CI identifies adversary intelligence capabilities to support friendly force protection requirements. A TVA may or may not address the technical aspects of our vulnerabilities to adversary EM collections.

Terms. See EP EMCON Glossary.

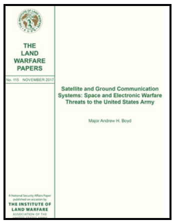
electromagnetic reconnaissance — The detection, location, identification, and evaluation of foreign electromagnetic radiations. (*DOD Dictionary*, 1 Jun 2020) *Prior to June 2020, the term was “electronic reconnaissance.”*

EP (electromagnetic protection) — Division of electromagnetic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability. (*DOD Dictionary*, 1 Jun 2020) *Prior to June 2020, EP was “electronic protection.” EW = EA + EP + ES.*

ES (electromagnetic support) — Division of electromagnetic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations. (*DOD Dictionary*, 1 Jun 2020) *Prior to June 2020, ES was “electronic warfare support.” EW = EA + EP + ES.*

TVA (threat vulnerability assessment) — Provides an in-depth analysis of intelligence, sabotage, subversive, and terrorist threats (and friendly vulnerabilities) associated with a physical installation such as ports, airfields, or base camps. (MCRP 2-10A.2 *Counterintelligence and Human Intelligence*, 21 Nov 2019)

References



THE LAND WARFARE PAPERS

No. 115 NOVEMBER 2017

Satellite and Ground Communication Systems: Space and Electronic Warfare Threats to the United States Army

Major Andrew H. Boyd

A National Security Affairs Paper published on occasion by THE INSTITUTE OF LAND WARFARE ASSOCIATION OF THE UNITED STATES ARMY

Andrew Boyd. *Satellite and Ground Communication Systems: Space and Electronic Warfare Threats to the United States Army*. Arlington, VA: AUSA, Nov 2017.

CCW OXFORD CHANGING CHARACTER OF WAR CENTRE

AXEL AND MARGARET AX:SON JOHNSON FOUNDATION

PEMBROKE COLLEGE OXFORD

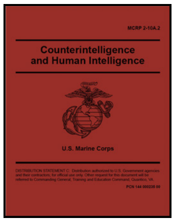
UNIVERSITY OF OXFORD

Changing Character of War Centre
Pembroke College, University of Oxford
With Axel and Margaret Ax:son Johnson Foundation

The Russian Reconnaissance Fire Complex Comes of Age
Lester W. Grau and Charles K. Bartles
May 2018

[illegible]

Lester Grau and Charles Bartles. *The Russian Reconnaissance Fire Complex Comes of Age*. Oxford, England: University of Oxford, 30 May 2018.



MCRP 2-10A.2

Counterintelligence and Human Intelligence

U.S. Marine Corps

DISTRIBUTION STATEMENT C: Distribution authorized to U.S. Government agencies and their contractors; for official use only. Other request for this document will be referred to Commanding General, Training and Education Command, Quantico, VA.

PCN 144 000235 00

MCRP 2-10A.2 *Counterintelligence and Human Intelligence*, 21 Nov 2019.
287 pages.

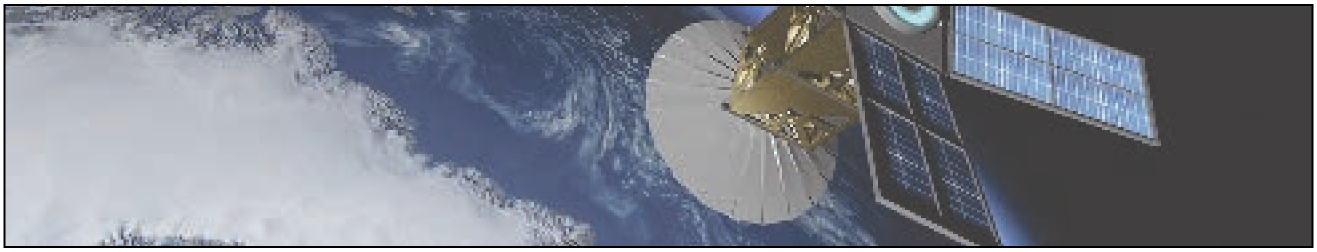
Includes an example Appendix 3 (CI) of Tab B (Intelligence)to the OPORDER. TSCM techniques to locate surveillance are ONLY done ISO sensitive locations.

Contributors: **BBM**, 1 Nov 2020.

Understand

Adversary Satellite ES Collections Capabilities

Purpose. To FIND information on adversary satellite electromagnetic reconnaissance threats.



Process

1. ASK the **S-2**, “What electromagnetic emissions can adversary satellites collect in our AO?”

2. SEARCH the classified U.S. intelligence sites on **SIPR**:

   NASIC (U.S. Air Force) provides intelligence on foreign air and space forces.

3. SEARCH the web for evolving satellite **capabilities**.

4. UNDERSTAND satellite **terms**. What kind of satellites do our adversaries possess and what capabilities do they provide?

Challenges to Security in Space. Defense Intelligence Agency, 2019. 46 pages. www.dia.mil/Military-Power-Publications

Explains key space concepts and capabilities, including communications satellites, ISR, missile warning, position, navigation, and timing, and satellite command and control architecture.

5. UNDERSTAND satellite **proliferation**.

Space Threat Assessment 2020. Washington DC: Center for Strategic and International Studies (CSIS), 2020. 80 pages. **csis.org**

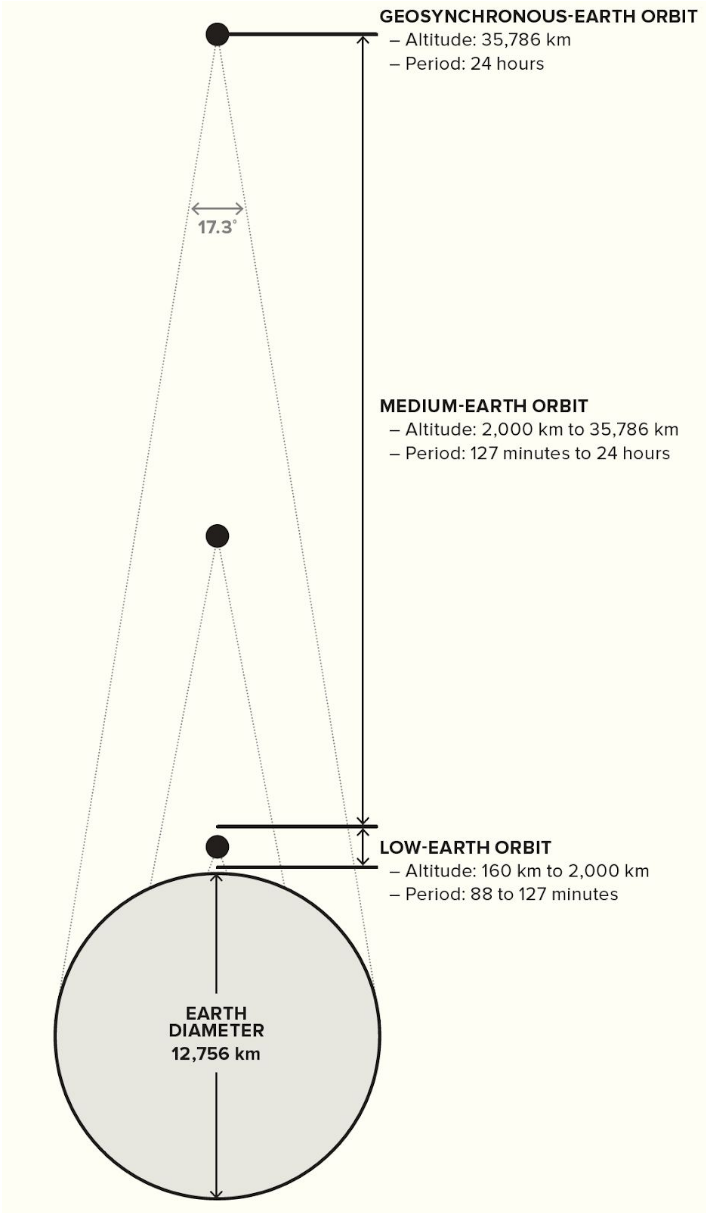
Summarizes government and commercial satellites. Although primarily a report on adversary counterspace capabilities, CSIS provides insight into the increasing technological advancements of great powers and illuminates U.S. vulnerabilities.

6. UNDERSTAND satellite **TTPs.**

   Because LEO satellites are not overhead continuously, the S-2 needs to request SATVUL (satellite vulnerability) windows and SATRAN (satellite reconnaissance advanced notification) reports. The S-2 can explain adversary collection tasking, processing, exploitation, and dissemination of SIGINT and GEOINT.

7. UNDERSTAND what U.S. **signatures** are vulnerable to adversary satellite ES collections.

Discuss with the S-2: Adversary SIGINT, EW, and GEOINT capabilities versus U.S. equipment and procedures.


GEOSYNCHRONOUS-EARTH ORBIT
– Altitude: 35,786 km
– Period: 24 hours
17.3°
MEDIUM-EARTH ORBIT
– Altitude: 2,000 km to 35,786 km
– Period: 127 minutes to 24 hours
LOW-EARTH ORBIT
– Altitude: 160 km to 2,000 km
– Period: 88 to 127 minutes
EARTH
DIAMETER
12,756 km

GEO is ***geosynchronous earth orbit.***

A high-altitude satellite orbit with the same period and direction as the earth's rotation. To an observer on the ground, the satellite appears motionless in the sky.

The advantage of GEO satellites for communications is that ground antennas do not need to track the satellite, and, because of the satellite's high altitude, coverage is almost the entire hemisphere.

MEO is medium earth orbit.

LEO is low earth orbit.

HEO, surprisingly, is NOT "high earth orbit," but "highly elliptical orbit." (DOD Dictionary, 1 Jun 2020)

Source: Boyd, *Satellite and Ground Communication Systems*, page 8.

Contributors: **BMW**, 1 Nov 2020.

Understand

Adversary Aircraft ES Collections Capabilities

Purpose. To FIND information on adversary aircraft electromagnetic reconnaissance threats.

Process

1. ASK the **S-2**, “What electromagnetic emissions can adversary aircraft collect in our AO?”

2. SEARCH the classified U.S. intelligence sites on **SIPR**:

   NASIC (U.S. Air Force) provides intelligence on foreign air and space forces.

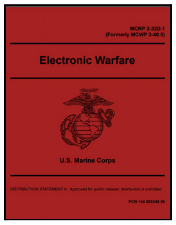
3. SEARCH the web for evolving aircraft EW **capabilities**.

   SOUTH CHINA SEA MILITARY CAPABILITY SERIES
   ELECTRONIC WARFARE AND SIGNALS INTELLIGENCE

   Electronic Warfare and Signals Intelligence. J. Michael Dahm. Johns Hopkins Applied Physics Laboratory, 1 Aug 2020. 35 pages.

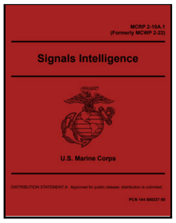
   The section starting on page 15 explains EW aircraft capabilities in the South China Sea.

4. UNDERSTAND aircraft EW **terms**. What adversary aircraft provide electromagnetic support versus electromagnetic attack or electromagnetic protection?

   MCRP 3-32D.1 *Electronic Warfare.* 4 Apr 2018.
   148 pages.

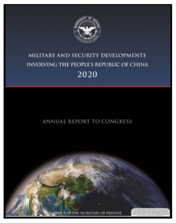
   Out-of-date ***2002*** *manual: Incorrect terms, old organizations, and zero discussion of modern threat capabilities. Re-numbered in 2016. Gender-neutralized in 2018.*

   MCRP 2-10A.1 *Signals Intelligence.* 4 Apr 2018.
   125 pages.

   Out-of-date ***1999*** *manual: Incorrect terms and old equipment. Re-numbered in 2004 and 2016. Gender-neutralized in 2018.*

5. UNDERSTAND EW aircraft **proliferation**.


MILITARY AND SECURITY DEVELOPMENTS
INVOLVING THE PEOPLE'S REPUBLIC OF CHINA
2020
ANNUAL REPORT TO CONGRESS
OFFICE OF THE SECRETARY OF DEFENSE

Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2020. OSD, 2020. 200 pages.

Explains modernization efforts by the PLAAF to increase aircraft capability, including specialized aircraft to "disrupt adversary battlespace awareness," and "amplify PLAAF's ability to detect, track, and target threats... at greater distances."

6. UNDERSTAND aircraft **TTPs**.

Adversary aircraft collections on our VHF and UHF are usually LOS—and for aircraft at 10,000 feet, there is a *lot* of LOS.

7. UNDERSTAND what U.S. **signatures** are vulnerable to adversary aircraft ES collections.

Talk to the S-2, S-6, and RadBn Marines to understand friendly vulnerabilities.

Contributors: **BMW**, 1 Nov 2020.

Understand

Adversary UAS ES Collections Capabilities

Purpose. To FIND information on adversary UAS electromagnetic reconnaissance threats.

Process

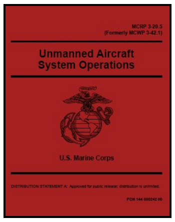
1. ASK the **S-2**, "What electromagnetic emissions can adversary UAS collect in our AO?"

2. SEARCH the classified U.S. intelligence sites on **SIPR**:

   NASIC (U.S. Air Force) provides intelligence on foreign air and space forces.

3. SEARCH the web for evolving UAS **capabilities**.

4. UNDERSTAND UAS **terms**.



MCRP 3-20.5
(Formerly MCWP 3-42.1)

Unmanned Aircraft
System Operations

U.S. Marine Corps

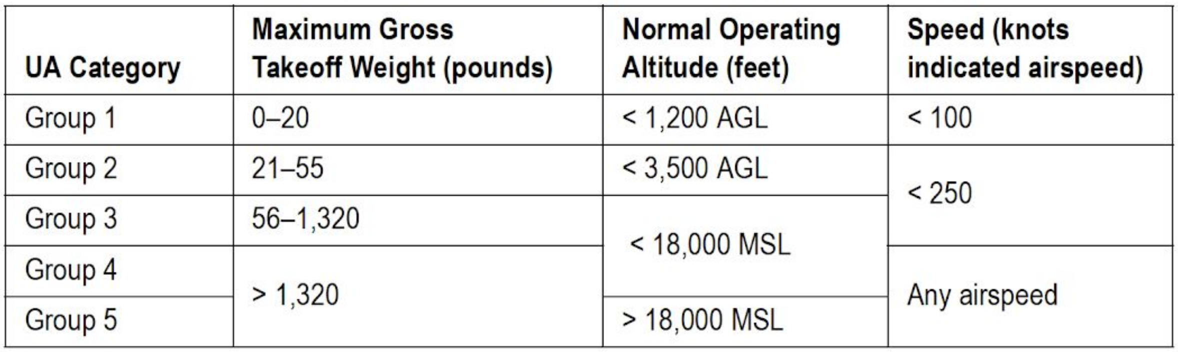
DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

PCN 144 000242 00

MCRP 3-20.5 *Unmanned Aircraft System Operations*, 2 May 2016.
61 pages.

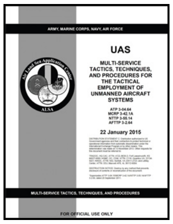
Chapter 1 explains UAS payloads, SIGINT and IMINT sensors, communications relays, and weapons. Explains the control element, support element, communications links, and defines the five UAS groups.

UAS Group Categories.



UA Category	Maximum Gross Takeoff Weight (pounds)	Normal Operating Altitude (feet)	Speed (knots indicated airspeed)
Group 1	0–20	< 1,200 AGL	< 100
Group 2	21–55	< 3,500 AGL	< 250
Group 3	56–1,320	< 18,000 MSL	
Group 4	> 1,320		Any airspeed
Group 5		> 18,000 MSL	

Source: Table 1-1 of MCRP 3-20.5 *UAS Operations*, 2 May 2016.
Notes: AGL—above ground level. MSL—mean sea level.


ARMY, MARINE CORPS, NAVY, AIR FORCE
UAS
MULTI-SERVICE TACTICS, TECHNIQUES, AND PROCEDURES FOR THE TACTICAL EMPLOYMENT OF UNMANNED AIRCRAFT SYSTEMS
ATP 3-04.64
MCRP 3-42.1A
NTTP 3-55.14
AFTTP 3-2.64
22 January 2015
MULTI-SERVICE TACTICS, TECHNIQUES, AND PROCEDURES
FOR OFFICIAL USE ONLY

MCRP 3-42.1A *UAS: Multi-Service TTPs for the Tactical Employment of UAS*, 22 Jan 2015. 110 pages.

Explains UAS employment procedures. No discussion of EW, EP, or EMCON.

5. UNDERSTAND UAS **proliferation**.

[Emerging Trends in China's Development of Unmanned Systems.](#)
Chase, et al. Rand Corporation, 2015. 14 Pages. **rand.org**

Explains emerging Chinese UAS capabilities and how aerial collections are integrated with long-distance targeting.

6. UNDERSTAND UAS **TTPs**.

[Small Unmanned Aerial System Adversary Capabilities.](#)
Wilson, et al. Rand Corporation, 2020. 147 Pages. **rand.org**

*Comprehensive explanations of UAS **terms**, **proliferation**, and **TTPs**. See chapter four for tactical use of UAS.*

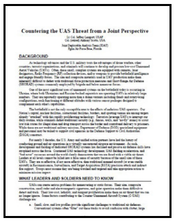
COMBATING TERRORISM CENTER
THE ISLAMIC STATE AND DRONES
SUPPLY, SCALE, AND FUTURE THREATS
Don Rassler

[The Islamic State and Drones: Supply, Scale, and Future Threats.](#)
Don Rassler. West Point, NY: U.S. Military Academy, 2018. **ctc.usmc.edu**

Details ISIS innovation and use of SUAS.

7. UNDERSTAND what U.S. **signatures** are vulnerable to adversary UAS ES collections.

Talk to the S-2, S-6, and RadBn Marines to understand friendly vulnerabilities.


Countering the UAS Threat from a Joint Perspective
BACKGROUND
WHAT LEADERS AND SOLDIERS NEED TO KNOW

[Countering the UAS Threat From a Joint Perspective.](#)
Jeffrey Lamport and Anthony Scotto. Eglin AFB, FL: JDAT, n.d. 4 pages.

Explains what warfighters need to know to understand UAS threats.

Contributors: **BMW**, 1 Nov 2020.

Understand

Adversary Ground ES Collections Capabilities

Purpose. To FIND information on adversary ground electromagnetic reconnaissance threats.

Process

1. ASK the **S-2**, “What EM emissions can adversary ground ES units collect in our AO?”

2. SEARCH the classified U.S., intelligence sites on **SIPR**:

   NGIC (U.S. Army) provides intelligence on foreign ground forces.

3. SEARCH the web for evolving ground ES unit **capabilities**.

4. UNDERSTAND ground ES unit **terms**.

   UNDERSTAND the terms—direction finding (DF), line of bearing—and the processes that adversary units use to fix and report our positions.

5. UNDERSTAND ground ES unit **proliferation**.

Russian Electronic Warfare
A Growing Threat to U.S. Battlefield Supremacy
ASP
Perspective
Patrick Smith
April 2020

Russian Electronic Warfare: A Growing Threat to U.S. Battlefield Supremacy. Patrick Smith. American Security Project, 2020.

Details the expansion of Russian EW following the Russia-Georgia conflict of 2008, and the role EW plays in Russian operations in Ukraine and Syria.

6. UNDERSTAND ground ES unit **TTPs**.

The Russian Way of War: Force Structure, Tactics, and Modernization of the Russian Ground Forces. Lester Grau and Charles K. Bartles. Foreign Military Studies Office, Fort Leavenworth, KS, 2016. 416 pages.

Pages 289-300 describe the equipment and capabilities of Russian Electronic Warfare Troops.

7. UNDERSTAND what U.S. **signatures** are vulnerable to adversary ground ES units.

See pages 292-297 of *The Russian Way of War*, referenced above, for the frequencies and ranges that are vulnerable to Russian jamming, intercepting, and direction finding.

Contributors: **BMW**, 1 Nov 2020.

Understand

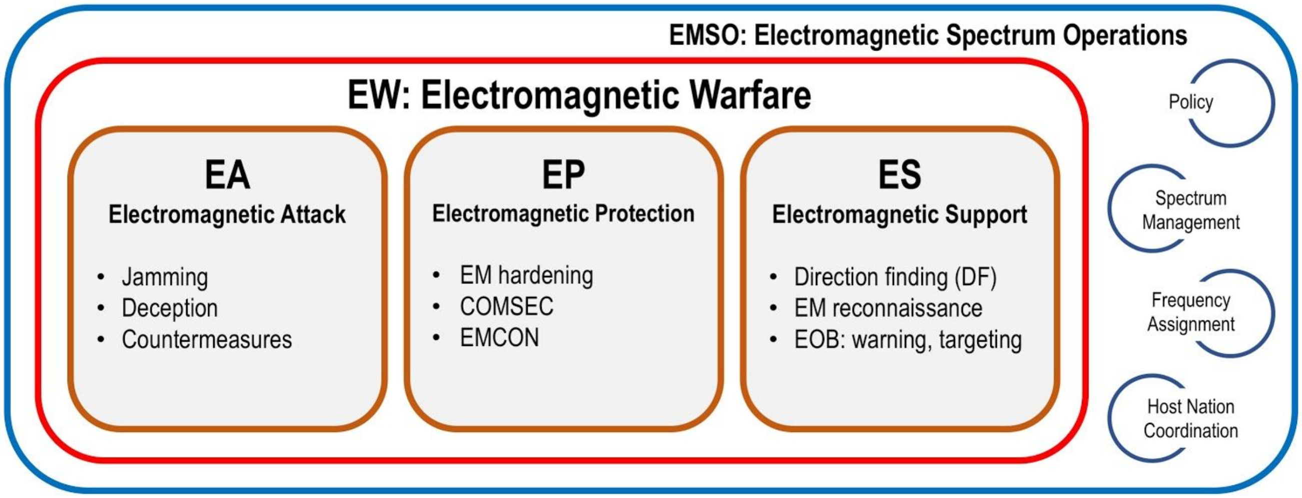
U.S. EW Doctrine

Purpose. To FIND information on U.S. electromagnetic warfare (EW) doctrine.

Doctrine

1. **EW**—military action in the electromagnetic (EM) spectrum—has three divisions:

EA: Electromagnetic Attack—attacking the adversary, a form of fires,
EP: Electromagnetic Protection—protecting friendly use of the EM spectrum, and
ES: Electromagnetic Support—finding adversary emitters.



EW is part of the larger electromagnetic spectrum operations (EMSO)—management of the electromagnetic environment. EMSO is called ‘JEMSO’ in joint doctrine.

See the EP EMCON Glossary for the new and current definitions of all EW terms. Before the June 2020 *DOD Dictionary*, EW was called ‘electronic warfare.’ All the EW terms and definitions in *all* EW manuals written prior to 2020 are now out-of-date. The term ‘ECCM,’ for example, is no longer included in the *DOD Dictionary*.

2. **EA: Electromagnetic Attack**—‘Division of electromagnetic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires.’ (*DOD Dictionary*, 1 Jun 2020)

EA includes jamming, deception of adversary ISR, countermeasures such as CREW, intrusion of false information into adversary nets, and probing.

3. **EP: Electromagnetic Protection**—'Division of electromagnetic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability.' (*DOD Dictionary*, 1 Jun 2020)

   EP includes electromagnetic hardening or shielding of equipment, COMSEC crypto and TRANSEC frequency hopping technology, and emission control (EMCON) actions such as reducing power and using directional antennas to limit signatures. Friendly EP minimizes the enemy's ability to conduct ES and EA against us. Wartime reserve modes are EP.

   Defensive EA—countermeasures to foil adversary guided weapons or electronically triggered weapons (CREW)—is NOT EP.

4. **ES: Electromagnetic Support—'**Division of electromagnetic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations.' (*DOD Dictionary*, 1 Jun 2020)

   ES collects data through direction finding (DF) and electromagnetic reconnaissance to update electromagnetic order of battle (EOB) files. This information is used for threat warning and targeting purposes.

   ES is short-term collections that support local commanders.
   SIGINT is a national-level collections effort. ELINT—collecting on non-communications devices such as radars and vehicles—is a subset of SIGINT.

5. **Employment of EW**

   Ground-based EW assets, particularly DF collections units co-located with forward units, are range-limited, masked by terrain, and vulnerable to enemy geolocation.

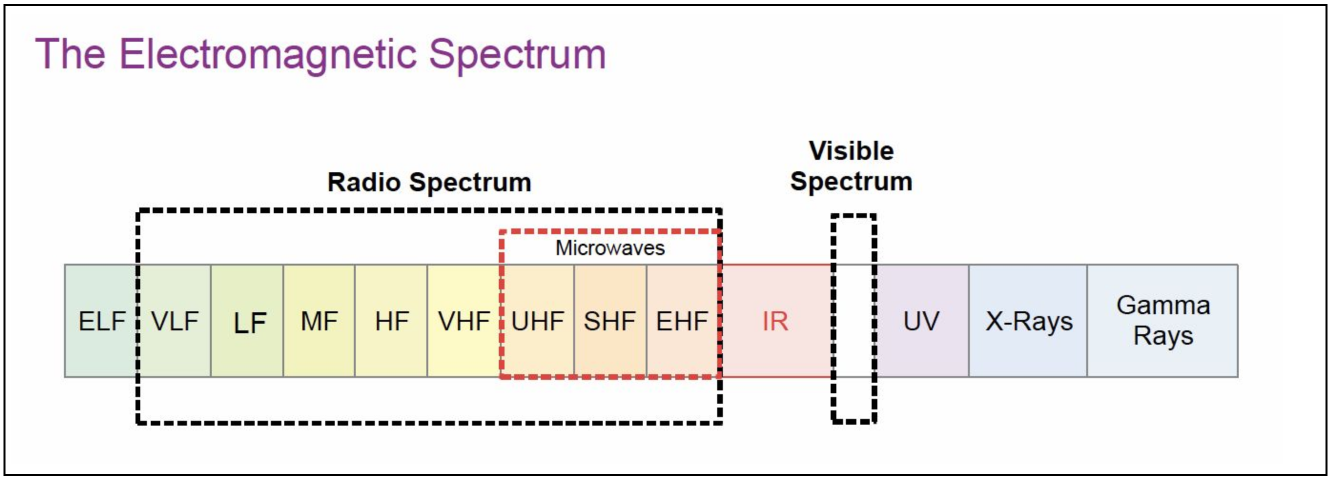
   Airborne EW assets, including UAS platforms, have greater LOS than ground-based assets, but are limited to short duration operations.

   EA operations depend on ES collections for targeting and BDA. EA operations can inadvertently affect host-nation networks.

   EP operations, which must be tailored to the specific threat and environment, require a vulnerability assessment of our own systems.

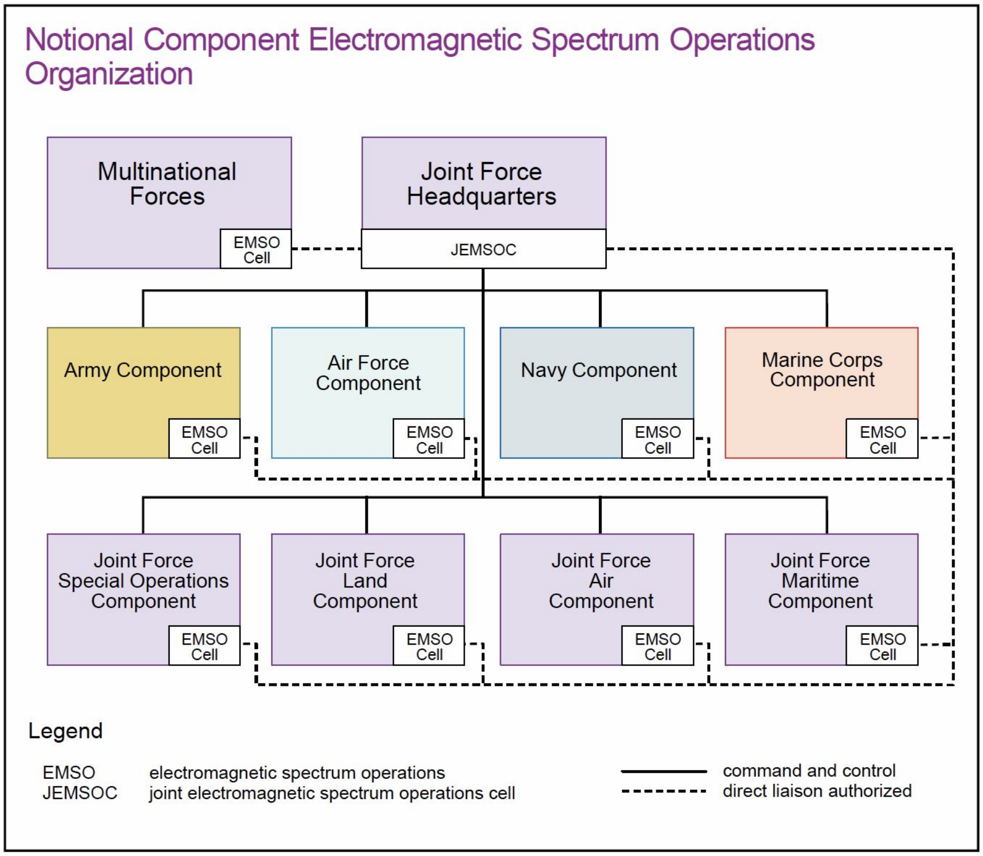
6. **EMSO:** electromagnetic spectrum management operations enable cyberspace, signal and EW operations. Spectrum management and frequency assignment efforts coordinate radios, radars, navigation, aircraft, and sensors across civil, joint and multinational partners.

   JEMSO: joint electromagnetic spectrum operations manage the electromagnetic operational environment, which includes the electromagnetic spectrum as well as terrain, weather, atmospheric conditions, and man-made facilities. Electromagnetic battle management (EMBM) and Joint spectrum interference resolution (JSIR) is part of JEMSO. JEMSO mission areas include cyberspace and space operations.


The Electromagnetic Spectrum

Source: Figure I-1 of JP 3-85 *JESO*, 22 May 2020.

7. At the joint level, all components, including the MAGTF, establish an **EMSO Cell** to coordinate electromagnetic spectrum operations (EMSO).


Notional Component Electromagnetic Spectrum Operations Organization
Multinational Forces
EMSO Cell
Joint Force Headquarters
JEMSOC
Army Component
EMSO Cell
Air Force Component
EMSO Cell
Navy Component
EMSO Cell
Marine Corps Component
EMSO Cell
Joint Force Special Operations Component
EMSO Cell
Joint Force Land Component
EMSO Cell
Joint Force Air Component
EMSO Cell
Joint Force Maritime Component
EMSO Cell
Legend
EMSO electromagnetic spectrum operations
JEMSOC joint electromagnetic spectrum operations cell
command and control
direct liaison authorized

Source: Figure II-3 of JP 3-85 *JESO*, 22 May 2020.

Notes on USMC Radio Battalion

“The mission of the radio battalion is to provide SIGINT, electronic warfare, limited cyberspace operations, and special intelligence communications support to the MAGTF and joint force commander.” (MCRP 1-10.1 *Organization of the Unites States Marine Corps*, 26 Aug 2016) On the modern battlefield, *all* units need to understand how EW—EA, EP, and ES—affects their mission.

Notes on Doctrine

EW doctrine is continually changing. Older manuals now include incorrect and contradictory EW information. For example, MCRP 3-40.3E *HF-ALE*, 1 Sep 2003, states that COMSEC has four divisions: cryptosecurity, transmission security (TRANSEC), emission security, and physical security. This definition is NOT reflected in the latest June 2020 *DOD Dictionary*. The best EW sources are the continually-updated joint publications followed by the recent U.S. Army manuals.

References

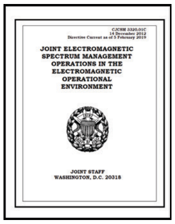
Joint Publication 3-85

Joint Electromagnetic Spectrum Operations

22 May 2020

JP 3-85 *Joint Electromagnetic Spectrum Operations*, 22 May 2020.
148 pages.

Supersedes JP 3-13.1 Electronic Warfare *and JP 6-01* Joint Electromagnetic Spectrum Management Operations*.*

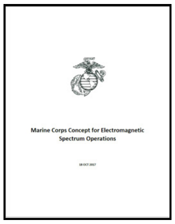


CJCSM 3320.01C
14 December 2012
Directive Current as of 5 February 2019

JOINT ELECTROMAGNETIC SPECTRUM MANAGEMENT OPERATIONS IN THE ELECTROMAGNETIC OPERATIONAL ENVIRONMENT

JOINT STAFF
WASHINGTON, D.C. 20318

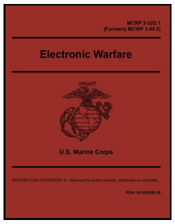
CJCSM 3320.01C *JEMSMO in the EOE*, 5 Feb 2019.
197 pages.



Marine Corps Concept for Electromagnetic Spectrum Operations

18 OCT 2017

Marine Corps Concept for Electromagnetic Spectrum Operations, 18 Oct 2017.
22 pages.



MCRP 3-32D.1
(Formerly MCWP 3-40.5)

Electronic Warfare

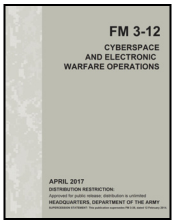
U.S. Marine Corps

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

PCN 144 000246 00

MCRP 3-32D.1 *Electronic Warfare*, 4 Apr 2018.
148 pages.

*Out-of-date **2002** publication. Incorrect terms, old organizations, and irrelevant procedures. Re-numbered in 2016. Gender-neutralized in 2018.*

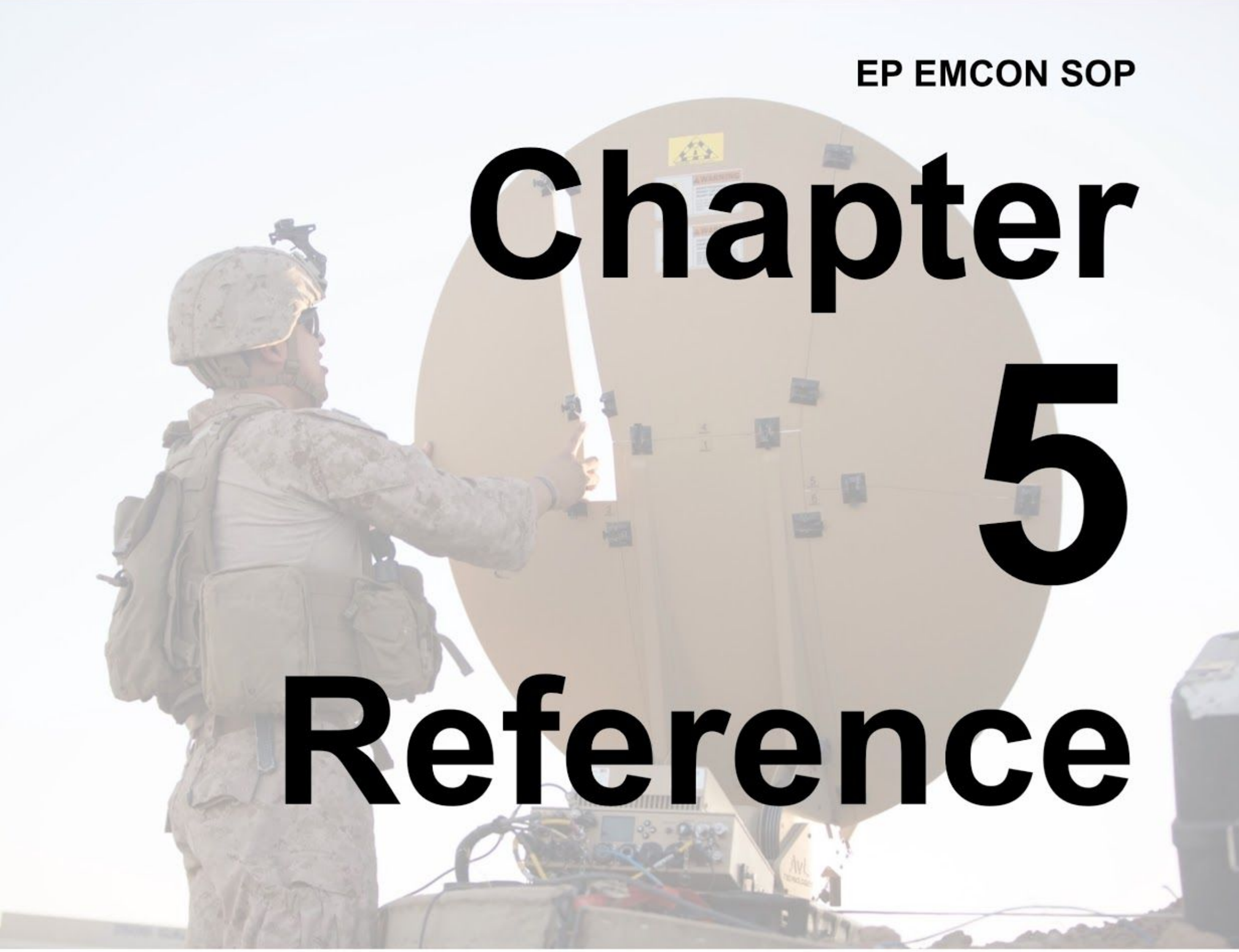


FM 3-12
CYBERSPACE
AND ELECTRONIC
WARFARE OPERATIONS

APRIL 2017
DISTRIBUTION RESTRICTION:
Approved for public release; distribution is unlimited
HEADQUARTERS, DEPARTMENT OF THE ARMY
SUPERCESSION STATEMENT: This publication supersedes FM 3-38, dated 12 February 2014.

FM 3-12 *Cyberspace and Electronic Warfare Operations*, 11 Apr 2017.
108 pages.

Contributors: BBM, 1 Nov 2020.



EP EMCON SOP

Chapter 5

Reference

In this Chapter

- EP EMCON Glossary
- EP EMCON Bibliography

Marine Corps Intelligence Schools
Intelligence Training Enhancement Program

SIGMAN EP EMCON SOP:
Chapter 5: Reference

Marine Corps Intelligence Schools (MCIS)
Intelligence Training Enhancement Program (ITEP)

Reference

EP EMCON Glossary

Purpose. To SHARE a standard understanding of EW terms, with a focus on EP.

2G, 3G, 4G, 5G (second generation,third generation, fourth generation, fifth generation). (MCRP 3-30B.3 *Tac Radios*, 19 May 2017)

administrative signature — Administrative signatures are created by an individual or unit when conducting planning movement, contracting, or other administrative actions that can be collected on by adversary OSINT, SIGINT, HUMINT, and offensive cyber operations (OCO). (*Marine Corps Concept of Employment for Signature Management*, 12 Dec 2019) (NO DOD definition)

AEHF (advanced extremely high frequency) — A system of communications satellites.

AFATDS (advanced field artillery tactical data system).

AFTTP (Air Force tactics, techniques, and procedures). (*DOD Dictionary*, 1 Jun 2020)

ALARM (EW brevity code) — Terminate or terminating emissions control procedures. Opposite of SNOOZE. (MCRP 3-30B.1 *Brevity*, 28 May 2020).

ALE (automatic link establishment). (MCRP 3-30B.3 *Tac Radios*, 19 May 2017) *See HF ALE.*

ANW2 (adaptive networking wideband waveform). (*DOD Dictionary*, 1 Jun 2020)

ARM (antiradiation missile). (*DOD Dictionary*, 1 Jun 2020)

BFT (blue force tracking). (FM 1-02.1 *Operational Terms*, 21 Nov 2019)

BLOS (beyond line-of-sight). (*DOD Dictionary*, 1 Jun 2020)

brevity code — A code word, which provides no security, that serves the sole purpose of shortening of messages rather than the concealment of their content. (*DOD Dictionary*, 1 Jun 2020)

BUZZER (EW brevity code) — Electronic communications jamming. Same as NATO term CHATTER. (MCRP 3-30B.1 *Brevity*, 28 May 2020).

C2D2E (command and control in a denied or degraded environment).

CDMA (code-division multiple access) — A telecommunications standard used by mobile phone networks. *CDMA and GSM are two competing standards used for 2G and 3G networks.*

CEMA (cyberspace electromagnetic activities). (*DOD Dictionary*, 1 Jun 2020) *A U.S. Army term.*

CEOI (communications-electronics operating instructions) — An instruction containing details on call sign assignments, frequency assignments, codes and ciphers, and authentication tables and their use. The communications-electronics operating instructions (CEOI) is designated to complement information contained in operational unit communication standard operating procedures or Annex K (Combat Information Systems) to the operation order. The most common version of CEOI in use by the Marine Corps is the automated communications-electronics operating instructions produced by the National Aeronautics and Space Administration. (MCRP 1-10.2 *Marine Corps Supplement to the DOD Dictionary*, 31 May 2018)

CESAS (communication emitter sensing and attacking system) (MCRP 1-10.2 *Marine Corps Supplement to the DOD Dictionary*, 31 May 2018) — An Marine EW communications package mounted on an M1165 HMMWV.

CI (counterintelligence) — Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities. (*DOD Dictionary*, 1 Jun 2020)

CNR (combat net radio).

COMINT (communications intelligence) — Technical information and intelligence derived from foreign communications by other than the intended recipients. (*DOD Dictionary*, 1 Jun 2020) *SIGINT = COMINT + ELINT + FISINT*.

COMMCON (communications control). (MCRP 3-30B.2 *MAGTF Communications System*, 2 May 2016)

COMSEC (communications security) — Actions designed to deny unauthorized persons information of value by safeguarding access to, or observation of, equipment, material, and documents with regard to the possession and study of telecommunications or to purposely mislead unauthorized persons in their interpretation of the results of such possession and study. (*DOD Dictionary*, 1 Jun 2020)

countermeasures — That form of military science that, by the employment of devices and/or techniques, has as its objective the impairment of the operational effectiveness of enemy activity. (*DOD Dictionary*, 1 Jun 2020)

CPOF (command post of the future).

CREW (counter radio-controlled improvised explosive device electronic warfare). (*DOD Dictionary*, 1 Jun 2020)

D2CE (degraded and denied communications environment). (MCRP 3-30B.3 *Tac Radios*, 19 May 2017)

D3SOE (denied, degraded, or disrupted space operational environment) — A composite of those conditions and influences in which space-enabled capabilities have been impaired by hostile threats or non-hostile means. (FM 1-02.1 *Operational Terms*, 21 Nov 2019)

DAGR (Defense advanced GPS receiver).

DAMA (demand assigned multiple access). (MCRP 3-30B.3 *Tac Radios*, 19 May 2017) *See UHF DAMA.*

DCGS (distributed common ground system).

DCO (defensive cyberspace operations) — Missions to preserve the ability to utilize blue cyberspace capability and protect data, networks, cyberspace-enabled devices, and other designated systems by defeating on-going or imminent malicious cyberspace activity. (*DOD Dictionary*, 1 Jun 2020)

DCO-IDM (defensive cyberspace operations - internal defensive measures) — Operations in which authorized defense actions occur within the defended portion of cyberspace. (*DOD Dictionary*, 1 Jun 2020)

DCO-RA (defensive cyberspace operations - response actions) — Operations that are part of a defensive cyberspace operations mission that are taken external to the defended network or portion of cyberspace without the permission of the owner of the affected system. (*DOD Dictionary*, 1 Jun 2020)

DF (direction finding) — A procedure for obtaining bearings of radio frequency emitters by using a highly directional antenna and a display unit on an intercept receiver or ancillary equipment. (*DOD Dictionary*, 1 Jun 2020)

DODIN (Department of Defense information network) — The set of information capabilities and associated processes for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone. (*DOD Dictionary*, 1 Jun 2020)

DSCS (Defense satellite communications system). (MCRP 3-30B.3 *Tac Radios*, 19 May 2017)

DTCS (distributed tactical communications system) — An L-Band satellite system.

E3 (electromagnetic environmental effects) — The impact of the electromagnetic environment upon the operational capability of military forces, equipment, systems, and platforms. (*DOD Dictionary*, 1 Jun 2020)

EA (electromagnetic attack) — Division of electromagnetic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. (*DOD Dictionary*, 1 Jun 2020) *Prior to June 2020, EA was "electronic attack." EW = EA + EP + ES.*

EACA (electromagnetic attack control authority). (*DOD Dictionary*, 1 Jun 2020)

EARF (electromagnetic attack (EA) request form).

ECM (electromagnetic countermeasures). (*DOD Dictionary*, 1 Jun 2020)

EHF (extremely high frequency). (*DOD Dictionary*, 1 Jun 2020) 30–300 GHz.

electromagnetic hardening — Action taken to protect personnel, facilities, and/or equipment by blanking, filtering, attenuating, grounding, bonding, and/or shielding against undesirable effects of electromagnetic energy. (*DOD Dictionary*, 1 Jun 2020)

electromagnetic jamming — The deliberate radiation, reradiation, or reflection of electromagnetic energy for the purpose of preventing or reducing an enemy's effective use of the electromagnetic spectrum, with the intent of degrading or neutralizing the enemy's combat capability. (*DOD Dictionary*, 1 Jun 2020)

electromagnetic masking — The controlled radiation of electromagnetic energy on friendly frequencies in a manner to protect the emissions of friendly communications and electronic systems against enemy electromagnetic support measures/signals intelligence without significantly degrading the operation of friendly systems. (*DOD Dictionary*, 1 Jun 2020) *Prior to June 2020, the term was "electronic masking."*

electromagnetic reconnaissance — The detection, location, identification, and evaluation of foreign electromagnetic radiations. (*DOD Dictionary*, 1 Jun 2020) *Prior to June 2020, the term was "electronic reconnaissance."*

electromagnetic security — The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from their interception and study of noncommunications electromagnetic radiations (e.g., radar). (*DOD Dictionary*, 1 Jun 2020) *Prior to June 2020, the term was "electronics security."*

ELF (extremely low frequency). 3–30 Hz.

ELINT (electronic intelligence) — Technical and geolocation intelligence derived from foreign noncommunications electromagnetic radiations emanating from other than nuclear detonations or radioactives sources. (*DOD Dictionary*, 1 Jun 2020) *SIGINT = COMINT + ELINT + FISINT*.

EM (electromagnetic). (*DOD Dictionary*, 1 Jun 2020)

EMBM (electromagnetic battle management) — The dynamic monitoring, assessing, planning, and directing of operations in the electromagnetic spectrum in support of the commander's concept of the operation. (*DOD Dictionary*, 1 Jun 2020)

EMC (electromagnetic compatibility) — The ability of systems, equipment, and devices that use the electromagnetic spectrum to operate in their intended environments without causing or suffering unacceptable or unintentional degradation because of electromagnetic radiation or response. (*DOD Dictionary*, 1 Jun 2020)

EMCON (emission control) — The selective and controlled use of electromagnetic, acoustic, or other emitters to optimize command and control capabilities while minimizing, for operations security: a. Detection by enemy sensors, b. Mutual interference among friendly systems, and/or c. enemy interference with the ability to execute a military deception plan. (*DOD Dictionary*, 1 Jun 2020)

EME (electromagnetic environment) — The resulting product of the power and time distribution, in various frequency ranges, of the radiated or conducted electromagnetic emission levels encountered by a military force, system, or platform when performing its assigned mission in its intended operational environment. (*DOD Dictionary*, 1 Jun 2020)

EMI (electromagnetic interference) — Any electromagnetic disturbance, induced intentionally or unintentionally, that interrupts, obstructs, or otherwise degrades or limits the effective performance of electromagnetic spectrum-dependent systems and electrical equipment. (*DOD Dictionary*, 1 Jun 2020)

emission security — Actions designed to deny unauthorized persons information of value as a result of intercept and analysis of compromising emanations from cryptographic equipment and telecommunications systems. (*DOD Dictionary*, 1 Jun 2020)

EMOE (electromagnetic operational environment). (JP 3-85 *JESO*, 22 May 2020) (FM 1-02.1 *Operational Terms*, 21 Nov 2019) *REMOVED from DOD Dictionary in June 2020.*

EMS (electromagnetic spectrum). (*DOD Dictionary*, 1 Jun 2020)

Table. International Telecommunication Union (ITU) Frequency Bands.

Band	Name	ITU	Frequency	Uses
TLF	Tremendously low frequency	0	< 3 Hz	Natural noise
ELF	Extremely low frequency	1	3–30 Hz	Submarine Communications
SLF	Super low frequency	2	30–300 Hz	Submarine Communications
ULF	Ultra low frequency	3	300–3,000 Hz	Submarine Communications
VLF	Very low frequency	4	3–30 kHz	Navigation, heart rate monitors
LF	Low frequency	5	30–300 kHz	European AM radio
MF	Medium frequency	6	300–3,000 kHz	AM radio
HF	High frequency	7	3–30 MHz	CB, RFID, Marine radio
VHF	Very high frequency	8	30–300 MHz	FM radio, television
UHF	Ultra high frequency	9	300–3,000 MHz	Mobile phones, microwaves, GPS
SHF	Super high frequency	10	3–30 GHz	Radars, communications satellites
EHF	Extremely high frequency	11	30–300 GHz	Microwave radio relay
THF	Tremendously high frequency	12	300–3,000 GHz	Medical imaging

EMSCA (electromagnetic spectrum coordinating authority). (*DOD Dictionary*, 1 Jun 2020) *The JFC usually delegates EMSCA to the JTF J-3. At the CCMD level, EMSCA is usually the JEMSOC director.*

EMSO (electromagnetic spectrum operations) — Coordinated military actions to exploit, attack, protect, and manage the electromagnetic environment. (*DOD Dictionary*, 1 Jun 2020)

EMSOC (electromagnetic spectrum operations cell). (*DOD Dictionary*, 1 Jun 2020) *A Marine Corps term.*

EO-IR (electro-optical-infrared). (*DOD Dictionary*, 1 Jun 2020)

EOB (electromagnetic order of battle). (*DOD Dictionary*, 1 Jun 2020) A subset of the overall order of battle that consists of the identification, strength, command structure, disposition, and operating parameters of the EMS-dependent systems. This includes radiating, receiving, and inactive systems within an OA or those that could be readily deployed. The EOB is the identification of transmitters and receivers in an area of interest (AOI), a linkage to system and platform supported, a determination of their geographic location and range of mobility, a characterization of their signals, EMS parameters, and, where possible, a determination of their role in the broader organizational order of battle. (JP 3-85 JESO, 22 May 2020) *Prior to 2020, EOB was 'electronic order of battle.'*

EP (electromagnetic protection) — Division of electromagnetic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability. (*DOD Dictionary*, 1 Jun 2020) *Prior to June 2020, EP was "electronic protection." EW = EA + EP + ES.*

EPLRS (enhanced position locating reporting system).

ES (electromagnetic support) — Division of electromagnetic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations. (*DOD Dictionary*, 1 Jun 2020) *Prior to June 2020, ES was "electronic warfare support." EW = EA + EP + ES.*

ESIP (enhanced SINCGARS improvement program).

EW (electromagnetic warfare) — Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. (*DOD Dictionary*, 1 Jun 2020) *Prior to June 2020, EW was "electronic warfare." EW = EA + EP + ES.*

EA (electromagnetic attack)
EP (electromagnetic protection)
ES (electromagnetic support)

EWCC (electromagnetic warfare coordination cell). (*DOD Dictionary*, 1 Jun 2020) *NATO term for JEMSOC.*

EWST (electromagnetic warfare support team). A mobile Marine Corps EW team. *The new DOD term 'electromagnetic warfare' replaces the legacy term 'electronic warfare.'*

FDMA *(frequency-division multiple access)* — A telecommunications standard used by mobile phone networks.

FFT (fast Fourier transform).

FH (frequency hopping). (MCRP 3-30B.3 *Tac Radios*, 19 May 2017)

FHSS (frequency hopping spread spectrum) — A method of transmitting radio signals by rapidly changing the carrier frequency across a wide spectral band. FHSS is used to avoid interference, prevent eavesdropping, and enable CDMA communications.

FISINT (foreign instrumentation signals intelligence) — A subcategory of signals intelligence consisting of technical information and intelligence derived from the intercept of foreign electromagnetic emissions associated with the testing and operational deployment of non-United States aerospace, surface, and subsurface systems. (*DOD Dictionary*, 1 Jun 2020) *SIGINT = COMINT + ELINT + FISINT*.

FM (frequency management). (*DOD Dictionary*, 1 Jun 2020)

FMV (full-motion video). (*DOD Dictionary*, 1 Jun 2020)

G/ATOR (ground / air task-oriented radar) — The AN/TPS-8 G/ATOR is a Marine Corps air surveillance/air defense and air traffic control radar.

GBS (Global Broadcast Service). (*DOD Dictionary*, 1 Jun 2020)

GEO (geosynchronous earth orbit). (*DOD Dictionary*, 1 Jun 2020) — A high-altitude satellite orbit with the same period and direction as the earth’s rotation. To an observer on the ground, the satellite appears motionless in the sky. The advantage of GEO satellites for communication is that ground antennas do not need to track the satellite, and, because of the satellite’s high altitude, coverage is almost the entire hemisphere. *See MEO and LEO.*

GETAC — Company partner of GE Aerospace that produces ruggedized computers.

GPS (global positioning system) — A satellite-based radio navigation system operated by the Department of Defense to provide all military, civil, and commercial users with precise positioning, navigation, and timing. (*DOD Dictionary*, 1 Jun 2020)

GSM (global system for mobile communications) — A telecommunications standard used by mobile phone networks. GSM and CDMA are two competing standards used for second and third-generation (2G)(3G) networks.

HCLOS (high capacity line of sight). (MCRP 3-30B.3 *Tac Radios*, 19 May 2017)

HEO (highly elliptical orbit). (DOD Dictionary, 1 Jun 2020)

HF (high frequency). (*DOD Dictionary*, 1 Jun 2020) 3–30 MHz.

HF ALE (high frequency automatic link establishment) — A feature of some HF radios that enables the radio to automatically make contact and initiate a circuit with a distant station. *Sometimes written HF 3G ALE.*

HF NVIS (high frequency near vertical incidence skywave). (NO DOD, NO Army definition)

HHQ (higher headquarters).

HQ (HAVE QUICK). (MCRP 3-30B.3 *Tac Radios*, 19 May 2017) — A frequency hopping system for UHF aircraft radios. HQ II is second generation.

IBS (integrated broadband system). (FM 1-02.1 *Operational Terms*, 21 Nov 2019)

INMARSAT (international maritime satellite). (MCRP 3-30B.3 *Tac Radios*, 19 May 2017)

IP (internet protocol). (*DOD Dictionary*, 1 Jun 2020)

Iridium — Iridium L-Band service is a satellite-based wireless communications network providing global voice, data, and paging services through a dedicated, Air Force Space Command (AFSPC) / Defense Information System Agency (DISA) - controlled Defense Information System Network (DISN).

IRC (internet relay chat). (*DOD Dictionary*, 1 Jun 2020)

ISTAR (intelligence, surveillance, target acquisition, and reconnaissance).

IW (integrated waveform) — The integrated waveform is the improved time division multiple access waveform standard defined in MIL-STD-188-181C, 188-182B, and 188-183B. Integrated waveform greatly improves quality of services and access to ultrahigh frequency satellite communications resources over Demand Assigned Multiple Access. (MCRP 3-30B.3 *Tac Radios*, 19 May 2017) *See UHF SATCOM IW.*

JBC-P (joint battle command-platform).

JCEOI (joint communications-electronics operating instructions). (*DOD Dictionary*, 1 Jun 2020) *See CJCSI 3320.03D* JCEOI*, 25 Jun 2018.*

JCR (Joint Capabilities Release) — An updated position reporting system that replaces Blue Force Tracking.

JEMSO (joint electromagnetic spectrum operations) — Military actions undertaken by a joint force to exploit, attack, protect, and manage the electromagnetic environment. (*DOD Dictionary*, 1 Jun 2020)

JEMSOC (joint electromagnetic spectrum operations cell). (*DOD Dictionary*, 1 Jun 2020) *CCDRs and JFCs normally establish a JEMSOC to control the EMS. The JEMSOC director receives delegated authority from the CCDR (or JFC).*

JFC (joint force commander) — A general term applied to a combatant commander, subunified commander, or joint task force commander authorized to exercise combatant command (command authority) or operational control over a joint force. (*DOD Dictionary*, 1 Jun 2020)

JFFT (joint friendly force tracking).

JRFL (joint restricted frequency list) — A time and geographically oriented listing of TABOO, PROTECTED, and GUARDED functions, nets, and frequencies and limited to the minimum number of frequencies necessary for friendly forces to accomplish objectives. (*DOD Dictionary*, 1 Jun 2020)

JSIR (joint spectrum interference resolution). (*DOD Dictionary*, 1 Jun 2020)

JSIRO (joint spectrum interference resolution online). (MCRP 3-30B.3 *Tac Radios*, 19 May 2017)

JTRS (joint tactical radio system). (MCRP 3-30B.3 *Tac Radios*, 19 May 2017)

LAN (local-area network).

LEO (low-earth orbit). (*DOD Dictionary*, 1 Jun 2020)

LF (low frequency). 30–300 kHz.

LOS (line of sight). (*DOD Dictionary*, 1 Jun 2020)

LPD (low probability of detection). (*DOD Dictionary*, 1 Jun 2020)

LPI (low probability of intercept). (*DOD Dictionary*, 1 Jun 2020)

LTE (long-term evolution) — A telecommunications standard for 4G wireless data transmission and mobile phone networks.

MCR (multi-channel radio). (MCRP 3-30B.2 *MAGTF Communications System*, 2 May 2016) *See SCR*.

MEO (medium earth orbit). (*DOD Dictionary*, 1 Jun 2020)

MF (medium frequency). 300–3,000 kHz.

MIJI (meaconing, intrusion, jamming, interference). (NO DOD, USMC, or Army definition)

MILSTAR (military strategic and tactical relay).

MRC-142 — USMC multi-channel UHF LOS radio set.

MRC-145 — USMC vehicle-mounted SINCGARS system with two radios and a power amplifier.

MSE (mobile subscriber equipment). (FM 1-02.1 *Operational Terms*, 21 Nov 2019)

MUOS (mobile user objective system).

MUOS OTM (mobile user objective system on-the-move).

NOTM (network on the move).

NSTR (nothing significant to report).

NTTP (Navy, tactics, techniques, and procedures). (*DOD Dictionary*, 1 Jun 2020)

NVIS (near vertical incidence skywave). A high take-off angle (60–90°) propagation pattern that reflects signals off the ionosphere and back to earth in a circular pattern around the transmitter. NVIS usually requires lower frequencies (2–8 MHz). *See HF NVIS.*

OFDM (orthogonal frequency-division multiplexing) — A telecommunications standard used by 4G and 5G mobile phone networks, digital television, wireless networks, and DSL internet access.

OPED (official portable electronic device). *See PED.*

OPSEC (operations security) — A capability that identifies and controls critical information, indicators of friendly force actions attendant to military operations, and incorporates countermeasures to reduce the risk of an adversary exploiting vulnerabilities. (*DOD Dictionary*, 1 Jun 2020)

OTH (over the horizon). (*DOD Dictionary*, 1 Jun 2020)

OTM (on-the-move). (MCRP 3-30B.2 *MAGTF Communications System*, 2 May 2016)

PACE (primary, alternate, contingency, emergency) — The primary, alternate, contingency, and emergency (PACE) communications plan is a communication plan for a specific mission or task, not a specific unit. (ATP 6-02.53 *Techniques for Tactical Radio Operations*, 13 Feb 2020)

PCC (precombat check). (FM 1-02.1 *Operational Terms*, 21 Nov 2019)

PED (portable electronic device) — Any piece of lightweight, electrically-powered equipment. These devices are typically consumer electronics devices functionally capable of communications, data processing and/or utility. (FAA Aviation Rulemaking Committee, 30 Sep 2013) *Examples of PED include: laptop computers; hand-held smart phones, tablet computers, media players, e-readers, and personal digital assistants; gaming and* *entertainment devices; medical devices such as pacemakers and hearing aids; asset trackers; data collection and monitoring devices; inventory management and point-of-sale devices; wearable computers and other devices with or without wireless transmitters and receivers.*

PED (processing, exploitation, and dissemination).

PFC (protected forward communications) — A program aimed to enable small unit tactical operations to persist under electronic warfare (EW) conditions.

physical signature — Physical signatures are those indicators that can be collected by adversary GEOINT assets or through direct observation. (*Marine Corps Concept of Employment for Signature Management*, 12 Dec 2019) (NO DOD definition)

PLI (position location information).

PNT (positioning, navigation, and timing). (*DOD Dictionary*, 1 Jun 2020)

PPED (personal portable electronic device). *See PED.*

PRC (portable radio communications). (MCRP 3-30B.3 *Tac Radios*, 19 May 2017)

PRC-104 — Voice radio capable of operating HF. (MCRP 3-30B.3 *Tac Radios*, 19 May 2017)

PRC-113 — Voice radio operating in the VHF and UHF AM mode used by forward air controllers for LOS air to ground communications. (MCRP 3-30B.3 *Tac Radios*, 19 May 2017)

PRC-117G (RT-1949) — Voice and data radio capable of operating SINCGARS, HQ II, VHF/UHF AM and FM, ANW2, MIL-STD-188-181B SATCOM, high-performance waveform SATCOM. (MCRP 3-30B.3 *Tac Radios*, 19 May 2017)

PRC-119 — Voice and data radio capable of operating SINCGARS VHF FM LOS in single channel and FH modes. This is the primary voice communications system for US Army and Marine Corps forces. (MCRP 3-30B.3 *Tac Radios*, 19 May 2017)

PRC-148 — Voice and data radio capable of operating HQ I/II, SINCGARS ESIP in single channel of FH mode; and analog narrowband capable. (MCRP 3-30B.3 *Tac Radios*, 19 May 2017)

PRC-150 — Voice and data radio capable of operating HF ALE. (MCRP 3-30B.3 *Tac Radios*, 19 May 2017)

PRC-152 — Voice and data radio capable of operating SINCGARS, VHF/UHF LOS in AM and FM, HQ II, SATCOM MIL-STD-188-181B. (MCRP 3-30B.3 *Tac Radios*, 19 May 2017)

PRC-153 — Voice radio capable of operating short distances within a small unit/team; primarily used by Marines. (MCRP 3-30B.3 *Tac Radios*, 19 May 2017)

PRC-160 — Voice and data radio capable of operating HF ALE.

proword (procedure word) — A word or phrase limited to radio telephone procedure used to facilitate communication by conveying information in a condensed standard form. (*DOD Dictionary*, 1 Jun 2020)

protected frequencies — Friendly, generally time-oriented, frequencies used for a particular operation, identified and protected to prevent them from being inadvertently jammed by friendly forces while active electromagnetic warfare operations are directed against hostile forces. (*DOD Dictionary*, 1 Jun 2020)

PSC (portable satellite communications). (MCRP 3-30B.3 *Tac Radios*, 19 May 2017)

PSC-5C — Voice and data radio capable of operating VHF and UHF LOS in AM and FM modes, SATCOM, DAMA, IW, ATC, and maritime. (MCRP 3-30B.3 *Tac Radios*, 19 May 2017)

PSC-5D — Voice and data radio capable of operating VHF and UHF LOS in AM and FM modes, SINCGARS, HQ I and II, SATCOM, DAMA, IW, ATC, and maritime. (MCRP 3-30B.3 *Tac Radios*, 19 May 2017)

PT (plain text). (MCRP 3-30B.3 *Tac Radios*, 19 May 2017)

PZ (pickup zone). (FM 1-02.1 *Operational Terms*, 21 Nov 2019)

R&S (reconnaissance and surveillance). (FM 1-02.1 *Operational Terms*, 21 Nov 2019)

RadBn (radio battalion) — A USMC EW unit.

radio silence — The status on a radio network in which all stations are directed to continuously monitor without transmitting, except under established criteria. (FM 1-02.1 *Operational Terms*, 21 Nov 2019)

RF (radio frequency). (*DOD Dictionary*, 1 Jun 2020)

RF CM (radio frequency countermeasures) — Any device or technique employing radio frequency materials or technology that is intended to impair the effectiveness of enemy activity, particularly with respect to precision guided weapons and sensor systems. (*DOD Dictionary*, 1 Jun 2020)

RFID (radio frequency identification). (*DOD Dictionary*, 1 Jun 2020)

RT (receiver transmitter). (MCRP 3-30B.3 *Tac Radios*, 19 May 2017)

RTX (retransmission).

S-2X — Battalion or brigade counterintelligence and human intelligence staff officer. (FM 1-02.1 *Operational Terms*, 21 Nov 2019)

SAA (satellite access authorization). (FM 1-02.1 *Operational Terms*, 21 Nov 2019)

SAASM (selective availability anti-spoofing modules).

SAR (synthetic aperture radar). (*DOD Dictionary*, 1 Jun 2020)

SATCOM (satellite communications) (*DOD Dictionary*, 1 Jun 2020)

SATRAN (satellite reconnaissance advanced notification).

SATVUL (satellite vulnerability) (NTRP 1-02 *Navy Supplement to the DOD Dictionary*, 1 Jun 2012) — A SATVUL period is a window of time when a friendly unit is vulnerable to adversary satellite collections. (NO DOD definition)

SC (single-channel) radio.

SCR (single-channel radio). *See MCR*.

SHF (super-high frequency). (*DOD Dictionary*, 1 Jun 2020) 3–30 GHz.

SINCGARS (single-channel ground and airborne radio system). (*DOD Dictionary*, 1 Jun 2020) — A frequency hopping system for VHF radios.

SIGCON (signature control). (*DOD Dictionary*, 1 Jun 2020)

SIGINT (signals intelligence) — 1. A category of intelligence comprising either individually or in combination all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted. 2. Intelligence derived from communications, electronic, and foreign instrumentation signals. (*DOD Dictionary*, 1 Jun 2020) *SIGINT = COMINT + ELINT + FISINT*.

SIGMAN (signature management) — Signature Management is a systems approach to identifying, reducing, modifying, or intentionally displaying select indicators that, if ignored, could be exploited by an adversary to achieve an operational advantage over friendly forces. (*Marine Corps Concept of Employment for Signature Management*, 12 Dec 2019) (NO DOD definition)

signature — A characteristic of an indicator that makes it identifiable or causes it to stand out. (*Marine Corps Concept of Employment for Signature Management*, 12 Dec 2019) (NO DOD definition)

SLF (super low frequency). 30–300 Hz.

SMART-T (secure mobile anti-jam reliable tactical terminal) — AN/TSC-154 satellite communications system.

SNOOZE (EW brevity code) — Initiate(ing) emission control procedures. Opposite of ALARM. (MCRP 3-30B.1 *Brevity*, 28 May 2020).

SOI (signal operating instructions) — A series of orders issued for technical control and coordination of the signal communication activities of a command. (*DOD Dictionary*, 1 Jun 2020)

SPEED (systems planning engineering and evaluation device).

SPINS (special instructions). (*DOD Dictionary*, 1 Jun 2020)

STRAPEX (boot strap exercise) — A communications configuration exercise.

SUAS (small UAS) —“Group 1 will be referred to as SUAS.” (NAVMC 3500.107A *Group 1 UAS T&R Manua*l, 26 Mar 2014)

TABOO frequencies — Any friendly frequency of such importance that it must never be deliberately jammed or interfered with by friendly forces including international distress, safety, and controller frequencies. (*DOD Dictionary*, 1 Jun 2020)

TAC CHAT (tactical chat).

TACLAN (tactical local area network). (FM 1-02.1 *Operational Terms*, 21 Nov 2019)

TACSAT (tactical satellite). (*DOD Dictionary*, 1 Jun 2020)

TDMA (time division multiple access). (MCRP 3-30B.3 *Tac Radios*, 19 May 2017) — A telecommunications standard used by mobile phone networks.

technical signature — Technical signatures are collected by adversary SIGINT or MASINT assets which can typically only be detected by use of specialized equipment. They include, but are not limited to: electro-optical, infrared, laser, spectral, radar, polarimetric, intentional and unintentional radio frequency emanations, geophysical (acoustic, seismic, hydroacoustic, infrasonic, magnetic, and gravitational), chemical, biological, or nuclear.
(*Marine Corps Concept of Employment for Signature Management*, 12 Dec 2019) (NO DOD definition)

THF (tremendously high frequency). 300–3,000 GHz.

TLF (tremendously low frequency). < 3 Hz.

TPED (transmitting portable electronic device). *See PED.*

TRANSEC (transmission security) — Actions designed to protect communications from interception and the exploitation by means other than cryptoanalysis. (*DOD Dictionary*, 1 Jun 2020) *TRANSEC is equipment engineering to change the signal—by frequency hopping or spread spectrum techniques—to reduce detection and interception, and prevent disruption or deception. Older Army doctrine places TRANSEC as a division of COMSEC.*

TRICS (tactical radio over internet protocol inter-communications system).

TSCM (technical surveillance countermeasures) — Techniques to detect, neutralize, and exploit technical surveillance technologies and hazards that permit the unauthorized access to or removal of information. (*DOD Dictionary*, 1 Jun 2020)

TVA (threat vulnerability assessment) — Provides an in-depth analysis of intelligence, sabotage, subversive, and terrorist threats (and friendly vulnerabilities) associated with a physical installation such as ports, airfields, or base camps. (MCRP 2-10A.2 *Counterintelligence and Human Intelligence*, 21 Nov 2019)

UAS (unmanned aircraft system) — That system whose components include the necessary equipment, network, and personnel to control an unmanned aircraft. (*DOD Dictionary*, 1 Jun 2020)

UFO (UHF follow on).

UHF (ultrahigh frequency). (*DOD Dictionary*, 1 Jun 2020) 300–3,000 MHz.

UHF DAMA (ultrahigh frequency demand assigned multiple access).

UHF SATCOM IW (ultrahigh frequency satellite communications integrated waveform).

ULF (ultra low frequency). 300–3,000 Hz.

VHF (very high frequency). (*DOD Dictionary*, 1 Jun 2020) 30–300 MHz.

VLF (very low frequency). (*DOD Dictionary*, 1 Jun 2020) 3–30 kHz.

VoIP (voice over internet protocol). (FM 1-02.1 *Operational Terms*, 21 Nov 2019)

VRC (vehicle radio communication). (FM 1-02.1 *Operational Terms*, 21 Nov 2019)

VSAT-L (very small aperture terminal-large) — A USMC satellite communications terminal.

VTC (video teleconferencing). (*DOD Dictionary*, 1 Jun 2020)

WAN (wide-area network). (*DOD Dictionary*, 1 Jun 2020)

WCDMA (wideband code division multiple access). (MCRP 3-30B.3 *Tac Radios*, 19 May 2017) *See CDMA.*

WGS (wideband global satellite communications) (*DOD Dictionary*, 1 Jun 2020) — The WGS communications system, called (SATCOM), is a DOD communications satellite network.

WIN-T (warfighter information network-tactical).

ZIPLIP (EW brevity code) — Limit transmissions to critical information only. (MCRP 3-30B.1 *Brevity*, 28 May 2020).

Reference

EP EMCOM Bibliography

Purpose. To SHARE primary sources of EW and EP EMCON guidance.

Throughout this *EP EMCON SOP*, secondary references are listed directly on each page.

Joint Doctrine

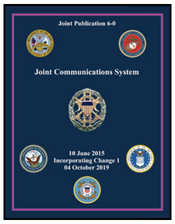
Joint Publication 3-85

Joint Electromagnetic Spectrum Operations

22 May 2020

JP 3-85 *Joint Electromagnetic Spectrum Operations*, 22 May 2020.
148 pages.

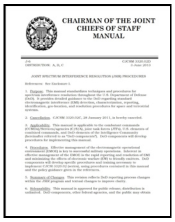
Supersedes JP 3-13.1 Electronic Warfare *and JP 6-01* Joint Electromagnetic Spectrum Management Operations*.*


Joint Publication 6-0

Joint Communications System

10 June 2015
Incorporating Change 1
04 October 2019

JP 6-0 *Joint Communications System*, 4 Oct 2019.
122 pages.


CHAIRMAN OF THE JOINT CHIEFS OF STAFF MANUAL

J-6
DISTRIBUTION: A, B, C

CJCSM 3320.02D
3 June 2013

JOINT SPECTRUM INTERFERENCE RESOLUTION (JSIR) PROCEDURES

References: See Enclosure L

1. Purpose. This manual standardizes techniques and procedures for spectrum interference resolution throughout the U.S. Department of Defense (DoD). It provides detailed guidance to the DoD regarding standard electromagnetic interference (EMI) detection, characterization, reporting, identification, geo-location, and resolution procedures for space and terrestrial systems.

2. Cancellation. CJCSM 3320.02C, 28 January 2011, is hereby canceled.

3. Applicability. This manual is applicable to the combatant commands (CCMDs)/Services/agencies (C/S/A), joint task forces (JTFs), U.S. elements of combined commands, and DoD elements of the Intelligence Community (hereinafter referred to as "DoD components"). DoD components will develop procedures for implementing this manual.

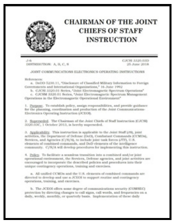
4. Procedures. Effective management of the electromagnetic operational environment (EMOE) is key to successful military operations. Inherent in effective management of the EMOE is the rapid reporting and resolution of EMI and minimizing the effects of electronic warfare (EW) to friendly emitters. DoD components will develop specific procedures and training necessary to implement CJCSI 3320.02 (series), using procedures contained in this manual and the policy guidance given in the references.

5. Summary of Changes. This revision reflects DoD reporting process changes within the JSIR program and textual changes to improve clarity.

6. Releasability. This manual is approved for public release; distribution is unlimited. DoD components, other federal agencies, and the public may obtain

CJCSM 3320.02D *Joint Spectrum Interference Resolution (JSIR) Procedures*, 3 Jun 2013. 60 pages.

See also CJCSI 3320.02F *Joint Spectrum Interference Resolution*, 8 Mar 2013.


CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-6
DISTRIBUTION: A, B, C, S

CJCSI 3320.03D
25 June 2018

JOINT COMMUNICATIONS ELECTRONICS OPERATING INSTRUCTIONS

References:
a. DoDD 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," 16 June 1992
b. CJCSI 3320.01 Series, "Joint Electromagnetic Spectrum Operations"
c. CJCSM 3320.01 Series, "Joint Electromagnetic Spectrum Management Operations in the Electromagnetic Operational Environment"

1. Purpose. To establish policy, assign responsibilities, and provide guidance for the planning, coordination and production of the Joint Communications-Electronics Operating Instruction (JCEOI).

2. Superseded. The Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3320.03C, 1 October 2013, is hereby superseded.

3. Applicability. This instruction is applicable to the Joint Staff (JS), joint activities, the Department of Defense (DoD), Combatant Commands (CCMDs), Services, and Agencies (C/S/A), to include joint task forces (JTF), U.S. elements of combined commands, and DoD elements of the intelligence community. C/S/A will develop procedures for implementing this instruction.

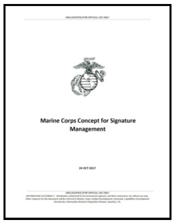
4. Policy. To facilitate a seamless transition into a combined and/or joint operational environment, the Services, Defense agencies, and joint activities are encouraged to incorporate the described policies and procedures into their unique contingency operations, training and exercises.

a. All unified CCMDs and the U.S. elements of combined commands are directed to develop and use a JCEOI to support routine and contingency operations, training, and exercises.

b. The JCEOI offers some degree of communications security (COMSEC) protection by directing changes to call signs, call words, and frequencies on a daily, weekly, monthly, or quarterly basis. Implementation of these daily

CJCSI 3320.03D *JCEOI*, 25 Jun 2018.
18 pages.

U.S. Marine Corps Publications

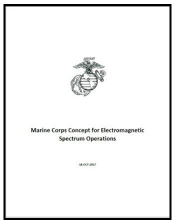

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Marine Corps Concept for Signature Management

24 OCT 2017

UNCLASSIFIED//FOR OFFICIAL USE ONLY
DISTRIBUTION STATEMENT C: Distribution authorized to US Government agencies and their contractors, for official use only. Other requests for this document will be referred to Marine Corps Combat Development Command, Capabilities Development Directorate, Information Warfare Integration Division, Quantico, VA.

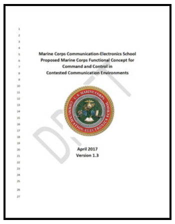
Marine Corps Concept of Employment for Signature Management, 12 Dec 2019.
48 pages.



Marine Corps Concept for Electromagnetic Spectrum Operations

18 OCT 2017

Marine Corps Concept for Electromagnetic Spectrum Operations, 18 Oct 2017. 22 pages.

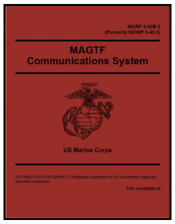


Marine Corps Communication-Electronics School
Proposed Marine Corps Functional Concept for
Command and Control in
Contested Communication Environments

DRAFT

April 2017
Version 1.3

Marine Corps Communications-Electronics School Proposed Marine Corps Functional Concept for Command and Control in Contested Communications Environments, 1 Apr 2019. 40 pages.



MCRP 3-30B.2
(Formerly MCWP 3-40.3)

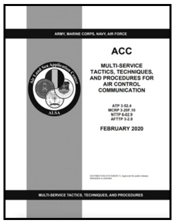
MAGTF
Communications System

US Marine Corps

DISTRIBUTION STATEMENT C: Distribution authorized to US Government agencies and their contractors.

PCN 144 000256 00

MCRP 3-30B.2 *MAGTF Communications System*, 2 May 216. 230 pages.



ARMY, MARINE CORPS, NAVY, AIR FORCE

ACC

MULTI-SERVICE
TACTICS, TECHNIQUES,
AND PROCEDURES FOR
AIR CONTROL
COMMUNICATION

ATP 3-52.4
MCRP 3-20F.10
NTTP 6-02.9
AFTTP 3-2.8

FEBRUARY 2020

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

MULTI-SERVICE TACTICS, TECHNIQUES, AND PROCEDURES

MCRP 3-20F.10 *ACC: Multi-Service TTPs for Air Control Communication*, 14 Feb 2020. 96 pages.

ARMY, MARINE CORPS, NAVY, AIR FORCE

BREVITY

MULTI-SERVICE TACTICS,
TECHNIQUES, AND PROCEDURES
FOR MULTI-SERVICE BREVITY
CODES

ATP 1-02.1
MCRP 3-30B.1
NTTP 6-02.1
AFTTP 3-2.5

MAY 2020

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.
This determination was made on [02 OCT 2019].

*Supersedes ATP 1-02.1/MCRP 3-30B.1/NTTP 6-02.1/AFTTP 3-2.5, dated 20 June 2018.

MULTI-SERVICE TACTICS, TECHNIQUES, AND PROCEDURES

MCRP 3-30B.1 *Brevity: Multi-Service TTPs for Brevity Codes*, 28 May 2020. 90 pages.

Defines standard ***brevity codes****. See the glossary of EW terms on page 73. Chapter II lists tactical chat abbreviations.*

ARMY, MARINE CORPS, NAVY, AIR FORCE

TAC RADIOS

MULTI-SERVICE
TACTICS, TECHNIQUES,
AND PROCEDURES FOR
TACTICAL RADIOS

ATP 6-02.72
MCRP 3-30B.3 [MCRP 3-40.3A]
NTTP 6-02.2
AFTTP 3-2.18

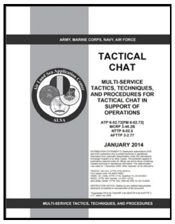
MAY 2017

DISTRIBUTION STATEMENT D: [illegible]

DESTRUCTION NOTICE: Destroy by any method that prevents disclosure of contents or reconstruction of the document.

MULTI-SERVICE TACTICS, TECHNIQUES, AND PROCEDURES

MCRP 3-30B.3 *Tac Radios: Multi-Service TTPs for Tactical Radios*, 19 May 2017. 200 pages.



ARMY, MARINE CORPS, NAVY, AIR FORCE

TACTICAL
CHAT

MULTI-SERVICE
TACTICS, TECHNIQUES,
AND PROCEDURES FOR
TACTICAL CHAT IN
SUPPORT OF
OPERATIONS

ATP 6-02.73[FM 6-02.73]
MCRP 3-40.2B
NTTP 6-02.8
AFTTP 3-2.77

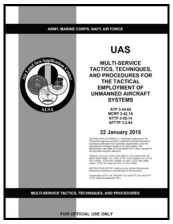
JANUARY 2014

DISTRIBUTION STATEMENT D: [illegible]

DESTRUCTION NOTICE: Destroy by any method that prevents disclosure of contents or reconstruction of the document.

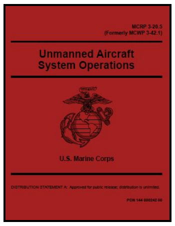
MULTI-SERVICE TACTICS, TECHNIQUES, AND PROCEDURES

MCRP 3-40.2B *Tactical Chat: Multi-Service TTPs for Tactical Chat in Support of Operations*, 17 Jan 2014. 80 pages.

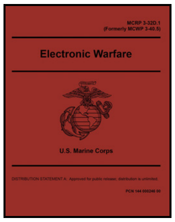

ARMY, MARINE CORPS, NAVY, AIR FORCE
UAS
MULTI-SERVICE TACTICS, TECHNIQUES, AND PROCEDURES FOR THE TACTICAL EMPLOYMENT OF UNMANNED AIRCRAFT SYSTEMS
22 January 2015
MULTI-SERVICE TACTICS, TECHNIQUES, AND PROCEDURES
FOR OFFICIAL USE ONLY

MCRP 3-42.1A *UAS: Multi-Service TTPs for the Tactical Employment of UAS*, 22 Jan 2015. 110 pages.

No discussion of EW, EP, or EMCON concerns or procedures for UAS.

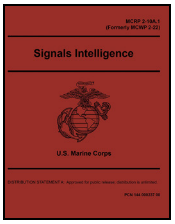


MCRP 3-20.5 *Unmanned Aircraft System Operation*s, 2 May 2016.
61 pages.



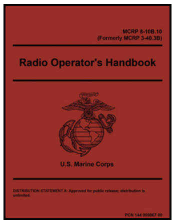
MCRP 3-32D.1 *Electronic Warfare*, 4 Apr 2018.
148 pages.

*Out-of-date **2002** manual: Incorrect terms, old organizations, and zero discussion of modern threat capabilities. Re-numbered in 2016. Gender-neutralized in 2018.*



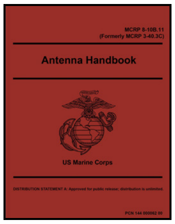
MCRP 2-10A.1 *Signals Intelligence*, 4 Apr 2018.
125 pages.

*Out-of-date **1999** publication. Re-numbered in 2004 and 2016. Gender-neutralized in 2018. Incorrect terms and old equipment.*



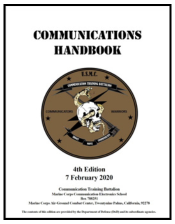
MCRP 8-10B.10 *Radio Operator's Handbook*, 4 Apr 2018.
152 pages.

*Out-of-date **1999** publication. Re-numbered in 2001 and 2016. Gender-neutralized in 2018.*



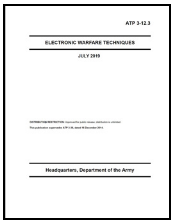
MCRP 8-10B.11 *Antenna Handbook*, 2 May 2016.
193 pages.

*Out-of-date **1999** publication. Re-numbered in 2001 and 2016.*



CTB Communications Handbook, 4th Edition. MCAGCC, CA: MCCES CTB, 7 Feb 2020. 232 pages.

U.S. Army Publications



ATP 3-12.3

ELECTRONIC WARFARE TECHNIQUES

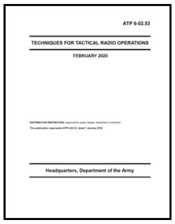
JULY 2019

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

This publication supersedes ATP 3-36, dated 16 December 2014.

Headquarters, Department of the Army

ATP 3-12.3 *Electronic Warfare Techniques*, 16 Jul 2019.
124 pages.



ATP 6-02.53

TECHNIQUES FOR TACTICAL RADIO OPERATIONS

FEBRUARY 2020

Headquarters, Department of the Army

ATP 6-02.53 *Techniques for Tactical Radio Operations*, 13 Feb 2020.
218 pages.

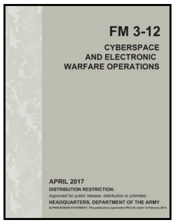
ATP 6-02.54

TECHNIQUES FOR SATELLITE COMMUNICATIONS

JUNE 2017

Headquarters, Department of the Army

ATP 6-02.54 *Techniques for Satellite Communications*, 5 Jun 2017.
106 pages.



FM 3-12

CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS

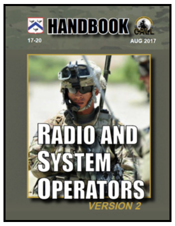
APRIL 2017

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited

HEADQUARTERS, DEPARTMENT OF THE ARMY

SUPERCESSION STATEMENT: This publication supersedes FM 3-38, dated 12 February 2014.

FM 3-12 *Cyberspace and Electronic Warfare Operations*, 11 Apr 2017.
108 pages.

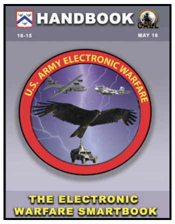


HANDBOOK

17-20 AUG 2017

RADIO AND SYSTEM OPERATORS VERSION 2

CALL 17-20 *Radio and System Operators Handbook V2*, 1 Aug 2017.
412 pages.



HANDBOOK

16-15 MAY 16

THE ELECTRONIC WARFARE SMARTBOOK

CALL 16-15 *The Electronic Warfare Smartbook*, 1 May 2016.
160 pages.

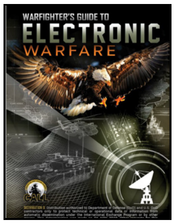
HANDBOOK

NO. 18-28 JUN 2018

OPERATING in a DENIED, DEGRADED, and DISRUPTED SPACE OPERATIONAL ENVIRONMENT

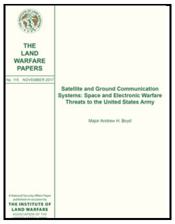
LESSONS AND BEST PRACTICES

CALL 18-28 *Operating in a Denied, Degraded, and Disrupted Space Operational Environment*, 1 Jun 2018. 128 pages.



CALL 20-05 *Warfighter's Guide to Electronic Warfare*, 6 Nov 2019.
229 pages.

Papers and Articles


THE LAND WARFARE PAPERS
Satellite and Ground Communication Systems: Space and Electronic Warfare Threats to the United States Army

Andrew Boyd. *Satellite and Ground Communication Systems: Space and Electronic Warfare Threats to the United States Army*. Arlington, VA: AUSA, Nov 2017. 39 pages.

Our systems are overly dependent on SATCOM. Reducing this satellite dependency makes us more *vulnerable to adversary ES direction finding.*

Space Threat Assessment 2020. Washington DC: **Center for Strategic and International Studies** (CSIS), 2020. 80 pages. **csis.org**

Summarizes government and commercial satellites. Although primarily a report on adversary counterspace capabilities, CSIS provides insight into the increasing technological advancements of great powers and illuminates U.S. vulnerabilities.

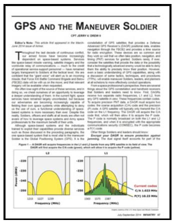
Michael S. Chase, *et al.* *Emerging Trends in China's Development of Unmanned Systems.* Rand Corporation, 2015. 14 Pages. **rand.org**

Explains emerging Chinese UAS capabilities and how aerial collections are integrated with long-distance targeting.

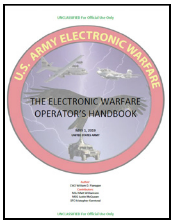
SOUTH CHINA SEA MILITARY CAPABILITY SERIES
ELECTRONIC WARFARE AND SIGNALS INTELLIGENCE

J. Michael Dahm. *Electronic Warfare and Signals Intelligence*. Johns Hopkins Applied Physics Laboratory, 1 Aug 2020. 35 pages.

Challenges to Security in Space. **Defense Intelligence Agency**, 2019.
46 pages. www.dia.mil/Military-Power-Publications



Jerry Drew. "GPS and the Maneuver Soldier." *Infantry*, Jul-Sep, 2014, pages 47–50.



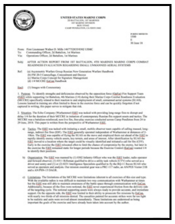
UNCLASSIFIED For Official Use Only

U.S. ARMY ELECTRONIC WARFARE

THE ELECTRONIC WARFARE OPERATOR'S HANDBOOK

UNCLASSIFIED For Official Use Only

William Flanagan. *The Electronic Warfare Operator's Handbook*. Fort Irwin, CA: NTC, 1 May 2017. 136 pages.



Adam Gilbert. *EWST Attachment to 3/3 After Action Report: 07 Oct - 03 Nov 2028*. MCBH Kaneohe Bay HI, 3rd RadBn, 8 Nov 2018.

Lester Grau and Charles Bartles. The Russian Reconnaissance Fire Complex Comes of Age. Oxford, England: University of Oxford, 30 May 2018.

COMBATING TERRORISM CENTER

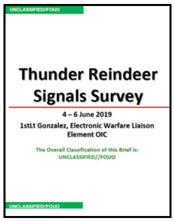
THE ISLAMIC STATE AND DRONES

SUPPLY, SCALE, AND FUTURE THREATS

Don Rassler

Don Rassler. The Islamic State and Drones: Supply, Scale, and Future Threats. West Point, NY: U.S. Military Academy, 2018. **ctc.usmc.edu**

Details ISIS innovation and use of SUAS.



UNCLASSIFIED/FOUO

Thunder Reindeer Signals Survey

4 – 6 June 2019

1stLt Gonzalez, Electronic Warfare Liaison Element OIC

The Overall Classification of this Brief is: UNCLASSIFIED//FOUO

UNCLASSIFIED/FOUO

Gabriella Ritter-Gonzalez. *Thunder Reindeer Signals Survey: 4–6 June 2019*. Boblingen, DEU: MARFOREUR/AF, 30 Jun 2020.

Small Unmanned Aerial System Adversary Capabilities

HSOAC

Bradley Wilson, et al. Small Unmanned Aerial System Adversary Capabilities. Rand Corporation, 2020. 147 Pages. **rand.org**

Comprehensive explanations of UAS ***terms***, ***proliferation***, *and* ***TTPs***.
See chapter four for tactical use of UAS.

Contributors: BBM, 1 Nov 2020.

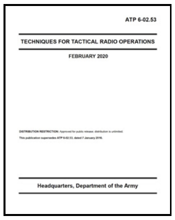
Reference

Prowords and Brevity Codes

Purpose. To REDUCE the length of radio calls IOT AVOID being located and targeted.

Procedures

1. USE **prowords** to REDUCE the length of radio transmissions. A proword is “A word or phrase limited to radio telephone procedure used to facilitate communication by conveying information in a **condensed** standard form.” (*DOD Dictionary*, 1 Jun 2020).



ATP 6-02.53

TECHNIQUES FOR TACTICAL RADIO OPERATIONS

FEBRUARY 2020

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

This publication supersedes ATP 6-02.53, dated 7 January 2016.

Headquarters, Department of the Army

ATP 6-02.53 *Techniques for Tactical Radio Operations*, 13 Feb 2020.
218 pages.

Appendix I defines the 47 standard **prowords**.

Table 1. Voice radio prowords.

ACKNOWLEDGE	**DO NOT ANSWER**	**I SAY AGAIN**	**ROGER**	**VERIFY**
ALL AFTER	EXEMPT	**I SPELL**	ROUTINE	**WAIT**
ALL BEFORE	**FIGURES**	I VERIFY	**SAY AGAIN**	**WILCO**
AUTHENTICATE	FLASH	MESSAGE	**SILENCE**	WORD AFTER
AUTHENTICATION IS	FROM	**MORE TO FOLLOW**	**SILENCE LIFTED**	WORD BEFORE
BREAK	GROUPS	**OUT**	**SPEAK SLOWER**	WORD TWICE
CLEAR	I AUTHENTICATE	**OVER**	**THIS IS**	**WRONG**
CORRECT	IMMEDIATE	PRIORITY	**TIME**	
CORRECTION	**INFO**	**READ BACK**	**TO**	
DISREGARD [1]	**I READ BACK**	**RELAY (TO)**	**UNKNOWN STATION**	

Source: ATP 6-02.53. Appendix C of MCRP 8-10B.10 *Radio Operator’s Handbook*, 4 Apr 2018, lists the old prowords as of 1999. **Notes:** 1. Full proword is DISREGARD THIS TRANSMISSION-OUT. Commonly-used prowords are **bolded**. Others, used for message traffic, are rarely used.

Proword Examples

Proword Transmission	Notes
“2-3, 2-2. POSREP. Checkpoint 1-6-B. BREAK. What vehicles are at phase line AMBER? OVER.”	BREAK indicates a new subject. BREAK can indicate a new recipient. AVOID repetition: “BREAK, BREAK, BREAK.”

Proword Transmission	Notes
"2-2, 2-3. POSREP. Grid 1-5-3… CORRECTION. Grid 1-5-5, 2-7-7. OVER."	CORRECTION fixes an error.

Proword Transmission	Notes
"2-3, 2-2. SAY AGAIN number of vehicles?" "2-2, 2-3. I SAY AGAIN. Two-zero vehicles in PZ."	SAY AGAIN asks for confirmation of critical information. Do NOT say "REPEAT." Transmit numbers digit by digit.

Proword Transmission	Notes
"2-3, 2-2. Understand your ETA is 1600. OUT."	OUT is the end of the transmission. Do NOT respond. Since OUT and OVER have opposite meanings, they are never used together.

Proword Transmission	Notes
"2-2, 2-3. Enemy sighted! WAIT. OUT."	WAIT indicates a pause. WAIT OUT indicates that I will call you back later.

Proword Transmission	Notes
"2-3. Move to phase line AMBER, OVER." "WILCO, OUT.	WILCO indicates I understand and **will comply**. SINCE the meaning of ROGER is included in WILCO, the two prowords are not used together.

2. USE **brevity codes** to REDUCE the length of radio transmissions. A brevity code is "A code word, which provides no security, that serves the sole purpose of shortening of messages rather than the concealment of their content." (*DOD Dictionary*, 1 Jun 2020)

USE standard **brevity codes** defined by MCRP 3-30B.1. Unit SOPs should define commonly-used brevity codes. All types of units—artillery, reconnaissance, engineers—use different subsets of common brevity codes.

ARMY, MARINE CORPS, NAVY, AIR FORCE

BREVITY

MULTI-SERVICE TACTICS, TECHNIQUES, AND PROCEDURES FOR MULTI-SERVICE BREVITY CODES

ATP 1-02.1
MCRP 3-30B.1
NTTP 6-02.1
AFTTP 3-2.5

MAY 2020

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.
This determination was made on [02 OCT 2019]

*Supersedes ATP 1-02.1/MCRP 3-30B.1/NTTP 6-02.1/AFTTP 3-2.5, dated 20 June 2016.

MULTI-SERVICE TACTICS, TECHNIQUES, AND PROCEDURES

MCRP 3-30B.1 *Brevity: Multi-Service TTPs for Brevity Codes*, 28 May 2020.
90 pages.

*Defines standard **brevity codes**, primarily originated by aviation units.*
EW terms are listed on page 73.

Table 2. Example brevity codes commonly used in ground-air communications.

Target Location	Friendly Location	Laser Targeting	EW	Aircraft ID
TALLY	VISUAL	TEN SECONDS	ALERT	BOGEY
NO JOY	BLIND	LASER ON	BUZZER	FRIENDLY

		LASING	SNOOZE	NEUTRAL
		SHIFT	ZIPLIP	HOSTILE
IR Markings	**IR Markings**	**Timeline**	**CAS**	**Status**
SNAKE	ROPE	ROLEX	CONTACT	WINCHESTER
SPARKLE	BUZZSAW	ETA	CLEARED HOT	BINGO

Brevity Codes Examples

Brevity code transmission	Notes
“2-3, 2-2. ROLEX LD plus twenty. OVER.” “2-2, 2-3. ROGER. LD at 1520. OVER”	ROLEX adjusts the timeline from a known point. “Plus” means later. “Minus” means earlier. Five minute increments. Two ROLEX calls are NOT additive. On covered nets, confirm with an absolute time hack. Relative time hacks—“in 30 minutes”— are easily misunderstood.

Brevity code transmission	Notes
“BRAVO-5, TALON-3. I have a VISUAL on your ROPE. OVER.” “From my position. Northeast 900 meters. SNAKE on the bridge.”	VISUAL indicates a friendly position. Opposite is BLIND. ROPE is circling an IR pointer. SNAKE is an IR pointer making a figure eight.
“I CONTACT the bridge.”	CONTACT is sighting a reference point.
“SHIFT north 100 meters. Two trucks by a building.”	SHIFT is moving an IR pointer.
“I TALLY two trucks north of the bridge.”	TALLY: enemy target seen. Opposite is NO JOY.

3. USE **execution checklists** to REDUCE the length of radio transmissions. An execution checklist is a list of **brevity codes** for a specific mission. Unit SOPs should define standard execution checklists for all recurring operations.

Execution Checklist: Raid on OBJ Zumat - 210920

		Event	Net	From	To	Time	Actual	Brevity Code
01	M	R/W CAS at BP ASP	HD-1	EFL	AMC	L-30		ANNIE
02	M	F/W CAS on station	HD-1	DASC	AMC	L-30		BETTY
03	M	F/W strike on OBJ 3 complete	HD-1	EFL	DASC			CATHY
04	M	Assault package in PZ	HD-1	Evil	AMC	L-30		DEBBIE
05	X	Assault package in LZ	HD-1	AFL	AMC	L-Hour		SUZY
10	M	“E” inserted at LZ	Tac-1	RFC	MC	L-Hour		PACKERS
11	M	“E” in ATK Pos	Tac-1	RFC	MC			STEELERS
12	X	“E” R/W suppression done	TAD	FAC	EFL			RAIDERS
13	M	OBJ secured	Tac-1	RFC	MC			VIKINGS

50	X	Friendly casualties	Tac-1	RFC	MC			BUDWEISER
51	X	Civilians in target area	Tac-1	RFC	MC			COORS

M - Mandatory, X - As required

Execution Checklist Best Practices

LIST each **event** in rough chronological order. List the minimum number of events that need **radio calls** to execute the SOP. Some internal events do NOT need radio calls. NUMBER events in separate decades to indicate phases.

IDENTIFY **mandatory**, mission-critical radio calls: ‘M’ is ‘mandatory’ and ‘X’ is ‘as required.’ LIST contingency radio calls—safety, enemy engagement, or CASEVAC—in gray at the bottom of the execution checklist.

ASSIGN who is responsible for each radio call: **Net**, **From**, and **To**. Note the technology of each net: ‘TAD (UHF)’ or ‘Tac1 (VHF FH).’

Time only scheduled events: ‘H-15.’ Do NOT estimate timing for every event on a rigid schedule. **Actual** time is filled in during the mission.

GROUP **Brevity** codes by theme. Aviation calls can be girls’ names and ground calls can be football teams. Some events do NOT need a brevity code.

For ease of memorization, use the *same standard brevity code* for the *same event* across all missions, particularly contingencies. No one remembers fifty brevity codes. Aviators do this well.

AVOID assigning a single overall theme to each separate mission: ‘TRAP codes are all BASEBALL teams.’ Under this model, the standard event, ‘Security element in position,’ would have a *different* brevity code for each different mission. This is NOT a best practice.

ENSURE no brevity code duplicates existing control measures or callsigns. SYNCHRONIZE brevity codes with higher, subordinate, adjacent, and supporting units to avoid misunderstandings.

The best brevity code is a two-syllable word, with the accent the first syllable, that starts with a hard consonant sound: “KICKBACK” is better than “CAESAR” or “DEBRIS.” Avoid four-syllable words.

TITLE and DATE the execution checklist for a specific mission in one AO against a specific adversary. During operations, do NOT state a brevity code unless it is TRUE. To inquire on the status of a given event, use the line number: “SAY AGAIN status of line eleven, OVER.”

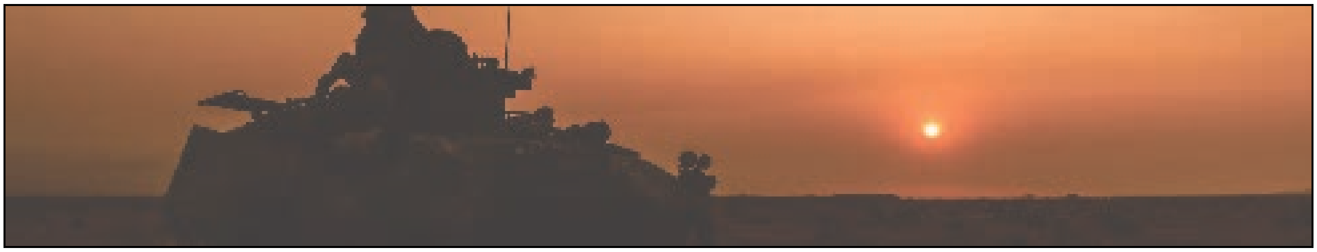
Brevity code transmission	Notes
“2-3, 2-2. SAY AGAIN status of line eleven. OVER.” “2-2, 2-3. STEELERS. I SAY AGAIN STEELERS. OVER.”	Use line numbers to inquire.

Contributors: **BBM**, ELK, 1 Nov 2020.

Reference

Example Annex K EP EMCON Plan

Purpose. To REDUCE electromagnetic emissions IOT AVOID being located and targeted.



Process for the S-6

1. DETERMINE adversary ES collections capabilities in the AO.
   DETERMINE friendly communications requirements for the mission.
   REDUCE friendly electromagnetic emissions by establishing EP EMCON guidance.

2. READ EMSO guidance from HHQ: EMSO plans and EMS operating instructions.

3. WRITE the Annex K. **WRITE a good EMCON SOP.** In the Annex K, **reference the SOP.**

4. COORDINATE EP EMCON planning with the S-3 and subordinate commanders.

Example Annex K

2/5
BLAZ, GUM
1 Nov 2020

Tab B to Appendix 3 (EW) to Annex K (Combat Information Systems) to OPORDER 1-20
Electromagnetic Protection (EP)

Ref: (a) ***EP EMCON SOP***

1. Adversary ES collections—airborne electromagnetic reconnaissance and DF capability—in the AO is PROBABLE (80%). IDF threat is IMPROBABLE (45%). See Annex B for adversary EOB.

2. All battalion operations will be conducted at EMCON 2 under an assumption of near-continuous adversary collections. Assault support inserts and extracts are most vulnerable to adversary collections.

3. Execution

   a. CONOPS for EP. COMSEC and EMCON will be executed IAW ***EP EMCON SOP***.

   b. Tasks for all units: organic, attached, and DS

      (1) SET and brief EMCON for each mission IAW ***EP EMCON SOP***.

(2) SUBMIT execution checklist and EMCON matrix for each mission at H-4:00 IAW ***EP EMCON SOP***.

(3) REPORT battle rhythm events ONLY during established comm windows IAW ***EP EMCON SOP***.

c. Coordinating Instructions

(1) Baseline for all missions is EMCON 2 IAW ***EP EMCON SOP***.

(2) Set and change EMCON, and transmit EMCON directives, IAW ***EP EMCON SOP***.

(3) CEOI, SPINS, and PACE plans will be updated weekly IAW ***EP EMCON SOP***.

(4) REPORT EMI IAW ***EP EMCON SOP***.

Notes

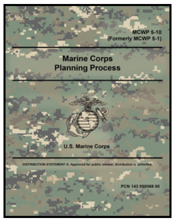
There is no published example of a Marine Corps Annex K (Combat Information Systems) that includes EP EMCON guidance. There is no example of an Annex C (Operations) that includes EW or EP EMCON guidance.

Training reduces the requirements for orders. Well-trained units, with well-understood SOPs, execute practiced EP EMCON procedures.

References

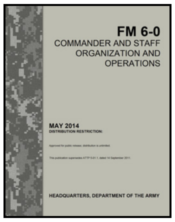
MCRP 3-30B.2 *MAGTF Communications System*, 2 May 2016.
230 pages.

Appendix F includes a sample Annex K "Communications Plan," but no EP or EMCON guidance.



MCWP 5-10 *Marine Corps Planning Process*, 4 Apr 2018.
184 pages.

No example Annex K "Combat Information Systems," and no guidance on EP or EMCON. In Appendix C3 "Information Operations," Tab C3B is titled "Electronic Warfare," but no example is included.



FM 6-0 *Commander and Staff Organization and Operations*, 22 Apr 2016.
394 pages.

Appendix C is "Plans and Orders Formats." In the Army order format, Appendix C12 is "Cyber Electromagnetic Activities" and Tab D (C12D) is "Electromagnetic Protection."

Contributors: **BBM**, 1 Nov 2020.

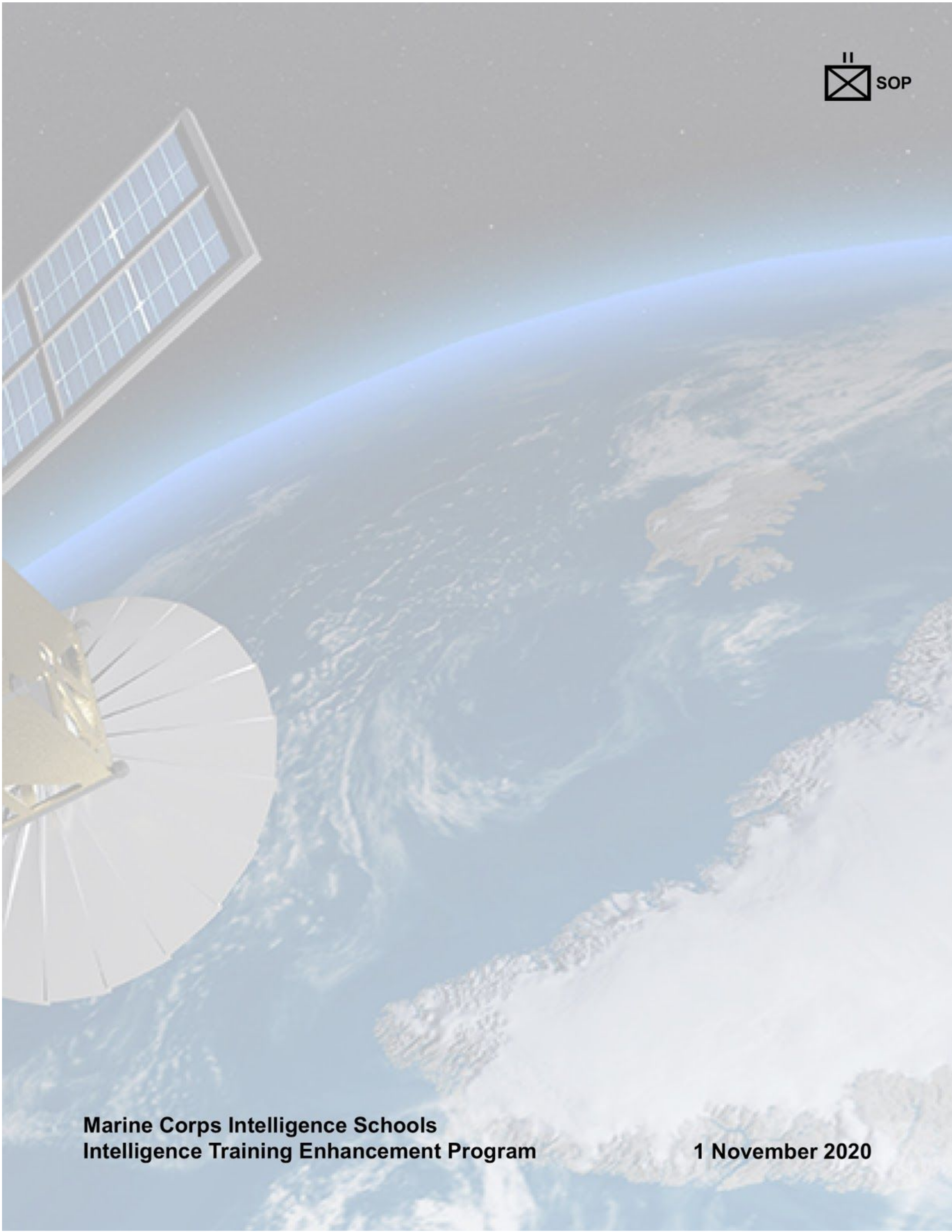
SIGMAN EP EMCON SOP:
A Guide to Reduce Technical Signature

Marine Corps Intelligence Schools (MCIS)
Intelligence Training Enhancement Program (ITEP)

1 November 2020

What is an SOP? *An SOP standardizes recurring procedures IOT save time on detailed orders. An SOP is directive and specific, setting clear coordination measures without explanation or justification. An SOP is NOT a checklist or a repetition of doctrine. An SOP does NOT replace tactical judgement. The endstate of an SOP is* ***execution****, not publication. Well-trained units execute a standard procedure with little or no direction.*

Photo credits: *Official Marine Corps photographs are in the public domain.* ***www.marines.mil***



II SOP

Marine Corps Intelligence Schools
Intelligence Training Enhancement Program

1 November 2020