

# Joint Counter Radio Controlled IED Electronic Warfare Handbook

GTA 90-10-047

15 Mar 2007

Expires 15 Mar 2008



**FOR OFFICIAL USE ONLY**

# JOINT COUNTER RADIO CONTROLLED IMPROVISED EXPLOSIVE DEVICE ELECTRONIC WARFARE (JCREW) HANDBOOK

## DISTRIBUTION RESTRICTION

The information in this handbook is classified "For Official Use Only (FOUO)," and will be handled in accordance with the following guidelines to prevent unauthorized disclosure outside the U.S.

Department of Defense (DoD) and its contractors, and to prevent automatic dissemination under the International Exchange Program:

*Do not store electronic copies of this handbook on unclassified servers that do not have appropriate user access restrictions to prevent its unauthorized disclosure or transmission.*

*Do not transmit this handbook via any unsecured e-mail network, to include the DoD Non-classified Internet Protocol Router Network (NIPRNet).*

*Do not distribute this handbook outside of DoD without authorization from the Director, Joint Improvised Explosive Device Defeat Organization (JIEDDO), 5000 Army Pentagon, Washington, D.C., 20310-5000.*

Unit commanders may duplicate and distribute this handbook as necessary in accordance with the above specified handling instructions.

## DESTRUCTION NOTICE

Destroy by any method that will prevent disclosure of contents or reconstruction of the document.

**FOR OFFICIAL USE ONLY**

## Forward

“SENDING SOLDIERS TO WAR WITHOUT **TRAINING** ON THEIR EQUIPMENT IS THE SAME AS SENDING THEM TO WAR WITHOUT **EQUIPMENT.**”

**KEEP THIS IN MIND:  
“THE ENEMY...IS ALWAYS WATCHING”**

Do not allow yourself to get lulled into the fatal habits of complacency.

TO OBTAIN ADDITIONAL COPIES OF THIS HANDBOOK REFER TO THE FOLLOWING LOCATIONS:

- Knowledge and Information Fusion Exchange  
<https://knife.jfcom.smil.mil>
- JCREW Web Portal  
<https://ieddefeat.jfcom.smil.mil>  
<http://ieddefeat.jfcom.mil>
- General Dennis Reimer Training and Doctrine Digital Library  
<http://www.train.army.mil/>
- Your Service Training Support Center



## OPSEC IS CRITICAL!!

- CREW information in this handbook is sensitive and FOR OFFICIAL USE ONLY (FOUO)\*.
- Do not talk about sensitive information in open areas. Do not share information with or talk to anyone who doesn't have a need to know.
- All CREW systems are high value sensitive items and require safeguarding.
- Guard all written information and dispose of material based on local security manager's (S2) policies.

### **Clearance + Need to Know = Access**

- Your Electronic Warfare Officer and Staff Planners have access to more (classified) information than you need to know to properly operate your system.
- The Joint CREW Security Classification Guide (OPNAVINST S5513.8B-88) includes designation of the following as SECRET:
  - Frequencies (programming loads)
  - Power (per frequency or across a range)
  - The specific techniques or methods used to defeat a Radio Controlled IED.
- Mission information about CREW systems is classified at the level of the mission.

**Your life may depend on keeping this information safe!**

*\* FOR OFFICIAL USE ONLY is a designation for information that if released could be expected to endanger the life or physical safety of an individual (DoDI 5200.1-R).*

## **CREW Table of Contents**

<b>Chapter 1 Electronic Warfare (EW) Principles .....</b>	<b>1</b>
1.1 Electronic Warfare .....	2
1.2 EW Components.....	3
1.3 Line-of-Sight (LOS).....	6
1.4 Masking .....	7
1.5 Frequency (FREQs).....	8
1.6 Frequency De-confliction .....	9
1.7 Power .....	9
1.8 Jamming Basics.....	10
1.9 Hard Truth.....	11
<b>Chapter 2 Improvised Explosive Device (IED) Threat and Tactics .....</b>	<b>13</b>
2.1 Definition and components of an IED .....	14
2.2 Enemy tactics .....	19
<b>Chapter 3 Electronic Warfare Officer (EWO) and Staff Planning.....</b>	<b>23</b>
3.1 EWO Process Flow .....	23
3.2 Basic EWO Responsibilities.....	24
3.3 Pre-mission EWO Responsibilities.....	27
3.4 Post-mission Responsibilities .....	29
<b>Chapter 4 CREW Systems.....</b>	<b>31</b>
4.1 Jammer Types .....	32
4.2 Preventative Maintenance Checks and Services (PMCS).....	33
4.3 Acorn System .....	45
4.4 Beech System.....	49
4.5 Blue System.....	52

**CREW Table of Contents (cont'd)**

4.6 Chameleon Electronic Countermeasure (ECM) System.....	58
4.7 Cottonwood System.....	71
4.8 Duke System .....	81
4.9 Guardian D (QRD) System.....	95
4.10 Green System.....	102
4.11 Hunter System.....	109
4.12 Ironwood System.....	113
4.13 mICE System.....	119
4.14 MMBJ System.....	122
4.15 Pecan System.....	125
4.16 Red System .....	129
4.17 Red / Green Combo .....	132
4.18 Spruce System .....	134
4.19 SSVJ System.....	138
4.20 Warlock LX System.....	141

**Chapter 5 CREW System Interoperability and Communication Alternatives ..... 149**

5.1 CREW System Interoperability.....	149
5.2 Communications Alternatives .....	153

**Chapter 6 Employment Considerations..... 155**

6.1 Pre-Convoy Measures .....	155
6.2 In-Convoy Measures.....	157
6.3 Post-Convoy Measures .....	172

**Additional Sources of Information**

**Acronym Decoder**

**Acknowledgements**

**Table of Figures**

**Systems Interoperability Chart.....Inside Back Cover**

**FSR Phone List.....Back Cover**

**FOR OFFICIAL USE ONLY**

# Chapter 1

## Electronic Warfare (EW)

### Principles

#### What you will learn in this chapter

##### Six Key Factors of Electronic Warfare

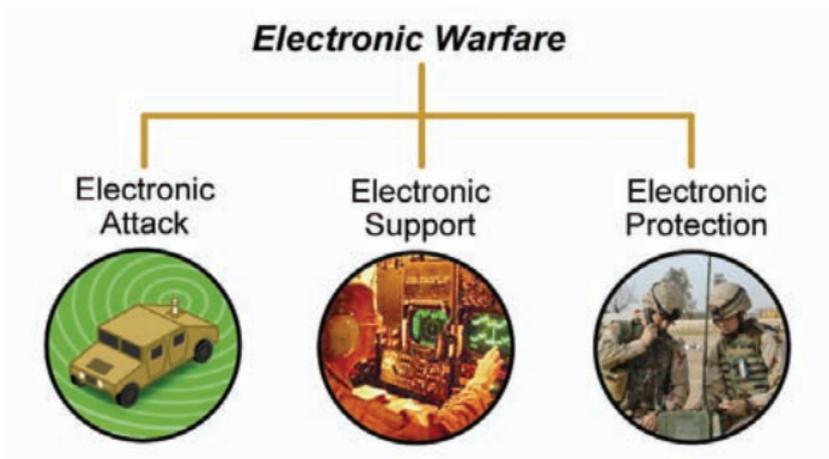
- What is a Transmitter?
- What is a Receiver?
- What is a Jammer?
- What is Line of Sight (LOS)?
- What is the impact of Masking?
- What are Frequencies?



This booklet provides information about how **CREW** systems defeat Radio Controlled Improvised Explosive Device (RCIED) threats. You will be provided with a few definitions and considerations that will help you understand these valuable tools.

## 1.1 Electronic Warfare

How does **Counter RCIED Electronic Warfare (CREW)** fit in to the bigger EW picture?



**Figure 1 - Components of Electronic Warfare**

- **Electronic Attack (EA)** - Active or reactive use of the electromagnetic spectrum by denying its use by the enemy. **Electronic Counter Measures (ECM)** (jamming) are used for Electronic Attack (EA).
- **Electronic Support (ES)** - The search, interception, identification, and location of sources of radiated energy.
- **Electronic Protection (EP)** - Protecting our own use of the Electromagnetic Spectrum.



In Electronic Warfare, the jammer is an offensive capability. A weapon fires bullets; a jammer fires electronic noise. **Both subdue the enemy.**

## 1.2 EW Components

### What are Transmitters, Receivers and Jammers?

#### Transmitter

- A *transmitter* is a device that sends information by radio frequency to a receiver.
- Transmitters send information on specific frequencies.
- The enemy forces use radio controlled transmitters to detonate RCIEDs.

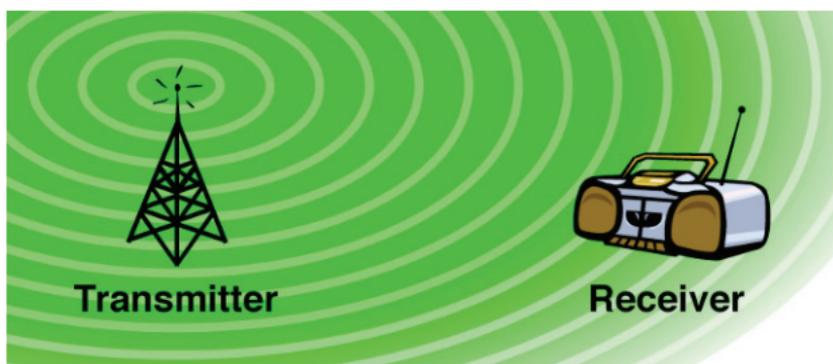


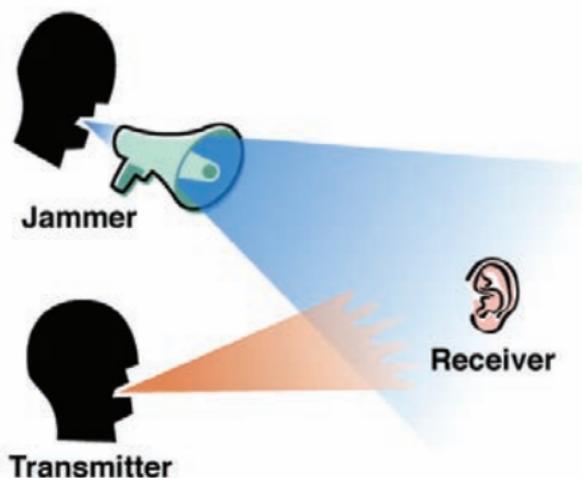
Figure 2 - Typical Communication

#### Receiver

- A *receiver* is the listening end of a communication channel from a transmitter.
- Receivers are tuned to specific frequencies and react when they hear a signal on those frequencies.
- An RCIED uses a receiver to acquire trigger signals from a transmitter.

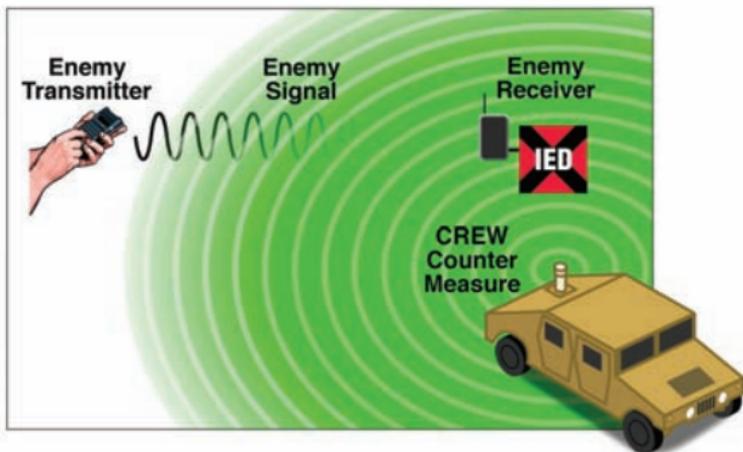
## Jammer

A *jammer* is a special transmitter that prevents a receiver from “hearing” a detonation command.



**Figure 3 - Jamming Simplified**

- Jamming is the use of a second radio transmitter at the same frequency as the first transmitter with higher power.
- Jamming prevents the receiver from getting an understandable signal.
- When a jammer is in use, the enemy transmitter is still talking at the same “volume” as before.



**Figure 4 - CREW Jamming**

- The jammer transmits a similar signal at a much higher volume, which distorts the command signals.
- The function of the jammer is to confuse the receiver enough to disable the capability for the receiver to act on the transmitter's instructions.

That is how CREW systems help protect you from the RCIED threat.

A **transmitter** sends the electronic information while the **receiver** is *listening* for the information. The **jammer** works to *block* the **receiver** from getting the information.

## 1.3 Line-of-Sight (LOS)

**How does Line-of-Sight impact the jammers capability to block the IED?**

LOS commonly refers to Radio Frequency (RF) communication links that rely on an unobstructed straight line (a clear path) between a transmitting antenna and a receiving antenna.

- If the CREW system does not have Line-of-Sight to the RCIED it cannot defeat it.
- Other types of IED triggers (pressure plate, etc.) do not need a clear LOS. They rely on other methods of transmitting the detonate commands.

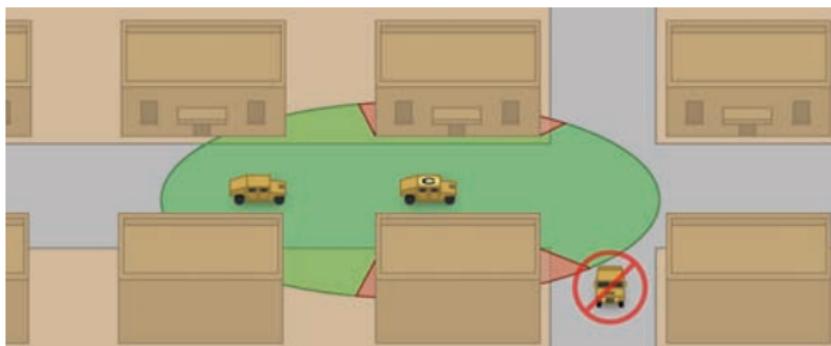


**Figure 5 - Line-Of-Sight**

**If the jammer LOS to the receiver is blocked,  
you are not protected.**

CREW protection is only effective for vehicles and personnel that are in direct LOS of the jammer. See Figure 6 and the comments that follow it.

CREW protection is reduced by objects that mask (block) the jammers LOS.



**Figure 6 – Stand-Off Vehicle Jammer in Urban Area**

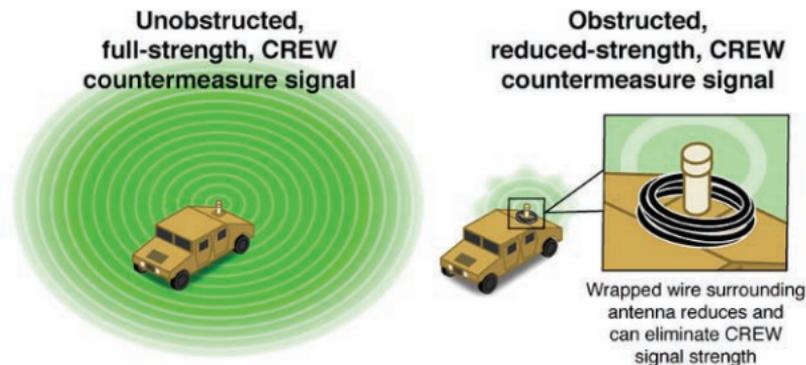
- Only center vehicle has a jammer
- Buildings mask protection
- Lead vehicle is unprotected
- Convoy needs to tighten up

## 1.4 Masking

**What is Masking and how does Masking affect the performance of CREW?**

- Another term for Masking is RF Path Blockage.
- RF waves radiating from antennas cannot penetrate solid objects.
- Blocking the direct line of sight between CREW antennas and RCIED receivers reduces CREW effectiveness. Keep areas around antennas clear of materials.

- Figure 7 is an example of how the coverage of CREW antennas can be reduced by field mistakes.



**Figure 7 – Antenna Coverage Comparison**



**DO NOT obstruct antennas  
in any way!**

## 1.5 Frequency (FREQs)

**What is Frequency and what is frequency de-confliction?**

- Frequency describes how often radio waves go through the air, which is typically measured in Hertz (Hz).
- Typical measurements are in kHz (kilohertz or thousands of cycles per second) and MHz (megahertz or millions of cycles per second).

- Think of frequency as how often a signal is sent in one second.
- The CREW system frequency needs to match the frequency of the RCIED receiver to stop it from detonating.

## 1.6 Frequency De-confliction

- Just as CREW can deny the enemy the use of the spectrum, it can also interfere with Blue Force communications. CREW weapons system targeting takes this into account, and frequencies are deconflicted through the targeting and frequency management processes. If you are having problems with your comm systems:
  - ◆ Conduct PMCI checks on your communications and CREW systems
  - ◆ Test your comm. systems for proper operation and note any discrepancies
  - ◆ Test your CREW for proper operation and note any discrepancies
  - ◆ Contact your unit EWO and S/G-6 to report the specifics of any interference and unit discrepancies

See Chapter 3 for further information.

## 1.7 Power

Jammer power must be greater than the power of the enemy's transmitter. Figure 8 shows the effect a jammer has on a typical transmitter.



**Figure 8 - Transmission Power**

Frequency and power are different measures of radio signals. Some signals are high frequency / low power, some are low frequency / high power. The correct combination of frequency and power is critical for effective communication in specific situations.

## 1.8 Jamming Basics

All CREW jammers jam the RCIED receiver, but there are two basic types of jammers:

### Noise Jammer

Prevents the receiver from hearing the enemy's transmitter signal

### Technique Jammer

Confuses the receiver so it does not understand the enemy's transmitter signal

## 1.9 Hard Truth

CREW is designed as a countermeasure to Radio Controlled IEDs only. Therefore, you must:

- Be aware of counter IED measures for other types of IEDs.
- Exercise standard 5/25 surveillance.
- Be aware of your surroundings at all times.
- Recognize when things don't "feel" or "look" right.

CREW works best when used by knowledgeable operators and leaders who understand:

- Line-of-Sight
- Distance / Power equation
- Frequency matching

CREW is **one** of the weapons you use. Like all other weapons, it works effectively against the enemy when used correctly.

The intelligent, dedicated men and women in our Services make the difference. Use your head and use your CREW system appropriately.

**YOU MAKE THE DIFFERENCE**

**What you learned in this chapter****Six Key Factors of Electronic Warfare**

- Definition of a Transmitter
- Definition of a Receiver
- Definition of a Jammer
- Definition of Line-of-Sight (LOS)
- The impact of Masking on your CREW devices
- Definition of Frequencies

**Your Responsibilities**

- Turn your jammer on
- Employ the jammer as a weapon
- Must have LOS to suspected RCIED
- DO NOT obstruct the antenna
- Ensure frequency loads are current

**Jammer Responsibilities**

- Match IED frequency
- Provide enough power to jam the IED

## Chapter 2

# Improvised Explosive Device (IED) Threat and Tactics

### What you will learn in this chapter

- What is an RCIED?
- How can you recognize different types of IEDs and RCIEDs?
- How are IEDs constructed?
- What are the enemy's tactics?



### IEDs / RCIEDs and the Enemy

**An extremely important point to remember is that IEDs and RCIEDs are *not the enemy*, the people using them are!**

### ***You can defeat those that employ them by:***

1. Being observant.
2. Watching for IED/RCIED indicators.
3. Capturing or killing those responsible for their use, whether it is the person that places them, the triggerman, the maker, or the supplier.

## 2.1 Definition and components of an IED

**An IED is a device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and is designed to destroy, incapacitate, harass, or distract.**

### The Charge

All IEDs contain a chemically and energetically unstable explosive material. This is the charge.

### The Detonator

The device used to trigger bombs, shape charges and other forms of improvised explosive devices is called the *detonator*.

There are many types of detonators. CREW is effective against Radio Controlled IEDs.

### Types of IED detonators

- Radio controller (RCIED)
- Command wire (CWIED)
- Vehicle borne (VBIED)
- Passive Infrared (PIR)
- Pressure / mechanical switches
- Victim Operated (VOIED)



**Figure 9 - Command Wire Detonator**

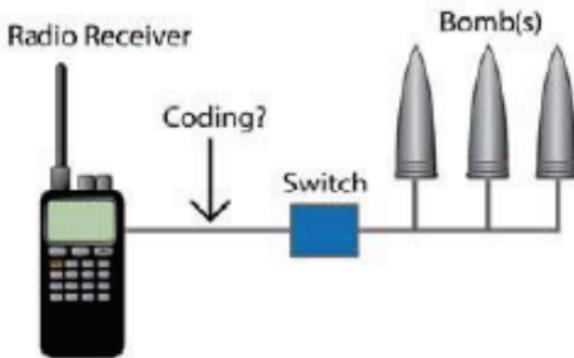


**Figure 10 - Vehicle Borne Detonator**

## 2.1.1 Radio Controlled Detonators

Commercially available, wireless Radio Frequency (RF) devices are adapted to trigger IEDs.

CREW targets the RCIED threat!!



**Figure 11 - Radio controlled detonation**

### Examples of Radio Controlled detonators

- Wireless doorbells
- RC car alarms and key fobs
- Long range, high powered cordless telephones (LRCTs)
- Push-to-talk walkie-talkies
- Handheld radios and transceivers
- Radio controlled toys like small cars & planes
- Remote garage door openers
- Two-way pagers
- Cellular telephones

### Low Power RCIED transmitters

- Inexpensive
- Unsophisticated
- Short range

- Short data stream signals with high / low signaling
- Varying frequency within frequency bands, due to design
- Triggerman usually in close proximity
- Low power charges
- Seldom used today

### High Power RCIED transmitters

- Much longer range than low powered devices
- Triggerman usually not in immediate area
- More difficult to jam
- More sophisticated and more difficult to counter
- Specific channels – narrow frequency bands
- High power charges
- RCIED trigger method of choice



**Figure 12 - High & Low Power Devices**

**CREW** is effective in deterring Radio Controlled Improvised Explosive Devices (RCIEDs)

## 2.1.2 Camouflage / Placement of Charges

There are several types of IED / RCIEDs, but no matter the style, most are considered masked devices. These devices are often disguised as debris. See Figure 13 for some examples.



**Pipe IED**



**Bagged IED**



**Livestock – Dead or Alive**

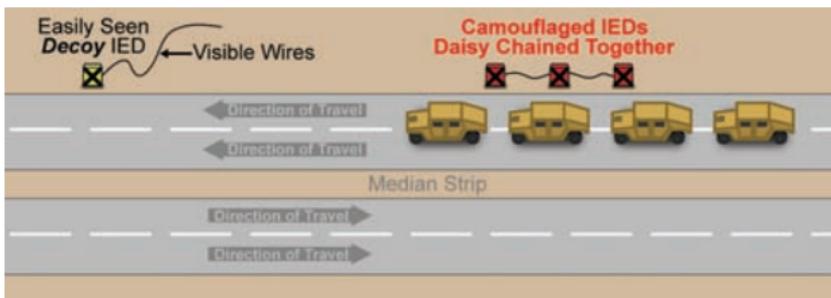
**Figure 13 - Masked Devices**

## 2.2 Enemy tactics

**What are some of the tactics used by the Enemy?**

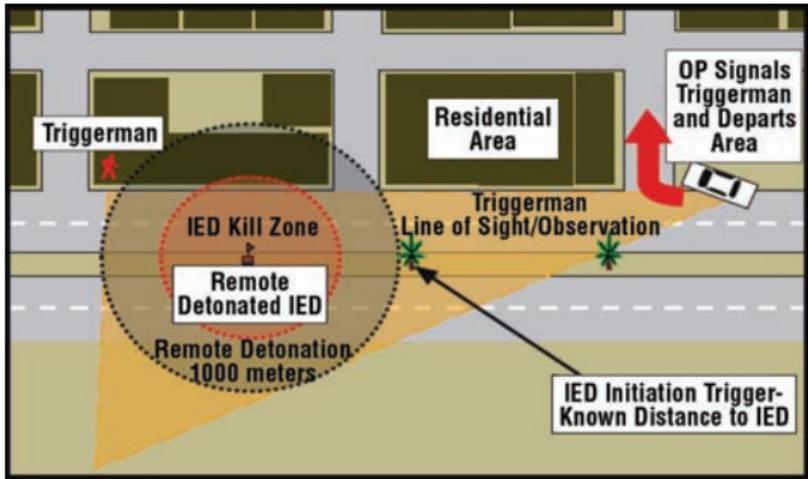
### How does the Enemy work?

- The "triggerman" is usually within Line of Sight (LOS) to the RCIED and outside of the explosive zone.
- The RCIED and the triggerman may not be obvious to the Warfighter because the enemy has hidden the IED, creating a false front to the Warfighter. A drainage ditch or guardrail would be a good location for this kind of deception, as shown in Figure 14.



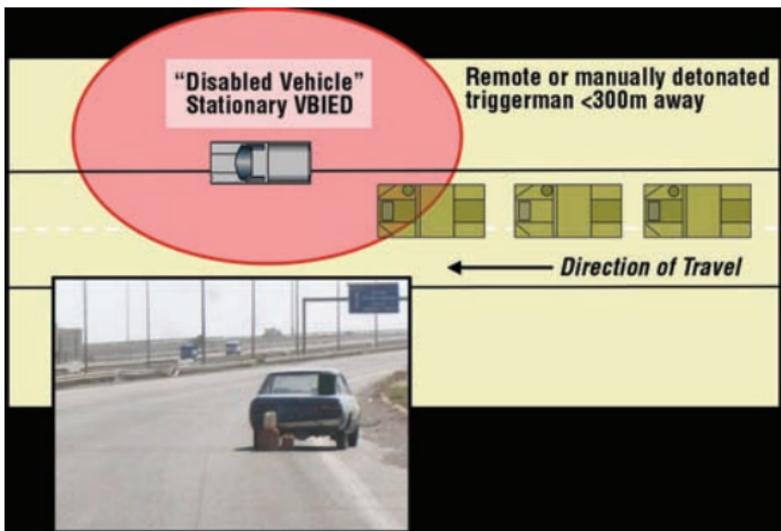
**Figure 14 - Baited Attack**

- Multiple charges can be linked together, or "daisy chained", for maximum effectiveness.



**Figure 15 – Attack using OP**

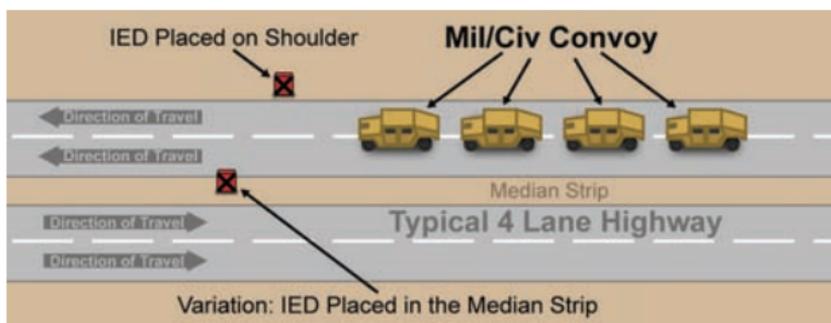
- The enemy often uses an Observation Post (OP) to coordinate timing of an explosion to cause the most destruction. OP may not be in LOS of the receiver. The OP will signal the triggerman to detonate the RCIED, as shown in Figure 15.



**Figure 16 - Broken Down Vehicle Attack**

## Likely Placement of RCIEDs

- Roads that have a high volume of coalition traffic.
- Shoulder of a roadway, usually within 10 feet of traffic lane
- In the median or inside guardrails.
- Choke points, boundary turn-around points and pre-placed locations.
- Under debris, inside broken down or damaged vehicles.



**Figure 17 – Typical Attack**

The Enemy and the RCIED receiver are usually not seen by the Warfighter.



**These are just some examples  
– look for other situations and  
report them immediately!**

### **What you learned in this chapter**

- Definition & components of IEDs and RCIEDs
- How to recognize different types of IEDs and RCIEDs
- How IEDs are constructed
- Common enemy tactics

### **Your Responsibilities**



- Stay alert
- Avoid complacency
- Watch for indicators of IEDs
- Understand LOS to suspected IED
- Capture or kill those responsible for using IED / RCIEDs when possible.

# Chapter 3

## Electronic Warfare Officer (EWO) and Staff Planning

### What you will learn in this chapter

- What process does the EWO follow?
- What are the basic responsibilities of an EWO?
- What are the pre-mission responsibilities?
- What are the post-mission responsibilities?

### 3.1 EWO Process Flow

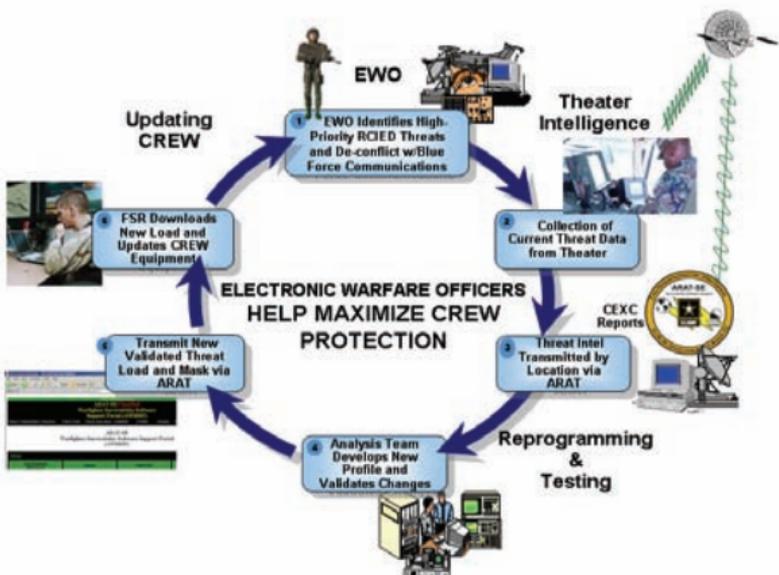


Figure 18 - EW Process Flow

## **Explanation of the EW Process Flow**

1. EWOs identify high priority RCIED threats and de-conflict with Blue Force comms frequencies.
2. RCIED intelligence collected by EOD units and/or through EWO
3. Data is SIPRed via Army Reprogramming Analysis Team (ARAT) website
4. Analysis team develops new Threat Load
5. Upon validation via "Chamber Test" new threat Load is posted back to ARAT website
6. FSR downloads file from website, and updates CREW equipment

## **3.2 Basic EWO Responsibilities**

Always alert the Commander that CREW is being employed.



- Coordinate spectrum management with G6/S6 to include de-conflicting EA
- Facilitate persistent and realistic EW training
- Obtain the most recent Intel, including an Intelligence Preparation of the Battlefield (IPB), for your Area of Operation (AO)
- Ensure operators are knowledgeable and competent with CREW system
- Monitor IED trends and emerging enemy TTPs
- Implement a maintenance plan for unit CREW Systems
- Conduct EW mission planning, to include the use of the Convoy Planning Tool
- Load, verify and update the loadsets based off fragos and the ARAT Web site.
- Utilize CREW Interoperability chart
- Ensure unit uses a spectrum analyzer for Pre-Combat checks on systems
- Ensure current Frequency load sets are valid
- Ensure CREW TTPs are valid and implemented
- Compel focused Counter RCIED operations
- Coordinate the integration of CREW assets within the AO
- Manage and oversee employment of assigned CREW assets and personnel
- Ensure lost, stolen, or destroyed CREW Systems procedures are in place

- Be the representative for all other CREW related issues
- Act as a liaison for C-IED efforts
  - Spectrum Managers
  - Airborne Assets
  - Electronics Officer (EO)
  - Communications Officers and frequency managers
  - Combat Engineers
  - EOD
  - Combined Explosives Exploitation Cell (CEXC)
  - Weapons Intelligence Team (WIT)
  - Joint IED Defeat Organization (JIEDDO)

### 3.3 Pre-mission EWO Responsibilities



- Make sure PMCS has been accomplished on CREW systems prior to leaving the FOB.
- Report CREW problems to FSR
- Know what equipment is operational/non-operational and status of all CREW systems.
- Contact S2/G2 (Intel) – know what current threat is in the area.
- Contact S3/S2 and receive updated enemy and friendly TTPs
- Ensure that your CREW system has the correct loadset and that it is optimized against the prevalent threats.

- Contact S6/G6 – Ask about possible interferences that may be encountered with friendly forces based on the CREW Loadset List.
- Contact S3/G3 (OPS) to find out what operations are happening along route to avoid operational conflicts.
- If needed, return to S2/S6 to coordinate operations.
- Utilize the Convoy Planning Tool to maximize EW protection utilizing CREW systems.
- Ensure pre-combat checks have been accomplished.
- Brief Convoy Commander with Intel information – what types of IEDs are in the area, possible interoperability problems that may be encountered, etc.

### 3.4 Post-mission Responsibilities



- Debrief with Convoy Commander.
- Report any new information that is gathered during convoy.
- Report any activity that is “not normal” in area.
- Download collected data from CREW systems.
- Coordinate with FSRs / operators for equipment PMCS and repair.
- Debrief S2/G2 and S3/G3

#### **What you learned in this chapter**

- The EWO Process Flow
- The basic responsibilities of an EWO
- Pre-mission responsibilities
- Post-mission responsibilities



## Chapter 4

# CREW Systems

### What you will learn in this chapter

- What are the different types of jammers?
- What are the basic PMCS procedures performed?
- How do different types of CREW devices operate?

The operator must receive interoperability distances before convoying with vehicles using CREW devices. Convoying with systems that are NOT compatible can cause system performance degradation. See your Field Service Representative (FSR) or S-2/S-6 for interoperability and current program load information.

### OPSEC

**In the event of possible compromise, shred, burn, or otherwise destroy all classified documentation associated with CREW equipment.**

Disable the hardware by any available means (axe, weapons fire, explosives, fire, etc.)



**Ensure system is OFF** while entering and in the FOB

**Ensure system is turned ON** when departing FOB

## 4.1 Jammer Types

- Different jammers are designed to defeat different RCIED threats.
- Jammers are programmed to defeat threats in specific Areas of Operation (AO) based on the best available intelligence.
- There are three types of jammers in use by the U.S. Military:
  - ◆ Active jammer
    - Always jams
    - Commonly used to defeat low-power threats
    - Doesn't have to hear a threat signal
    - Can interfere with everything that operates on the jamming frequencies.
  - ◆ Reactive jammer
    - Listens for RF signals and then jams (Scan & Jam) - listens for, and reacts to, everything we tell it is a threat
    - Commonly used to defeat high-power threats
    - Must hear threat signal to jam
  - ◆ Combination (both Reactive & Active) jammers

### Active Jammers

#### **Pros**

- Constantly transmits on all programmed frequencies or bandwidths
- Can defeat multiple threats simultaneously
- Very efficient at defeating low power threats
- Easy to operate: turn it on and ignore

#### **Cons**

- Spreads available power across entire bandwidth

- Susceptible to exploitation of programmed frequencies
- Relatively low power per MHz
- Not effective vs. high-power threats
- Constantly jamming comms, including Blue Force

### **Reactive Jammers**

#### ***Pros***

- Focused “response” puts available power directly on threat frequency
- Capable of modifying threat signal
- Low exploitation risk; intermittent transmission
- Most efficient way to defeat high-power threats

#### ***Cons***

- Requires acute receiver sensitivity
- Hears all RF signals in programmed “threat” band

### **Combination Jammers**

- Both Active and Reactive capabilities to defeat a wide range of threats

## **4.2 Preventative Maintenance Checks and Services (PMCS)**

The chart on the following pages lists the PMCS steps required for all CREW devices. Note the device-specific items identified in the first column.

The following table describes the columns used in the PMCS charts presented on the next pages:

B	This procedure is to be performed BEFORE each convoy leaves the FOB.
A	This procedure is to be performed AFTER each convoy returns to the FOB.
W	This procedure is to be performed on a WEEKLY basis.
M	This procedure is to be performed on a MONTHLY basis.

Your antenna and mount may differ but the general PMCS are generic and similar to many other systems.

Use a low power and/or high power test set to ensure a Fully Mission Capable (FMC) system.

Preventative Maintenance Checks & Services						
Item #	B	A	W	M	Procedure	Acceptance Criteria
1	X	X	X	X	Visually inspect power cable, blanking cable (if installed), power and blanking connectors (on Red/Green Systems), RF connectors	<ul style="list-style-type: none"> <li>a. Cable connectors connected and not loose</li> <li>b. No cuts in cables penetrating through insulation</li> <li>c. Cables are not pinched or crushed</li> <li>d. Power cables connected to connectors</li> <li>e. Antenna cables connected to connectors</li> <li>f. (Red/Green Systems) Blanking cable connected to J3 (Mid Band and Low Band) connectors (as appropriate)</li> </ul>

Preventative Maintenance Checks & Services						
Item #	B	A	W	M	Procedure	Acceptance Criteria
2	X	X	X	X	<ul style="list-style-type: none"> <li>a. Visually inspect antenna(s) for damage or missing components</li> <li>b. Verify antenna(s) are in place and fastened hand tight onto antenna base (MCE).</li> <li>c. Verify antenna mount(s) are securely attached to vehicle and fasteners greater than hand tight</li> </ul>	<ul style="list-style-type: none"> <li>a. Antenna(s) present and securely fastened to base</li> <li>b. Antenna mount(s) securely attached to vehicle</li> </ul>
3	X	X	X	X	<ul style="list-style-type: none"> <li>a. Remove dirt, dust and debris from chassis, system connectors and switches</li> <li>b. Ensure cooling fins (if any) are not obstructed</li> <li>c. Ensure cooling fan screen is not obstructed (SSVJ)</li> </ul>	<ul style="list-style-type: none"> <li>a. System and components clean</li> <li>b. Cooling fins unobstructed</li> <li>c. Cooling fan flow-path unobstructed (SSVJ)</li> </ul>

Preventative Maintenance Checks & Services						
Item #	B	A	W	M	Procedure	Acceptance Criteria
4				X	<ul style="list-style-type: none"> <li>a. Disconnect antenna cable connectors at system and antenna base</li> <li>b. Clean cable end connectors using clean dry cloth or cleaning pad</li> <li>c. Clean antenna base and system connectors using clean dry cloth or cleaning pad</li> <li>d. Reconnect antenna cable connectors at system and antenna base</li> </ul>	<ul style="list-style-type: none"> <li>a. Antenna connectors fastened greater than hand tight (as appropriate)</li> <li>b. Antenna connector fittings clean and dry</li> </ul>

Preventative Maintenance Checks & Services					Acceptance Criteria	
Item #	B	A	W	M	Procedure	
MIMBJ Only				Annually	<ul style="list-style-type: none"> <li>a. Remove GPS battery compartment cover</li> <li>b. Replace GPS battery with DL 123 or equivalent 3V Lithium battery</li> <li>c. Replace GPS battery compartment cover</li> <li>d. Start up per operators manual and verify GPS functions normally</li> </ul>	GPS sync display shows "SYNC OK" within 20 minutes
mICE Only	X	X	X	X	Visually inspect switches	Switch covers and switches in place
mICE Only	X	X	X	X	Visually inspect Hour Meter	Hour Meter in place and reads less than 600 hours. If greater than 600 hours, depot level preventive maintenance may be required
mICE	X				The following switch operations should be performed using the Remote Control Unit	<ul style="list-style-type: none"> <li>a. Chassis SW1 and SW2 block plate</li> </ul>

**FOR OFFICIAL USE ONLY**

Preventative Maintenance Checks & Services						
Item #	B	A	W	M	Procedure	Acceptance Criteria
Only					<p>(RCU). If an RCU is not installed, operate switches located on chassis front panel.</p> <ol style="list-style-type: none"> <li>If remote unit is present, verify that switch block plate is installed on main chassis front panel.</li> <li>Verify SW1 is in OFF and POWER light is extinguished.</li> <li>Verify SW2 is in STANDBY</li> <li>Move SW2 from STANDBY to RADIATE and back to STANDBY. Ensure switch moves up and down freely.</li> <li>Move SW1 from OFF to ON. Verify the POWER light is illuminated.</li> <li>Pull main circuit breaker (CB) to the OUT position. Verify that the FAULT</li> </ol>	<p>installed (if applicable)</p> <ol style="list-style-type: none"> <li>SW1 and SW2 move up and down freely</li> <li>Power light illuminates and extinguishes on command</li> <li>Fault light illuminates on command</li> <li>CB operates properly</li> </ol>

Preventative Maintenance Checks & Services						
Item #	B	A	W	M	Procedure	Acceptance Criteria
					light is extinguished. g. Push the CB IN. Verify the FAULT light illuminates. h. If system operation is no longer required, move SW1 from ON to OFF	



Preventative Maintenance Checks & Services						
Item #	B	A	W	M	Procedure	Acceptance Criteria
m/CE Only			X	X	<ol style="list-style-type: none"> <li>Visually inspect antenna(s) for damage or missing components</li> <li>Remove antenna(s) from mount(s) and disassemble antenna(s) (if required)</li> <li>Clean antenna(s) and antenna mount(s) threaded fasteners using clean dry cloth, cotton/poly rope, or cleaning pad. (NOTE: do not use steel wool or sandpaper) Wipe clean with clean cloth.</li> <li>Reinstall antenna(s) and verify at least hand tight</li> <li>Verify antenna mount(s) are securely attached to vehicle and fasteners are greater than hand tight</li> </ol>	<ol style="list-style-type: none"> <li>Antenna(s) present and securely fastened to base</li> <li>Antenna mount(s) securely attached to vehicle</li> <li>Antenna threaded fittings clean and dry</li> </ol>

Preventative Maintenance Checks & Services						
Item #	B	A	W	M	Procedure	Acceptance Criteria
mICE Only				X	<ul style="list-style-type: none"> <li>a. Disconnect antenna cable connectors at chassis and antenna base</li> <li>b. Clean cable end connectors using clean dry cloth or cleaning pad</li> <li>c. Clean antenna base and chassis connectors using clean dry cloth or cleaning pad</li> <li>d. Reconnect antenna cable connectors at chassis and antenna base</li> </ul>	<ul style="list-style-type: none"> <li>a. Antenna connectors fastened greater than hand tight (as appropriate)</li> <li>b. Antenna connector fittings clean and dry</li> </ul>



Preventative Maintenance Checks & Services						
Item #	B	A	W	M	Procedure	Acceptance Criteria
mICE Only			X	X	<p>The following switch operations should be performed using the Remote Control Unit (RCU). If an RCU is not installed, operate switches located on chassis front panel.</p> <ol style="list-style-type: none"> <li>Verify SW2 is in STANDBY</li> <li>Move SW1 from OFF to ON. Verify the POWER and FAULT lights illuminate.</li> <li>Pull main circuit breaker (CB) to the OUT position. Verify that the POWER and FAULT lights extinguish.</li> <li>Push the CB IN. Verify that the POWER and FAULT lights illuminate.</li> <li>Move SW1 from ON to OFF</li> </ol>	Circuit Breaker operates properly



## 4.3 Acorn System



Figure 19 - Acorn Device

### 4.3.1 General Description

- Active
- Threat-specific

### 4.3.2 Antennas

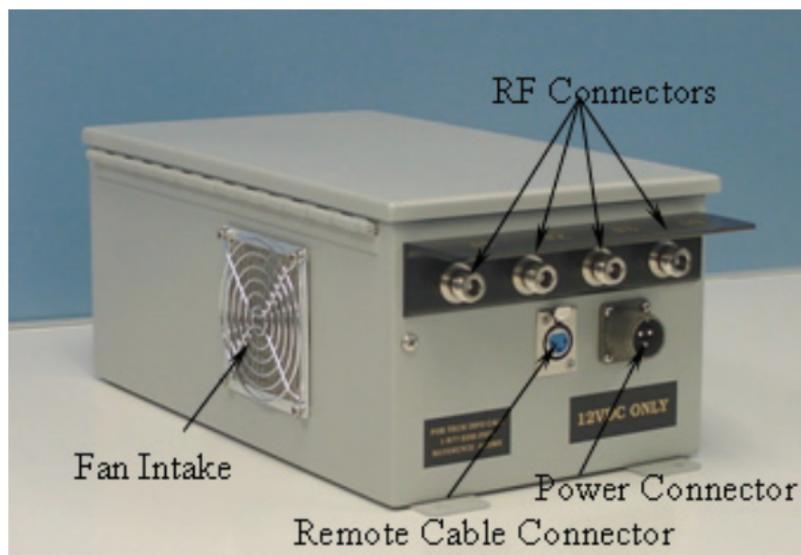
- Whip (3)



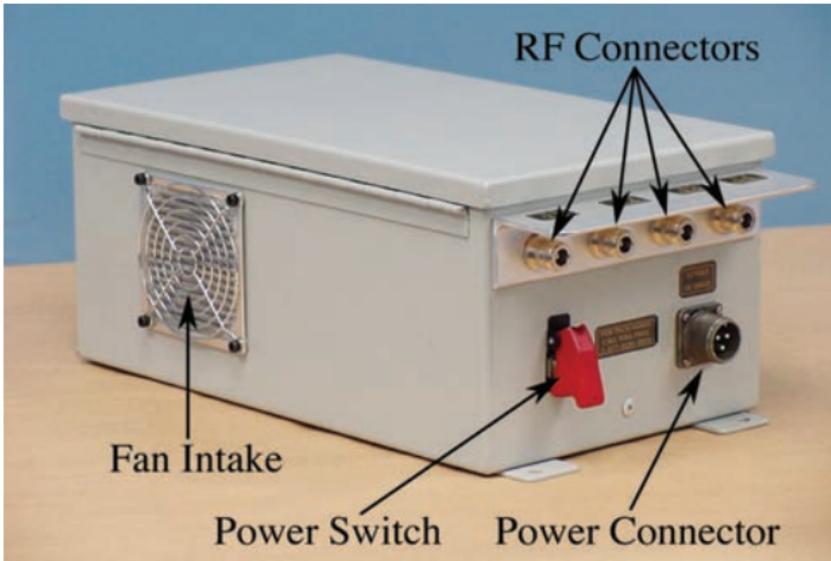
**ALWAYS CHECK** power cables, antenna cables, nuts, bolts and lock-washers, cable tie-downs, and security fasteners. Inspect the antenna locations for missing or broken parts.

### 4.3.3 Operator Controls & Indicators

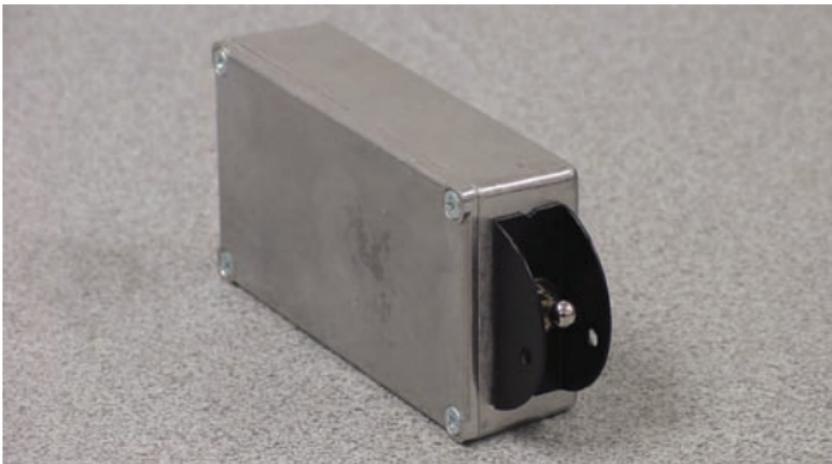
The Acorn system comes in two configurations. One configuration uses a remote switch as shown in Figure 20. The other one has all controls on the electronics box, shown in Figure 21.



**Figure 20 – Acorn with Remote Switch**



**Figure 21 - Acorn without Remote Switch**



**Figure 22 - Remote Switch**

#### **4.3.4 Device Operation**

##### **Turn ON Procedure**

Locate the power switch and turn it **ON**.

### **Turn OFF Procedure**

To remove power from the system, turn the power switch **OFF**.

Although testing against specific tools and systems has not been conducted, Acorn will pose interference only on specific frequencies.

### **4.3.5 Zeroize / Emergency Erase**

This system does not have a Zeroize capability.

## 4.4 Beech System



Figure 23 - Beech Device

### 4.4.1 General Description

- Active
- Threat-specific

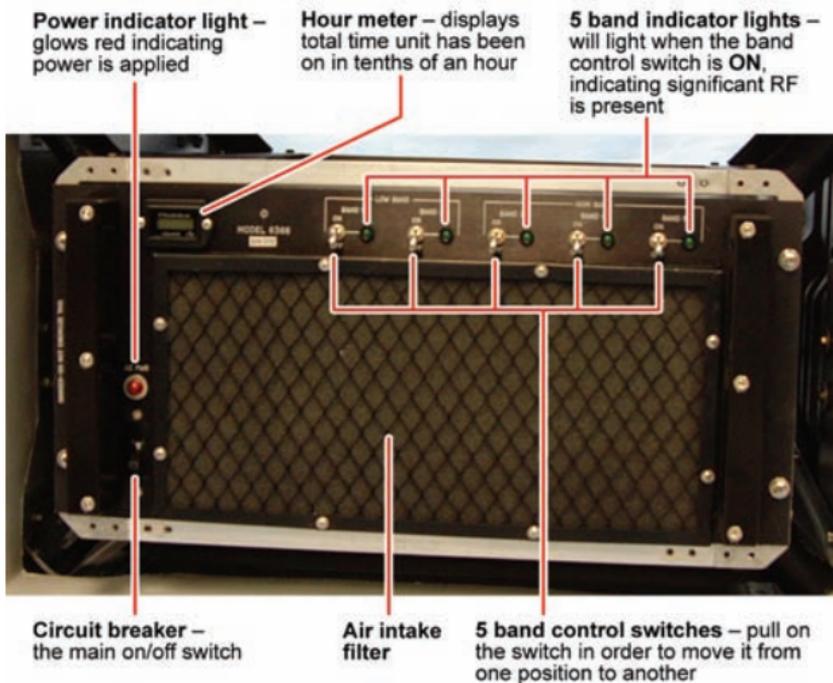
### 4.4.2 Antennas

- Dipole (2)



**ALWAYS CHECK** power cables, antenna cables, nuts, bolts and lock-washers, cable tie-downs, and security fasteners. Inspect the antenna locations for missing or broken parts.

### 4.4.3 Controls & Indicators



**Figure 24 – Beech Controls & Indicators**

There is a large air intake filter on the Front Panel in addition to the following controls and indicators:

CIRCUIT BREAKER	Main on/off switch
BAND CONTROL SWITCHES	Pull on the switch in order to move it from one position to another.
BAND INDICATORS	Illuminates when the switch is <b>ON</b> , indicating significant RF is present.
POWER INDICATOR	Glows red to indicate power is applied
HOUR METER	Displays the total time the unit has been operating to the tenth of an hour.

#### **4.4.4 Device Operation**

##### **Turn ON Procedure**

1. Turn **ON** circuit breaker
2. Make sure fans are operational
3. Switch **ON** Select Band Control Switch

##### **Turn OFF Procedure**

1. Turn **OFF** band control switches
2. Turn **OFF** circuit breaker

#### **4.4.5 Zeroize / Emergency Erase**

This system does not have a Zeroize capability.

## 4.5 Blue System



**Figure 25 - Blue Device**

### 4.5.1 General Description

- Small, portable jammer
- Active jammer

## 4.5.2 Antennas

- Personal Antenna
- Vehicle Antenna



**Module must have antenna properly attached and LED continuously ON for proper operation.**

## 4.5.3 Operator Controls & Indicators



**Figure 26 – Blue Controls & Indicators**

POWER	Turns module on and off
ANTENNA	Attach antenna to BNC connector
LED INDICATOR	OFF: Module is turned off FLASHING: Module is on and not programmed ON: Module is operational
ZEROIZE	If depressed, program will be erased and module will be inoperable until reprogrammed or cloned. Flashing LED indicator will confirm program is erased.

## 4.5.4 Device Operation



**The system should be worn at shoulder height with the antenna at least 1 inch away from the face.**

### Turn ON Procedure

1. Turn on the Power switch.
2. The LED should illuminate.

### Turn OFF Procedure

1. Turn off the Power switch.
2. The LED should go off.

### Cloning Procedure

Cloning is the process used to copy a device configuration from one device to other devices.

1. Remove the ODU dust cover from the side of the unit. Pull firmly to remove.
2. Using a cloning cable, attach one end of the ODU connector to the module, as shown. The red dots must be aligned for proper connection to the Zeroized device as shown in Figure 27.



**Figure 27 - Proper cable alignment**

3. Plug the other end of the ODU cloning cable to the properly loaded Blue device.
4. Turn on the properly loaded Blue device.
5. Turn on the Blue device that needs to be programmed. Wait for LED light to stop flashing.
6. Disconnect the cable by grasping the collar of the ODU connector and pulling it away from the Blue device.



**Figure 28 – Cloning**

#### **4.5.5 Zeroize / Emergency Erase**

1. Turn the module on. If it is programmed the LED should remain on.
2. Using the tool attached on the lanyard, press down on the ZEROIZE switch. Figure 29 shows this step.
3. The LED Indicator should be flashing, which confirms that the previous program has been deleted and a new one can be reloaded.



The module is not operational until a new program is loaded.



**Figure 29 - Zeroizing**

#### **4.5.6 Vehicle Mounted Blue System**

Use the same procedure as the portable operation described in the previous sections, except:

1. Let the vehicle warm up for at least 3 minutes before turning unit on.
2. Ensure the Power Cable is properly attached to the vehicle power cable.
3. Red dots must be aligned for proper connection.

**For Blue System vehicle mount installation procedures, see your Joint CREW Field Service Representative (FSR).**

## 4.6 Chameleon Electronic Countermeasure (ECM) System

### 4.6.1 General Description

- Active jammer

### 4.6.2 Antennas

- Shakespeare whip
- Radome



**ALWAYS CHECK** power cables, antenna cables, nuts, bolts and lock-washers, cable tie-downs, and security fasteners. Inspect the antenna locations for missing or broken parts.

### 4.6.3 Operator Controls & Indicators



Figure 30 - Mobile Countermeasures (MCM) Unit



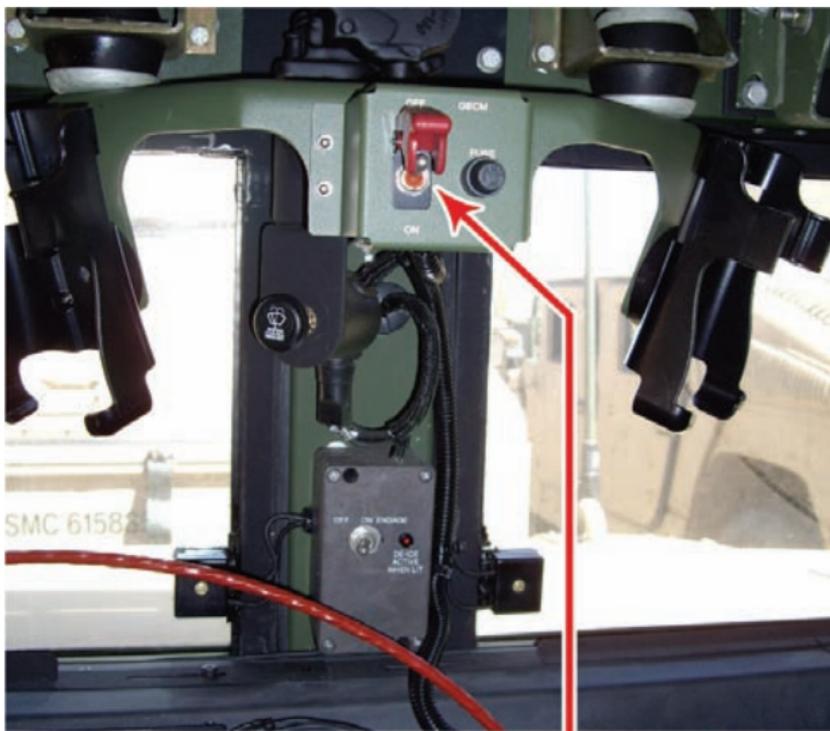
**Figure 31 - Remote Control Unit (RCU)**

#### **4.6.4 Device Operation**

##### **Turn On Procedure**

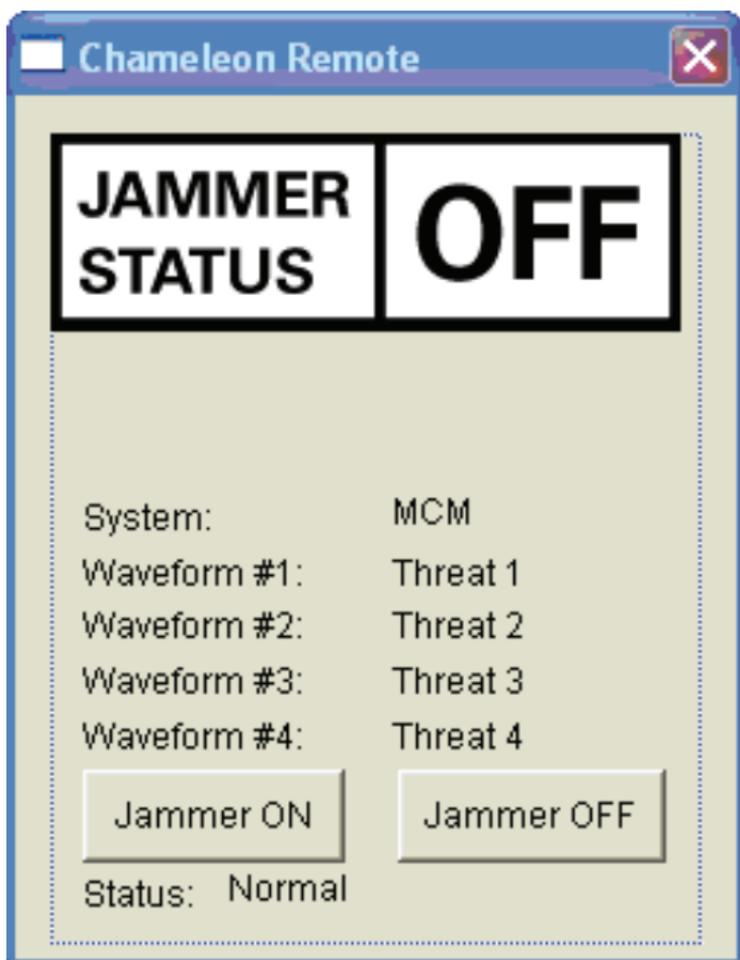
1. Ensure pre-mission checks are complete.
2. Start the vehicle engine.
3. Switch on the RCU.
4. Start the Chameleon Remote application.
5. Select **Start**.

6. Select **Chameleon Remote**.
7. Switch on the Master MCM switch in the front of the vehicle.



**Figure 32 - Master MCM Switch**

8. Wait for 20 seconds. You will see the Chameleon Remote screen displayed on the RCU screen.

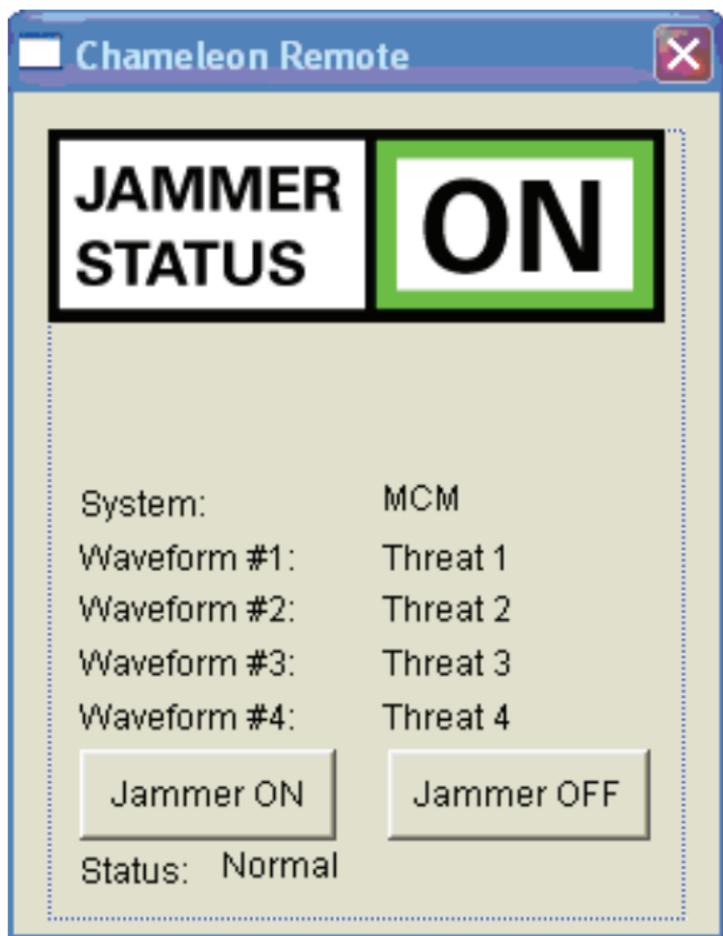


**Figure 33 - Remote Screen**

**If the RCU still shows that the jammer is not connected, check that the MCM Power switch is ON.**

9. Select Jammer ON
10. Select **Yes** when asked if you want to start the ECM.
11. Wait 20 seconds for the Built-in Test (BIT) to complete on the MCM.

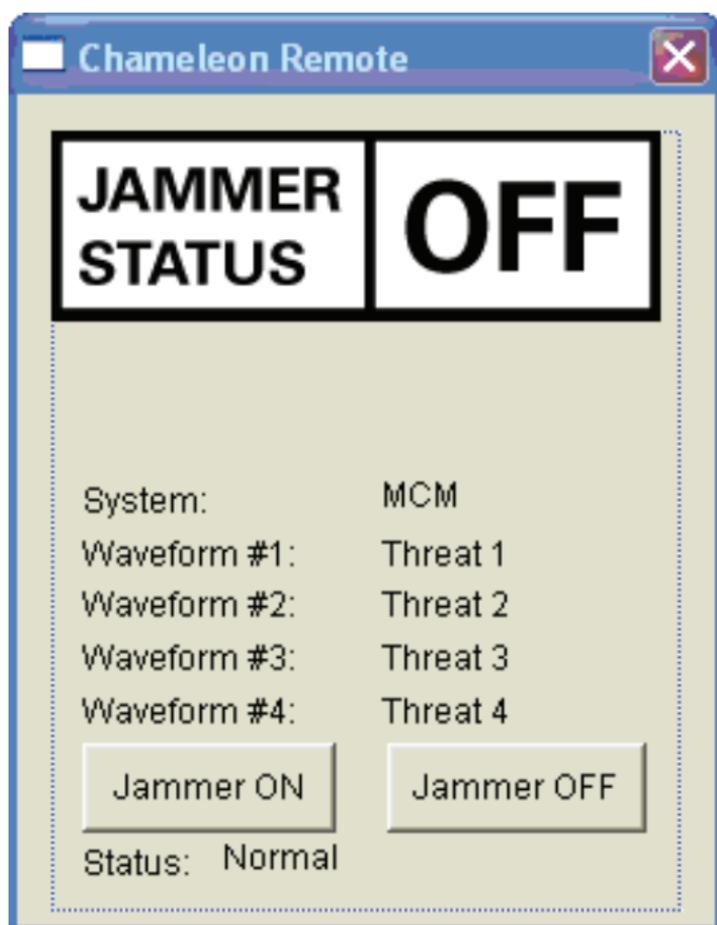
- Once the BIT is complete and the ECM is working you will see Jammer Status **ON** displayed.



**Figure 34 - Jammer is ON**

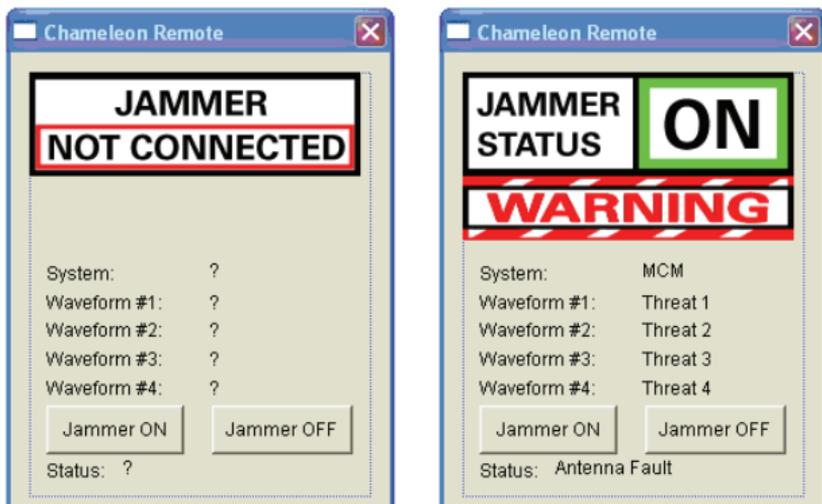
### **Turn OFF Procedure**

- Select Jammer OFF.
- When prompted, press **YES** to confirm ECM off.
- Jammer status should now read **OFF**.



**Figure 35 - Jammer status is OFF**

## Fault Indications



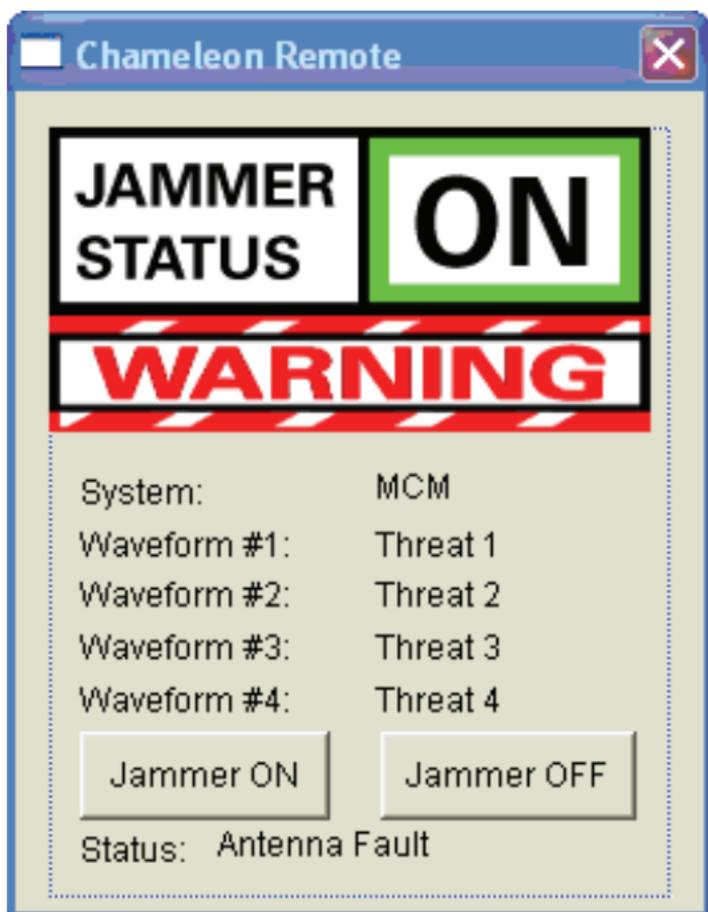
**Figure 36 - ECM Fault Screens**

The screens shown in Figure 36 indicate a fault. Check the following:

1. Ensure the Master On/Off Switch is **ON**.
2. Stop jamming and re-try.
3. Stop jamming and check cabling.
4. Contact the FSR.

### ECM Fault

If the following is observed, perform Lost ECM Procedure in accordance with Unit/Mission TTP.



**Figure 37 - Lost ECM Fault Screen**

### **RCU Lockout**

If the RCU locks out, re-boot by holding the On/Off switch for five seconds.

You will have to restart the CHAMELEON Remote Program

## **Emergency RCU Failure Procedure**

If the RCU becomes damaged or fails to work:

1. Disconnect the RCU by removing the computer lead. If the ECM is ON it will remain on regardless.
2. Use the Master ON/OFF switch to control ECM.
3. You are now able to manually control the MCM using the master on/off switch until RCU fault is cleared.

## **MCM Fault Indications**



**Figure 38 - System jamming OK**

The system is working when:

- Green light is lit
- No audio alarm
- No error messages are displayed on the RCU or MCM

## **Fault Conditions**

- If the light is Amber or Red, the RCU and MCM Audio Alarm will sound to indicate an installation fault.
- If a fault can not be rectified, contact FSR.



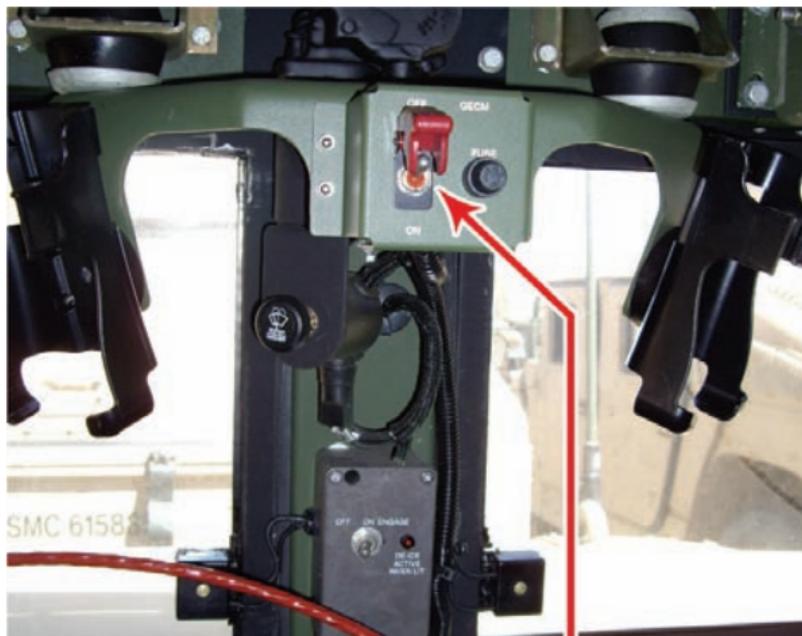
**Figure 39 - Fault but still jamming**



**Figure 40 - Fault and not jamming**

If there is no power to the MCM, check:

1. Vehicle ignition
2. Master ON/OFF
3. Rear panel Trip Switch
4. Rear panel Power Cabling
5. MCM switched ON at the unit



**Figure 41 - Master ON/OFF**



**Figure 42 - Rear Panel**

## 4.6.5 Zeroize / Emergency Erase

Local TTPs in theater will dictate when Emergency Erase should be performed.



**Once the data load is erased, it needs to be reinstalled by the FSR.**

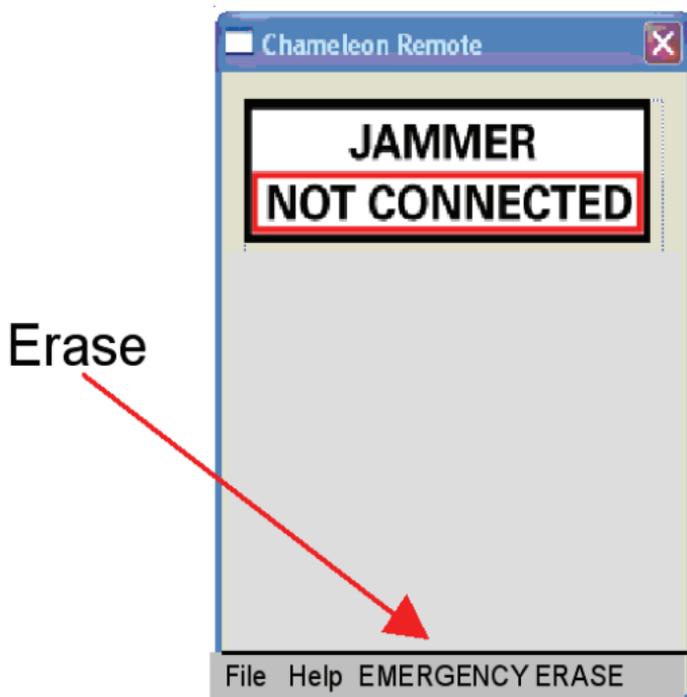
There are two ways to erase the Data Load:

### Erase using RCU

1. At the bottom of the screen, select **EMERGENCY ERASE**.
2. Select **YES** on the pop-up screen.
3. Select **YES** on the Warning screen to erase.
4. Hold the RESET button in for ten seconds to clear the memory.



**The system and laptop remain classified and must be properly handled after Zeroizing.**



**Figure 43 - Erase using RCU**

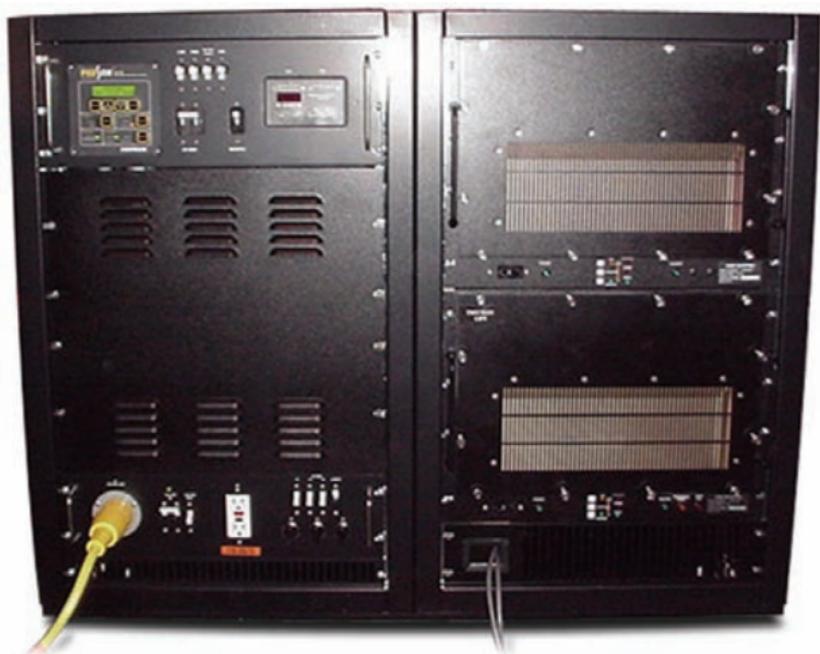
**Erase manually**

On the front of the MCM, press the yellow ERASE button.



**Figure 44 - MCM Erase Button**

## 4.7 Cottonwood System



**Figure 45 - Cottonwood Device**

### 4.7.1 General Description

- Combination (Active & Reactive) jammer

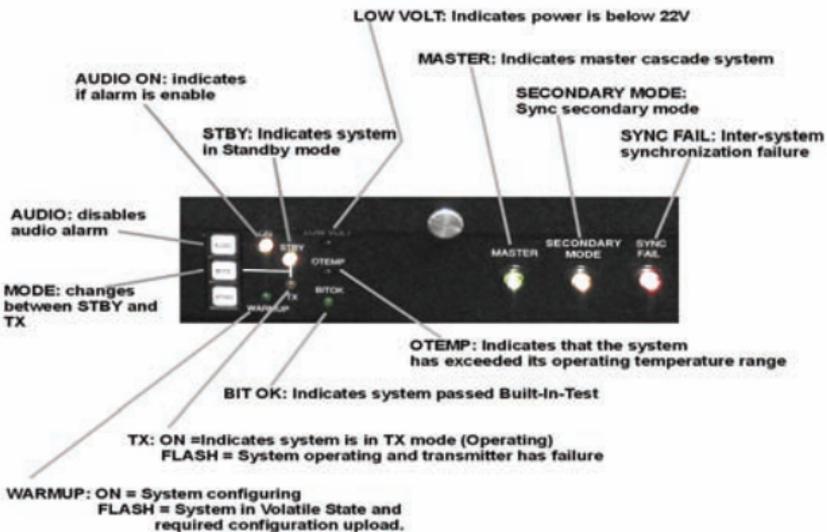
### 4.7.2 Antennas

- Broadband omni-directional
- Cottonwood system is integrated in a vehicle



**ALWAYS CHECK** power cables, antenna cables, nuts, bolts and lock-washers, cable tie-downs, and security fasteners. Inspect the antenna locations for missing or broken parts.

### 4.7.3 Operator Controls & Indicators



**Figure 46 - User Front Panel**



Figure 47 - Remote Control

#### 4.7.4 Device Operation

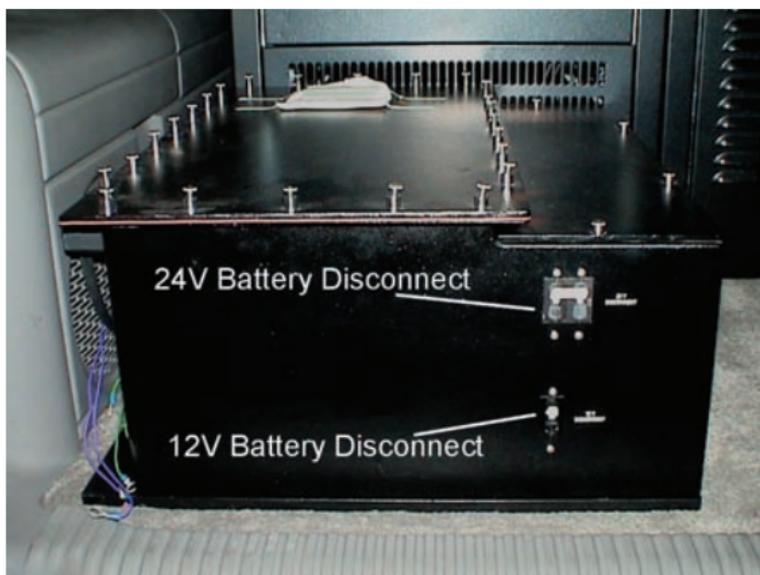
##### Turn ON Procedure



The system will not operate correctly with the chassis front panels removed.

1. Turn on the vehicle or attach a shore power cable.
2. Make sure that the LOW, HIGH and U-HIGH chassis front panels are attached.
3. Turn ON the circuit breakers (CB) on the equipment inside the vehicle, as listed on the following pages:

## Turn ON the Battery Box



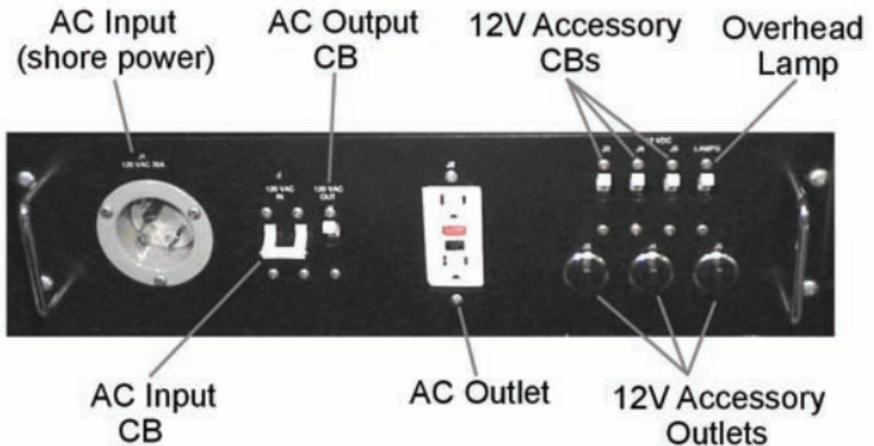
**Figure 48 - Battery Box**



**WARNING:** The 24V Disconnect circuit breaker on the battery box at the rear of the vehicle should remain ON at all times unless maintenance to the 24V power system is being performed. Damage to the electronic systems may result otherwise.

1. Turn the 24V Battery Disconnect switch to **ON**.
2. Turn the 12V Battery Disconnect switch to **ON**.

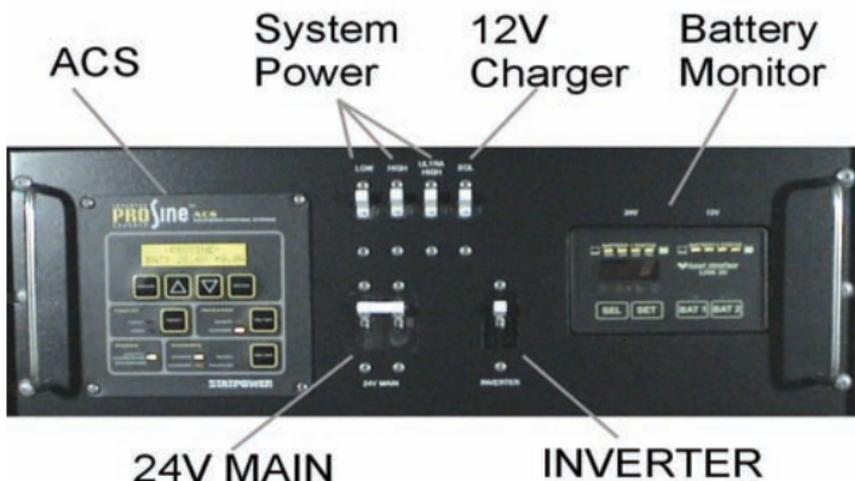
## Turn ON the Power Distribution Unit (PDU)



**Figure 49 - PDU Connections & Breakers**

1. Turn the 120 VAC OUT switch to **ON**
2. Turn the J3 CB to **ON**
3. Turn the J4 CB to **ON**
4. Turn the J5 CB to **ON**
5. Turn the LAMP switch to **ON**
6. Turn on the Power Monitor Unit (PMU), as described on the following page.

**Turn ON the Power Monitor Unit (PMU)**



**Figure 50 - Power Monitor Unit (PMU)**

1. Switch the 24V MAIN CB to **ON**
2. Turn the INVERTER switch to **ON**
3. Turn the LOW switch to **ON**
4. Turn the HIGH switch to **ON**
5. Turn the ULTRA-HIGH switch to **ON**
6. Turn the 12V POWER CB to **ON**
7. Turn the EQL switch to **ON**
8. Once the power system is energized, power up the system by switching each of the LOW and the HIGH system circuit breakers on as follows:
  - a. Switch the CC LOW CB to **ON**
  - b. Switch the CC HIGH CB to **ON**
  - c. Switch the CC ULTRA HIGH CB to **ON**

- The LEDs on the Front Panel and the Remote Control will flash on briefly. The system begins a boot-up sequence that typically ends with the system entering the Standby state and the Built-In-Test (BIT) passing.

This condition is noted by viewing the **STBY** and **BIT OK** LEDs illuminated. This process takes approximately 60 seconds.

- Allow for a minimum warm-up time for all equipment of five minutes.
- If the WARMUP LED flashes, this indicates the system requires configuration information to operate.
- If needed, transfer the file with the operator's settings (frequency, bandwidth etc.) from the laptop to the hardware.



If the ambient temperature within the vehicle is below 10 °C, the system requires a five minute warm up period. If the system has not had adequate time to warm up, it may fail its Built-In-Test (BIT). It is recommended that system be configured following this warm-up period under these environmental conditions.

- Connect the laptop computer.
- Start the laptop computer and the software.

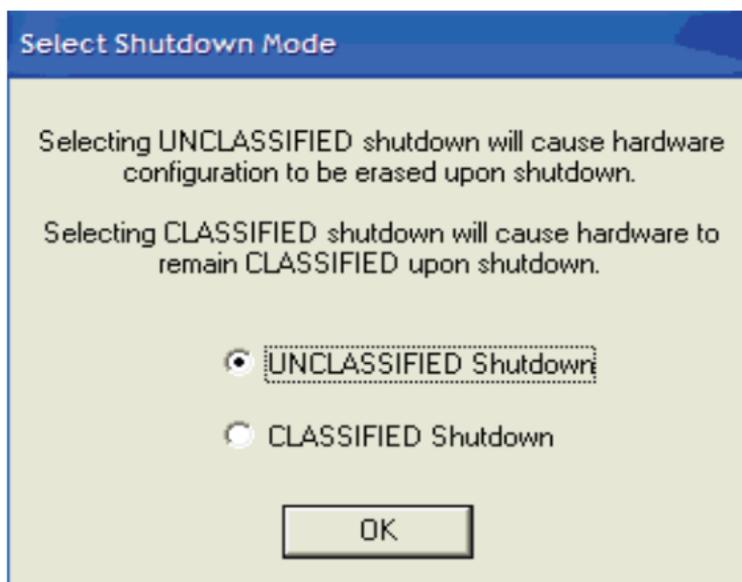
- c. If a file holding hardware settings has been created previously, open it on the laptop.
13. If the hardware settings file does not exist, create a new one using the menus.
14. Click the **Configure Hardware** button at the bottom of the configuration screen to transfer the file from the laptop to the hardware.
15. If the configure button is not pressed after setting up the file, none of the changes that you have made will be loaded into the hardware. If you close the configuration window without saving, your edits will be lost.
16. Click the **Save and Configure** button to save any changes to the file.
17. Once configuration is complete, the Operate Screen is brought up automatically and the system is ready for operation.

### **Turn OFF Procedure**

There are two different modes the system can be left in at shutdown, as follows:

### **UNCLASSIFIED Shutdown**

- The system hardware will have all configuration information erased from its memory.
- The system will immediately become incapacitated and be inoperable until it is again configured with a laptop computer.
- The system can now be treated as unclassified equipment.



**Figure 51 - Unclassified Shutdown**

### **CLASSIFIED Shutdown**

- The system hardware will be left with configuration information intact, even after power has been removed.
- All configuration parameters are retained, and the system may be operated once it is powered up, even if no computer is available to configure the system.
- The system will operate using the most recent configuration file sent into it.
- Classified information is retained on the system, and the system must be treated as classified equipment.

After either method of shutdown, perform the following final steps:

1. Exit the software program.

2. Shut down the computer and disconnect the laptop.
3. The laptop contains classified information; store it in an appropriate location.
4. Turn **OFF** the equipment circuit breakers.
5. Turn **OFF** the vehicle or disconnect the shore power cable.

#### **4.7.5 Zeroize / Emergency Erase**

To zeroize the unit, perform the Unclassified Shutdown described earlier in this section.

## 4.8 Duke System

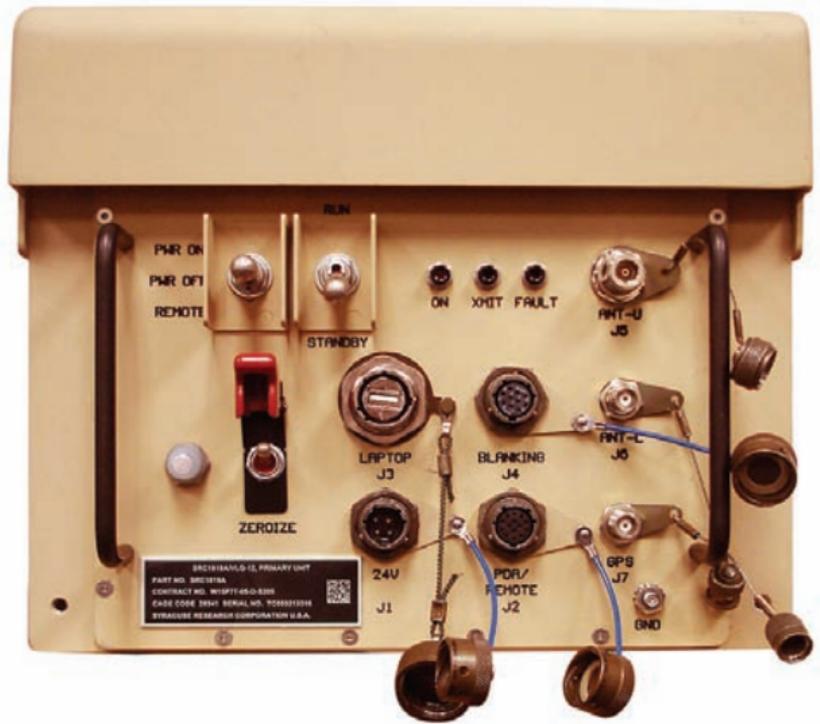


Figure 52 - Duke Device

### 4.8.1 General Description

- Combination (Active & Reactive) Jammer

### 4.8.2 Antenna

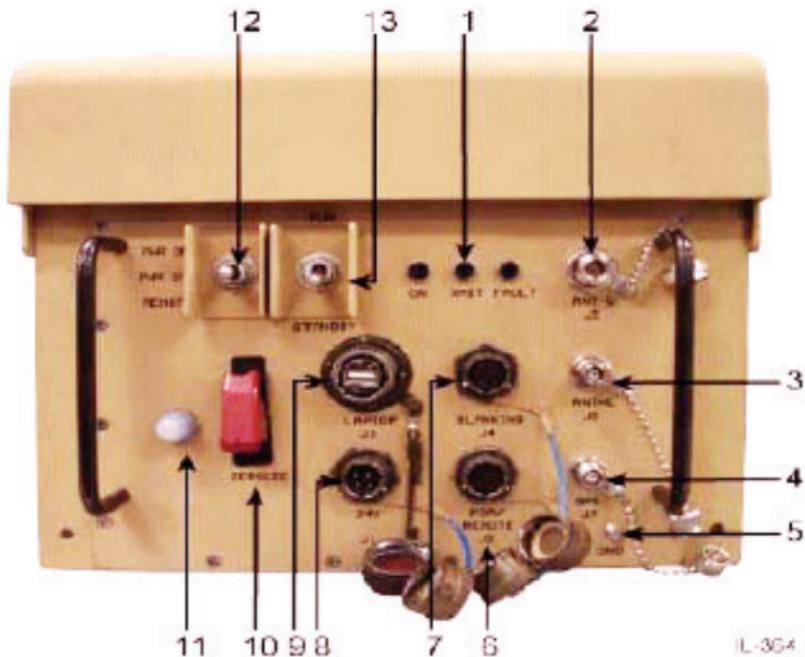
- Dual Band



**ALWAYS CHECK** power cables, antenna cables, nuts, bolts and lock-washers, cable tie-downs, and security fasteners. Inspect the antenna locations for missing or broken parts.

### 4.8.3 Operator Controls & Indicators

#### Primary Control Unit



**Figure 53 - Duke Primary Unit Controls & Indicators**

Item #	Control / Indicator	Condition	Function
1	ON	Green	Indicates power is applied. Green LED will blink in STANDBY mode
	XMIT	Amber	Indicates system is jamming
	FAULT	Red	Indicates system Fault
2	ANT-U (J-5) Connector		Connects Dual Band antennas upper Band (Type N to Type N) cable to the Primary Unit
3	ANT-L (J-6) Connector		Connects Dual Band antennas Lower Band (Type BNC to Type BNC) cable to the Primary Unit
4	GPS Connector		Used to connect the GPS antenna and cable to (J7). The GPS cable has a Type-TNC connector
5	GND Connector		Used to ground the Primary Unit to the vehicle
6	PDA / REMOTE Connector	PDA	Used to connect the PDA Interface Cable to (J2). The PDA is used to upload or retrieve Event Log information and mission configuration data to and from the Primary Unit.
		REMOTE	When operating the system with the RCU, it is used to connect the RCU cable (J2) on the Primary Unit and (J2) on the RCU

Item #	Control / Indicator	Condition	Function
7	BLANKING Connector		Currently reserved for future expansion of the system
8	24V Power Connector		All power sources for Duke are connected to the 24V connector (J1)
9	LAPTOP Connector		Connects the Laptop Interface Cable
10	ZEROIZE Switch	UP	Normal operation
		DOWN	Zeroizes or disables the Primary Unit
11	24V Circuit Breaker		Protects the Primary Unit from input power over-voltage conditions
12	PWR ON / OFF / REMOTE Switch	PWR ON	Provides power to the Primary Unit
		PWR OFF	Removes power from the Primary Unit
		REMOTE	Enables RCU operation
13	RUN / STANDBY Switch	RUN	Places Primary Unit in operational mode
		STANDBY	Places Primary Unit in standby mode

## Remote Control Unit



**Figure 54 - Duke Remote Control Unit Controls & Indicators**

Item #	Control / Indicator	Condition	Function
1	PWR ON / OFF Switch	PWR ON	Provides Power to the Primary Unit
		PWR OFF	Removes Power from the Primary Unit
2	RUN / STANDBY Switch	RUN	Places Primary Unit in operational mode
		STANDBY	Places Primary Unit in standby mode
3	ZEROIZE Switch	UP	Normal Operation
		DOWN	Disables or Zeroizes the Primary Unit
4	ON	GREEN	Indicates Power is Applied. Green LED will Blink in standby mode
	XMIT	AMBER	Indicates System is Actively Jamming

Item #	Control / Indicator	Condition	Function
	FAULT	RED	Indicates System Fault
5	System Connector		Used to connect the RCU cable to (J1) on the RCU and (J2) on the Primary Unit
6	PDA Connector		Used to connect the PDA Interface cable to (J2) on the Primary Unit and (J2) on the RCU. The PDA enables the Operator to remotely transfer new configuration data or download Event Logs remotely from the front of the vehicle.

Duke Fault Indicators			
System State	GREEN ON LED	AMBER XMIT LED	RED FAULT LED
System is Not Booted	ON	ON	ON
System is ON System is Not Reactive Jamming – Transmitting No Fault	ON	OFF	OFF
System is ON System is Jamming-Transmitting No Fault	ON	ON	OFF
System is ON System is Not Reactive Jamming-Transmitting There is a Fault Condition	ON	OFF	ON
System is ON System is Jamming-Transmitting There is a Fault Condition	ON	ON	ON

Duke Fault Indicators			
System State	GREEN ON LED	AMBER XMIT LED	RED FAULT LED
System is ON System is Not Reactive Jamming-Transmitting There is an Antenna-Transmission Line Fault	ON	OFF	ON-Blinking
System is ON System is Jamming-Transmitting There is an Antenna-Transmission Line Fault	ON	ON	ON-Blinking
System is in Standby System is Not Reactive Jamming-Transmitting No Fault Condition	ON-Blinking	OFF	OFF
System is in Standby System is Not Reactive Jamming-Transmitting There is a Fault Condition	ON-Blinking	OFF	ON
System Zeroized	ON-Blinking	ON-Blinking	ON-Blinking

## 4.8.4 Device Operation

### Primary Unit

#### Turn On Procedure

When the Primary Unit is powered on, the four blower assemblies (located under the shroud cover) will start and air will blow out from under the cover.

If the fans are not functioning properly a maintenance action should be initiated, as required, during pre-mission inspection. Ensure there is a 1-inch clearance on the sides and rear of the Primary Unit to allow for adequate air flow.

5. Let the vehicle warm up for at least 3 minutes before turning on the Duke device.
6. Ensure RUN/STANDBY switch is in the **STANDBY** (Down) position.
7. Set the PWR switch on the Primary Unit to the **PWR ON** (Up) position. The green LED will be ON-Blinking.
8. Set the RUN/STANDBY switch on the Primary Unit to the **RUN** (Up) position. The green LED will be ON solid.

#### Set Standby Procedure

1. To place the Primary Unit in standby mode, set the RUN/STANDBY switch to the **STANDBY** (Down) position. The green LED will blink while in Standby mode.

2. To take the Primary Unit out of the standby mode, set the RUN/STANDBY switch to the **RUN** (Up) position. The green LED will return to a solid state.

### Turn Off Procedure

1. Set the RUN/STANDBY switch on the Primary Unit to the **STANDBY** position.
2. Set the PWR switch on the Primary Unit to the **PWR OFF** (Middle) position. The green LED will go out, indicating the power has been removed from the Primary Unit.

### Remote Control Unit

#### Turn On Procedure

1. Ensure the RUN/STANDBY switch on the Primary Unit is in the **RUN** (Up) position.
2. Ensure the PWR switch on the Primary Unit is in the **REMOTE** (Down) position.
3. Ensure the RUN/STANDBY switch on the RCU is in the **STANDBY** (Down) position.
4. Set the PWR switch on the RCU to the **PWR ON** (Up) position. The green LED will be On-Blinking.
5. Set the RUN/STANDBY switch on the RCU to the **RUN** (Up) position. The green LED will be On Solid.

### Set Standby Procedure

1. To remotely place the Primary Unit in standby mode, set the RUN/STANDBY switch on the RCU to the **STANDBY** (Down) position. The green LED will blink while in Standby mode.
2. To take the Primary Unit out of the standby mode, set the RUN/STANDBY switch on the RCU to the **RUN** (Up) position. The green LED will return to a solid state.

### Turn Off Procedure

**DO NOT** turn off vehicle before turning RCU off.

1. Set RUN/STANDBY switch on the RCU to the **STANDBY** (Down) position.
2. Set the PWR switch on the RCU to the **PWR OFF** (Down) position. The green LED will go out indicating the power has been removed from the Primary Unit.
3. Turn off vehicle ignition switch.

### Addressing a fault

Even though there is a fault indication, operators should not leave the system off.

If a fault occurs during a mission, the red LED will light or blink and the system will not function properly.

### To clear the fault

1. Cycle the power from either the Primary Unit (or RCU if being operated remotely) by setting the PWR switch to the **PWR OFF** (Middle) position, waiting 10 seconds, and then setting the PWR switch back to the **PWR ON** (Up) position.
2. If the red LED is not lit or blinking upon power-up, the operator should continue the mission.
3. If the fault does not clear after cycling power (red LED remains lit or blinking), remove power and check the Primary Unit and antenna cable connections.
4. Restore power to the system.
5. If the red LED is not lit or blinking upon power-up, the operator should continue the mission.
6. If the red LED is lit or blinking, the fault has not been cleared. The operator should initiate a maintenance action and contact a Field Service Representative (FSR), as required.

### 4.8.5 Zeroize / Emergency Erase

#### DUKE Primary Unit Zeroize (Disable) Function



**Power must be applied to the Primary Unit to Zeroize the Duke System. Zeroizing the Primary Unit will delete all critical systems information.**

### Zeroize using the Primary Unit

1. Lift the red cover and press down and hold the ZEROIZE switch on the Primary Unit for 10 seconds before releasing the switch.
2. Set the PWR switch on the Primary Unit to the **PWR OFF** (Middle) position.
3. Wait 10 seconds before setting the PWR switch on the Primary Unit to the **PWR ON** (Up) position. All of the LEDs will blink.

### Zeroize using the RCU



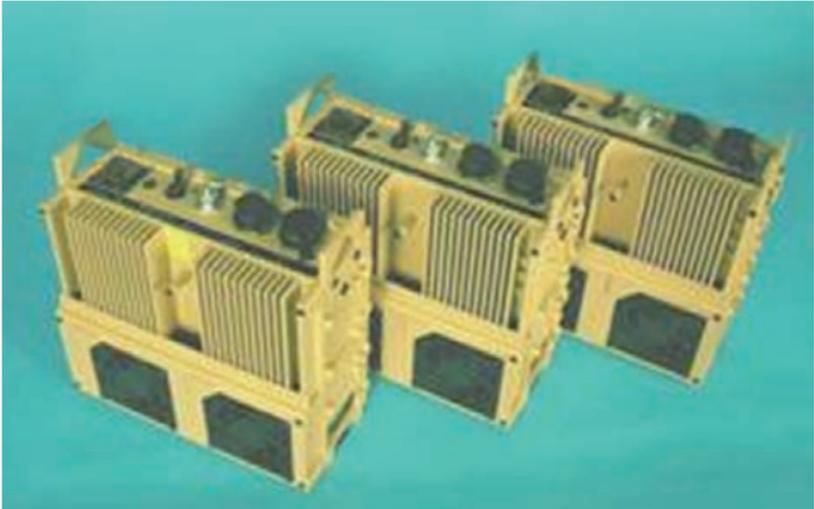
**The Duke System will be disabled and rendered inoperable using the ZEROIZE (3) switch on the RCU. Zeroizing the Primary Unit will delete all critical systems information from the Primary Unit.**

1. Lift the red cover and press down on the RCU ZEROIZE switch for 10 seconds before releasing the switch.
2. Set the PWR switch on the RCU to the **PWR OFF** (Down) position.
3. Wait 10 seconds before setting the PWR switch on the RCU to the **PWR ON** (Up) position. All of the LEDs will blink.



## 4.9 Guardian D (QRD) System

### 4.9.1 General Description



**Figure 55 - Guardian D (QRD) System**

The Guardian D (QRD) system is comprised of three man-portable units; Guardian B1, Guardian B, and Guardian C. Each unit can be used alone; however, when used as a suite of systems, protection is increased. Each unit is comprised of:

- Main equipment
- Antenna
- (2) BB/UBI2590 Lithium rechargeable batteries

Other equipment includes:

- Assault pack
- Battery charger



**Figure 56 - Assault Pack**

Estimated Weights:

- Guardian B - 24.6 lbs.
- Guardian B1 - 24.8 lbs.
- Guardian C - 23.5 lbs.



**Figure 57 - Typical Guardian Device (with battery pack)**

## 4.9.2 Antenna

- Man-pack whip



ALWAYS CHECK power cables, antenna cables, nuts, bolts and lock-washers, cable tie-downs, and security fasteners. Inspect the antenna locations for missing or broken parts.

## 4.9.3 Controls and Indicators



**Figure 58 - Guardian Controls & Indicators**

Antenna sockets are coded for the correct antenna. They are:

System	Socket	Antenna
Guardian B	2 rivets	2 rings
Guardian B1	3 rivets	3 rings
Guardian C	1 rivet	1 ring



This equipment produces enough power to cause RF burns



**Figure 59 – BB/UBI2590 Battery**

### **Self-Test and Fault Indications**

Upon startup, the equipment condition is indicated by the LED on the front panel and an audible buzzer inside the equipment.

When the LED is RED and there is no audible buzzer it indicates that the equipment has been tampered with.

1. Equipment is operational - The LED is green and a double beep is heard approximately 12 seconds after the unit is turned on.
2. When a fault occurs, the LED will turn red and one of four of the following buzzer sequences will be heard:
  - ◆ Antenna Failure - three short beeps, in quick succession, every few seconds – this also indicates the antenna has been connected incorrectly, the Code Plug is faulty, or the GPS unit is obstructed / faulty. Switch off the unit, check/replace the antenna, check/change the Code Plug, or check/change the GPS unit.
  - ◆ Low Battery - one short audible beep every 0.25 seconds for 30 seconds - a replacement battery must be fitted within 10 minutes.
  - ◆ Battery Failure - continuous audible tone – equipment shutdown is imminent. The equipment must be shut down and batteries replaced.
  - ◆ Internal Failure - continuous audible tone – this also indicates a self-test failure and the equipment is no longer operating. It is presumed the equipment has an internal failure and should be returned for repair.

#### 4.9.4 Device Operations



**DANGER** from exploding batteries. Batteries may explode and/or release explosive or poisonous gases if overcharged.

### **Turn ON Procedure**

1. Connect a fully charged battery pack to the unit.
2. Ensure either a Code Plug or GPS unit is connected to the remote socket.
3. Place the unit into an assault pack and secure using webbing straps provided.

Ensure two cooling fans are clear of obstruction.

4. Connect the correct antenna to the antenna socket on the Guardian being used.
5. Turn the unit on by pulling the ON/OFF switch and moving to the **ON** (right) position.
6. Ensure that the double beep sounds indicating that the kit has passed Built-In Test (BIT) and is operational.
7. Ensure LED remains on and green.

### **Turn OFF Procedure**

1. Turn the unit off by pulling the ON/OFF switch and moving it to the **OFF** (left) position.
2. Disconnect the antenna from the antenna socket.
3. Disconnect the Code Plug or GPS unit from the remote socket.
4. Remove the unit from the assault pack.
5. Disconnect the battery pack from the unit and place on an appropriate charger.



The battery pack **MUST** be disconnected from the unit when not being utilized to prevent battery cells from total electrical discharge leading to permanent damage.

### To change a battery pack

1. Turn the unit off by pulling the ON/OFF switch and moving it to the **OFF** (left) position.
2. Disconnect the battery pack using the two spring-loaded, turn latch clamps.
3. Replace the batteries in the battery pack.
4. Secure the battery pack to the unit using the two spring-loaded, turn latch clamps.
5. Turn the unit on by pulling the ON/OFF switch and moving to the **ON** (right) position and ensure the double beep sounds and the LED remains green.

## 4.10 Green System



Figure 60 - Green Device

### 4.10.1 General Description

- Reactive jammer

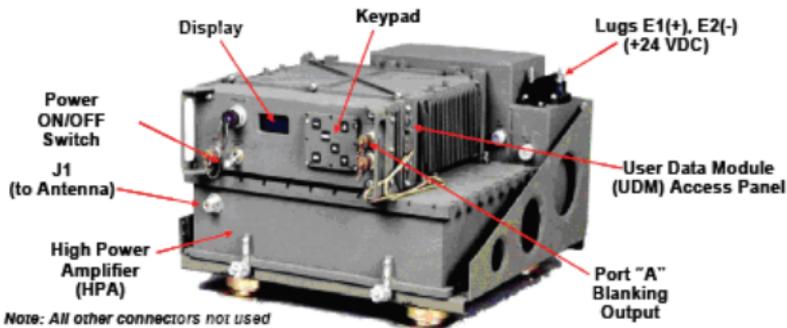
### 4.10.2 Antennas

- Dual band
- Smith



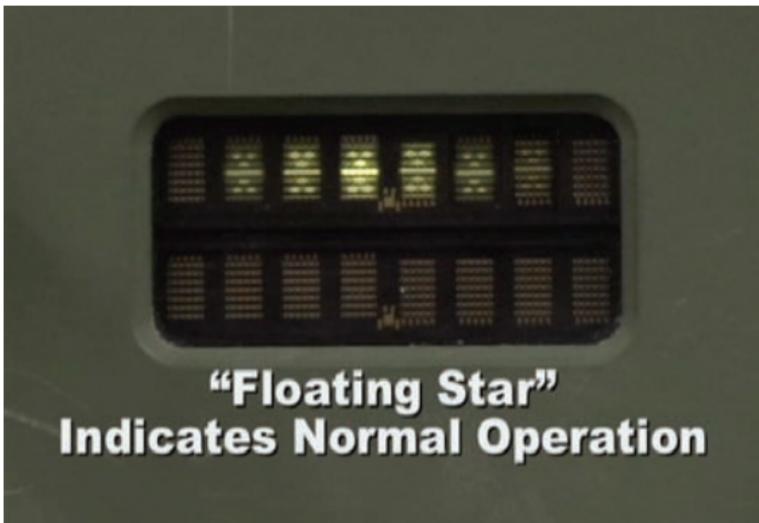
**ALWAYS CHECK** power cables, antenna cables, nuts, bolts and lock-washers, cable tie-downs, and security fasteners. Inspect the antenna locations for missing or broken parts.

### 4.10.3 Operator Controls & Indicators



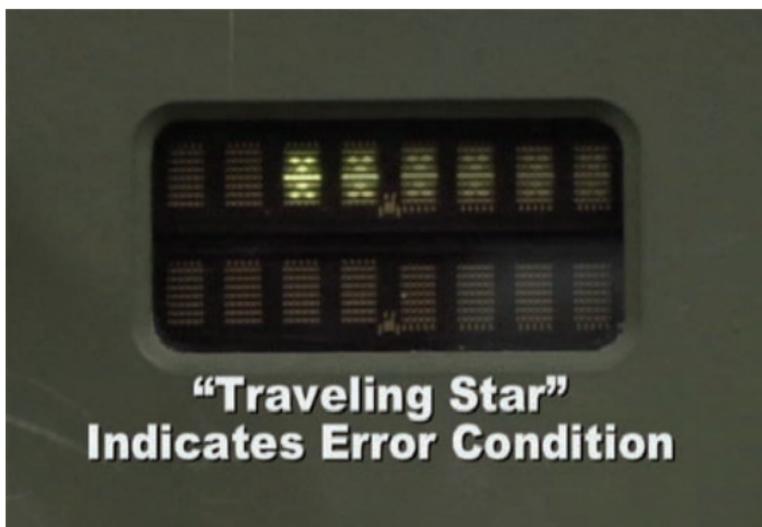
**Figure 61 – Green Controls & Indicators**

The front panel includes an alphanumeric display that is used to provide a quick view of the system status. Two patterns are used – a Floating Star and a Traveling Star. See Figure 62 and Figure 63 for examples of these indications



**Figure 62 - Floating Star indication**

A Floating Star "flickers" and means the device is operating normally.



**Figure 63 - Traveling Star indication**

A Traveling Star "bounces" from side to side and means the device is not operating normally.

#### **4.10.4 Device Operation**

##### **Turn ON Procedure**

1. Let the vehicle warm up for at least 3 minutes before turning on the Green device.
2. Ensure a UDM card is installed.
3. Pull and move the power switch to the **ON** (up) position.
4. The screen will display INIT WARLOCK.

5. The display will display numerous information messages as the Green goes through its initialization and Built-In Test (BIT).
6. System will indicate WARLOCK OK if initialization is successful. The Green system will then automatically go into the Operate Mode. The display will show OPERATE for 10 seconds. Then the system will show a Floating Star \*\*\*\*\*.
7. The display will show which channel(s) it is transmitting on as it detects signals.

If, during power on, the screen shows "OSS1 VER 5.6" you need to see your FSR for an upgrade to the system to a Blanking Green.

### Turn OFF Procedure

1. Turn off the Green device prior to turning off the vehicle.
2. To avoid damage to the system place it in STANDBY before turning off power.
3. Press the MENU button once, the screen will display OPERATE.
4. Press the down arrow until the screen shows STANDBY.
5. Press the SEL (select) button (now in STANDBY).
6. Pull and move the power switch to the **OFF** (down) position.
7. The display will go off.

## Force Jam Mode



**Figure 64 - Green Force Jam Mode**

**This operation is critical for performance against some threats.**

1. Ensure the Green is in Operate mode and press MENU, then press the DOWN arrow. Once STANDBY is displayed, press SEL.
2. Press MENU then the DOWN arrow until CHANNEL is displayed. Press SEL.
3. Press the UP or DOWN arrows to scroll to the desired channel, then press SEL.
4. Press the UP arrow. When FOR is displayed press SEL.
5. Press the MENU then press SEL; OPERATE is displayed

**Channel # and TX will appear steady while the receiver is saturated**

6. The system is now in the Force Jam mode for the selected channel. An audible tone will sound and FOR Channel # will appear after 10 seconds
7. If additional channels are required for Force Jam mode, repeat Steps 1-6
8. To return to the normal Operation Mode:
  - a. Repeat steps 1-3 then press the down arrow once. ON is displayed.
  - b. Then press SEL, press MENU, press SEL; the Forced Channel is restored to normal operation.

Up to three channels can be selected for Force Jam mode. Check with the program office or S-2/S-6 for Force Jam Channels.

#### **4.10.5 Zeroize / Emergency Erase**

1. Turn off the Power.
2. Remove the UDM card.



## 4.11 Hunter System

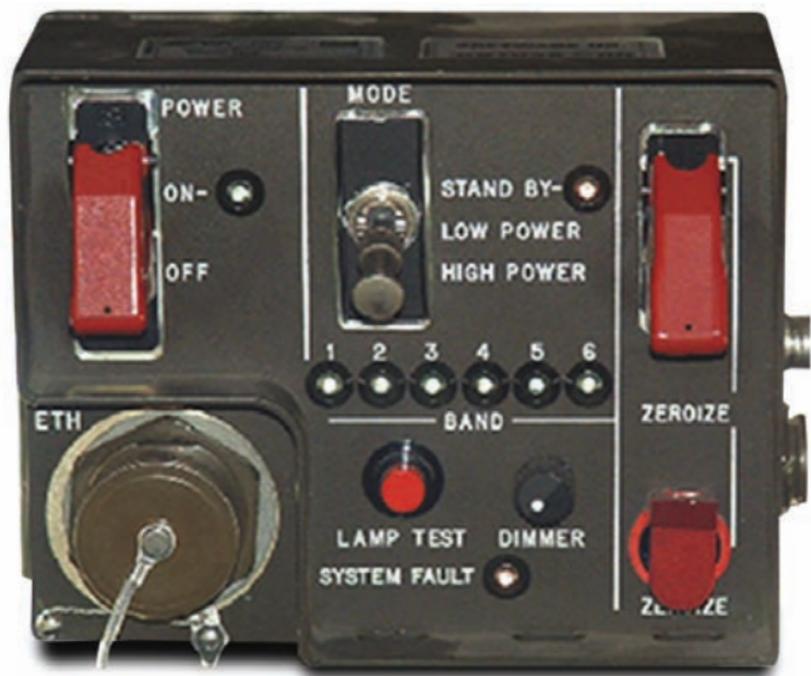


Figure 65 – Hunter Remote Control Unit

### 4.11.1 General Description

- Active jammer

### 4.11.2 Antennas

- Shakespeare whip
- Radome



**ALWAYS CHECK** power cables, antenna cables, nuts, bolts and lock-washers, cable tie-downs, and security fasteners. Inspect the antenna locations for missing or broken parts.

### 4.11.3 Controls & Indicators

Band LED Indicators	
GREEN	Normal operation (RF power OK)
BLINKING (at start up)	<p>Slow blink = BIT</p> <p>Two fast blinks repeating = Standby</p> <p>Rapid blinking = <b>low power</b> – notify FSR</p>
BLINKING (in operation)	<p>Single blink, long pause w/ red Fault LED = continue operations, notify FSR possible VSWR problem</p> <p>Double blink, long pause w/ red Fault LED = continue operations, notify FSR possible vehicle voltage problem</p> <p>Triple blink, long pause w/ red Fault LED = continue operations, internal temperature higher than normal, fault should clear after unit cools to normal operating temp, report to FSR after mission</p> <p>Rapid blinking w/ red Fault LED = continue operations, notify FSR possible power amp problem</p> <p>All bands blinking six times, short pause = system is Zeroized, notify FSR no waveform</p>
OFF	Not transmitting (system is off, channel off or there is a fault) - notify FSR

If any band light does not illuminate or the fault light stays illuminated, contact the FSR.

Mode Switch	
HIGH POWER	Normal operation, all bands working
LOW POWER	Enables low power transmission
STAND BY	Power is on, all bands are configured but not transmitting

Fault LED	
Steady RED	System fault, notify FSR
Off	System OK

#### 4.11.4 Device Operation

##### Turn ON Procedure

1. Let the vehicle warm up for at least three minutes.
2. Ensure STANDBY/LOW POWER/HIGH POWER switch is in the **STANDBY** (up) position.
3. Place the power switch in the **ON** (up) position.
4. The fault light will illuminate and all six band lights will blink once per second for approximately 15 seconds.
5. After 15 seconds, the fault light will go off and all band lights will blink two times and pause.
6. The system is now in standby mode and not radiating.

### **Once in an approved operating area**

1. Move the STANDBY/LOW POWER/HIGH POWER switch to the **HIGH** (down) position.
2. The Fault light will illuminate.
3. All six band lights will blink once per second for approximately 15 seconds.
4. After 15 seconds, the Fault light will go off and all band lights will go solid.
5. The system is now in **HIGH POWER JAMMING** mode.

### **Turn OFF Procedure**

1. Ensure the STANDBY/LOW POWER/HIGH POWER switch is in the **STANDBY** (up) position.
2. Place the power switch in the **OFF** (down) position.

### **4.11.5 Zeroizing / Emergency Erase**

1. Lift and hold protected upper switch and simultaneously push the protected Zeroize push button.
2. Leave power on for at least 90 seconds after pushing Zeroize.

## 4.12 Ironwood System

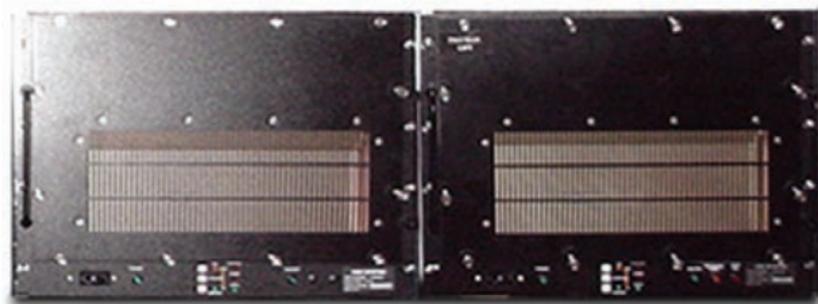


Figure 66 - Ironwood Device

### 4.12.1 General Description

- Reactive jammer

### 4.12.2 Antennas

- Integrated into a vehicle



**ALWAYS CHECK** power cables, antenna cables, nuts, bolts and lock-washers, cable tie-downs, and security fasteners. Inspect the antenna locations for missing or broken parts.

### 4.12.3 Operator Controls & Indicators

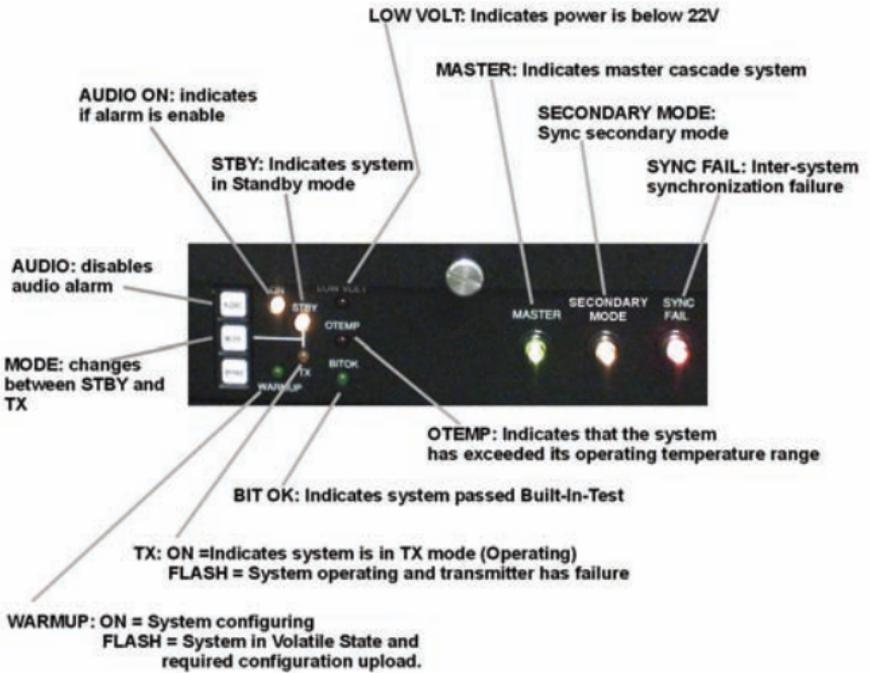


Figure 67 - Front Panel

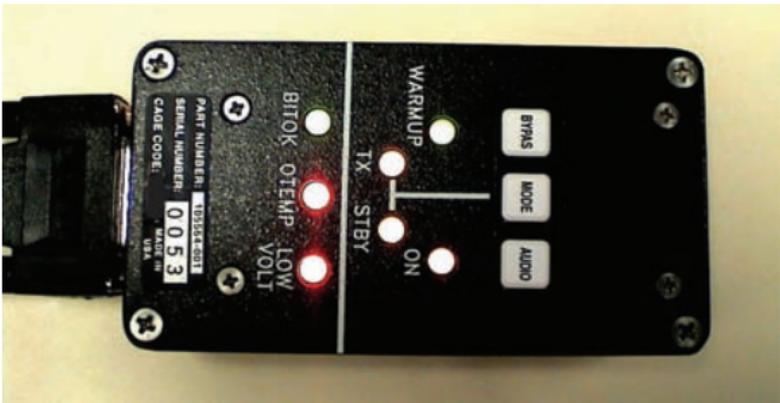


Figure 68 - Ironwood Remote Control

## 4.12.4 Device Operation



The system will not operate correctly with the chassis front panels removed.

The Ironwood system consists of two chassis plus antennas and associated cabling. The LOW System is the master. Commands for the HIGH System are routed through the LOW System. If the LOW System is not in place, the system will not work.

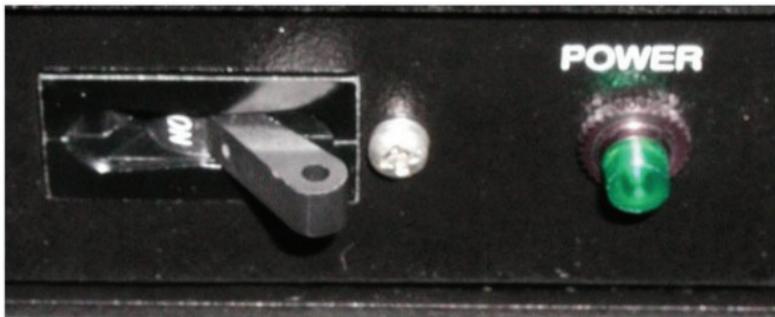
The Ironwood Remote Control operates exactly the same as the Front Panel interface.

### Turn ON Procedure

1. Start the vehicle engine.
2. Let the vehicle warm up for at least three minutes.



If the ambient temperature within the vehicle is below 0 °C, the system requires a five minute warm up period. If the system has not had adequate time to warm up, it may fail its Built-In Test (BIT). It is recommended that system be configured following this warm-up period under these environmental conditions.



**Figure 69 – Low and High Band subsystem circuit breaker**

3. Turn on the circuit breakers on the front of the Low and High Band panels.
4. Connect the laptop computer.
5. Start the laptop
6. Enter a user name and password for Windows login.
7. Double click on the CI software icon.
8. Enter the user name and password for the CI software.
9. If a file holding CI hardware settings has been created previously, open it on the laptop.
10. If the CI hardware settings file does not exist, create a new one using the menus.
11. Click the **Configure Hardware** button at the bottom of the Configuration Screen.
12. Transfer the file from the laptop to the hardware.

13. Click the **Save and Configure** button to save any changes to the file.
14. Once configuration is complete, verify that the Built-In Test has passed by checking the **BIT LED** on the system or the **BIT** lamp on the software screen.
15. If the WARMUP LED flashes, this indicates that the system requires configuration information to operate.



The engine should be running at all times that the system is powered on. If the system is run without the engine, the vehicle batteries **WILL BE DRAINED**

### Turn OFF Procedure

1. Shut down the computer and disconnect the laptop.
2. The laptop contains classified information; store it in an appropriate location.
3. Turn off all circuit breakers on the Power Monitor Unit (PMU).
4. Turn off the vehicle.

### **4.12.5 Zeroize / Emergency Erase**

#### To Zeroize the system using the laptop

1. With the laptop connected to the Ironwood system, go to the Windows Control Software -TW System Summary menu.

2. Select **Reset Hardware**.
3. Select **YES** to declassify the system, which will erase the configuration stored in the EEPROM.
4. Select **NO** to leave the system CLASSIFIED.
5. Exit the software program.
6. Store the laptop in an appropriate location.

## 4.13 mICE System



Figure 70 - mICE Device

### 4.13.1 General Description

- mICE: Modified IED Countermeasure Equipment
- Active jammer

### 4.13.2 Antennas

- Shakespeare
- MaxRAD Dipole



**ALWAYS CHECK** power cables, antenna cables, nuts, bolts and lock-washers, cable tie-downs, and security fasteners. Inspect the antenna locations for missing or broken parts.

### 4.13.3 Operator Controls & Indicators

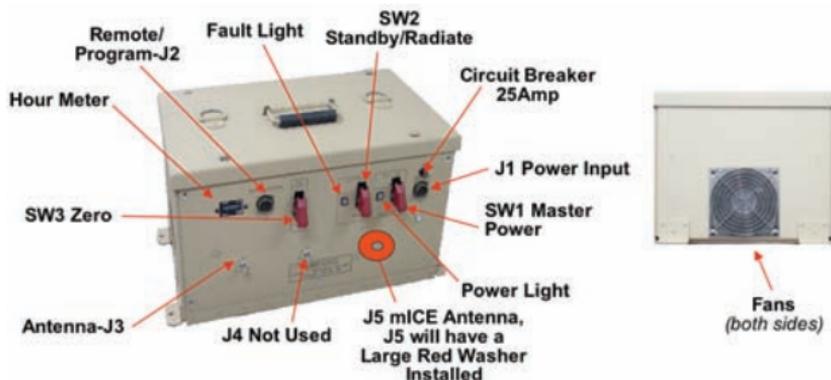


Figure 71 - mICE Controls & Indicators

### 4.13.4 Device Operation

#### Turn ON Procedure

1. Let the vehicle warm up for at least three minutes before turning the unit on.
2. Ensure that the STANDBY/RADIATE switch is in the **STANDBY** (up) position.
3. Place the Master Power switch in the **ON** (down) position.
4. The Fault Light should illuminate and stay on for three to five minutes. If the light does not go out after five minutes – possibly longer in cold weather – there is a fault. Inform your supervisor and / or FSR.
5. Ensure the exhaust fans are operating and clear of debris.
6. When the Fault Light goes out, place the STANDBY/ RADIATE switch in the **RADIATE** (down) position.

Remote unit switch position  
ON = UP = RADIATE  
OFF = DOWN = STANDBY

### **Turn OFF Procedure**

1. Turn off the mlCE prior to turning off the vehicle.
2. Place the STANDBY/RADIATE switch in the **STANDBY** (up) position.
3. Place the MASTER POWER switch in the **OFF** (up) position.
4. Ensure the Power Light is off.



**If using whip antennas, be sure that they are in the upright position.**

### **4.13.5 Zeroize / Emergency Erase**

1. Be sure that the system is powered ON.
2. Lift the Zeroize switch cover and hold the switch in the up position and release.

## 4.14 MMBJ System



Figure 72 - MMBJ Device

### 4.14.1 General Description

- MMBJ: Mobile Multi-Band jammer
- Active jammer

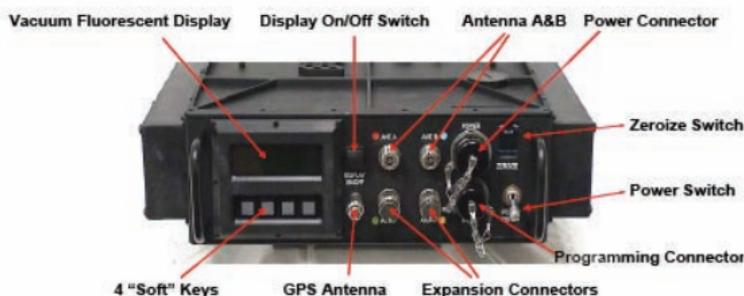
### 4.14.2 Antennas

- A/D Band
- B/C Band



**ALWAYS CHECK** power cables, antenna cables, nuts, bolts and lock-washers, cable tie-downs, and security fasteners. Inspect the antenna locations for missing or broken parts.

### 4.14.3 Operator Controls & Indicators



**Figure 73 - MMBJ Controls & Indicators**

### 4.14.4 Device Operation

#### Turn ON Procedure

1. Let the vehicle warm up for at least three minutes before turning the unit on.
2. Pull and move the Power switch to the **ON** (up) position.
3. The display will come on and cycle through its initialization and Built-In Test (BIT).
4. Press the RF ON 'soft key'.
5. Press the YES 'soft key' to confirm RF is on.
6. Ensure that the fans are turning and moving air.
7. If the display reads "UNIT ZEROIZED" the system is non-functional. Contact FSR for reprogramming software / firmware.

#### Turn OFF Procedure

1. Turn off the MMBJ prior to turning off the vehicle.

2. Press the RF OFF 'soft key'.
3. Press the YES 'soft key' to confirm RF is off.
4. Pull and move the Power switch to the **OFF** (down) position. The display will go off.

## 4.15 Pecan System



Figure 74 - Pecan Device

### 4.15.1 General Description

- Active jammer

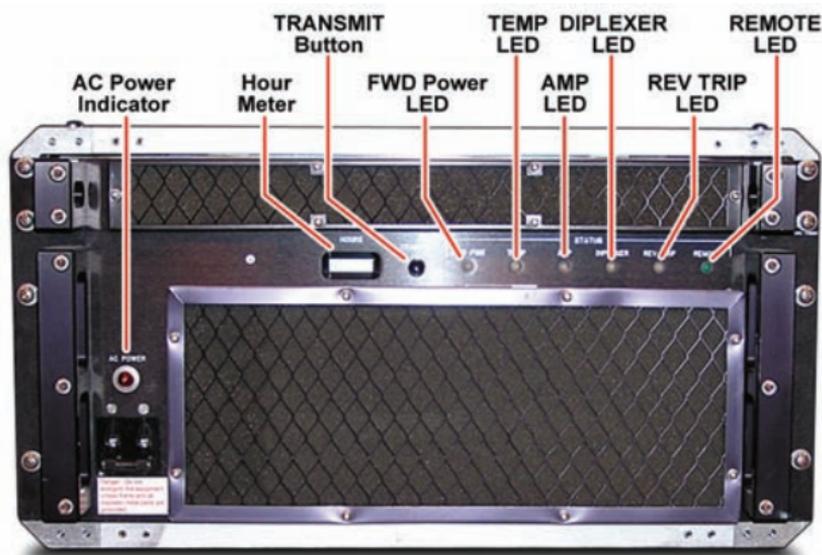
### 4.15.2 Antennas

- Bi-conical
- Omni-directional



**ALWAYS CHECK** power cables, antenna cables, nuts, bolts and lock-washers, cable tie-downs, and security fasteners. Inspect the antenna locations for missing or broken parts.

### 4.15.3 Operator Controls & Indicators



**Figure 75 – Pecan Controls & Indicators**

The chart on the following page shows the indicator conditions and meanings.

Pecan Error Indicators						
	FWD POWER	TEMP	AMP	DIPLEXER	REV TRIP	
Green	Transmit FWD POWER normal	TEMP normal	AMP status normal	DIPLEXER status normal	No REVERSE TRIP detected	
Amber	Transmit FWD POWER marginal	TEMP marginal	N/A	N/A	N/A	
Red	Transmit FWD POWER critical	TEMP critical	Amplifier DC power level(s) are low	DIPLEXER power level is low	REVERSE TRIP condition has occurred	
OFF	Transmit is off or power is off	Power off	Power off	Power off	Power off	

## **4.15.4 Device Operation**

### **Turn ON Procedure**

1. Turn ON the system power switch
2. Make sure the TEMP, AMP, DIPLEXER, and REV TRIP LEDs are green.
3. Push the TRANSMIT button.
4. The system is now transmitting.

### **Turn OFF Procedure**

1. Push the TRANSMIT button.
2. Turn OFF the circuit breaker.

## 4.16 Red System

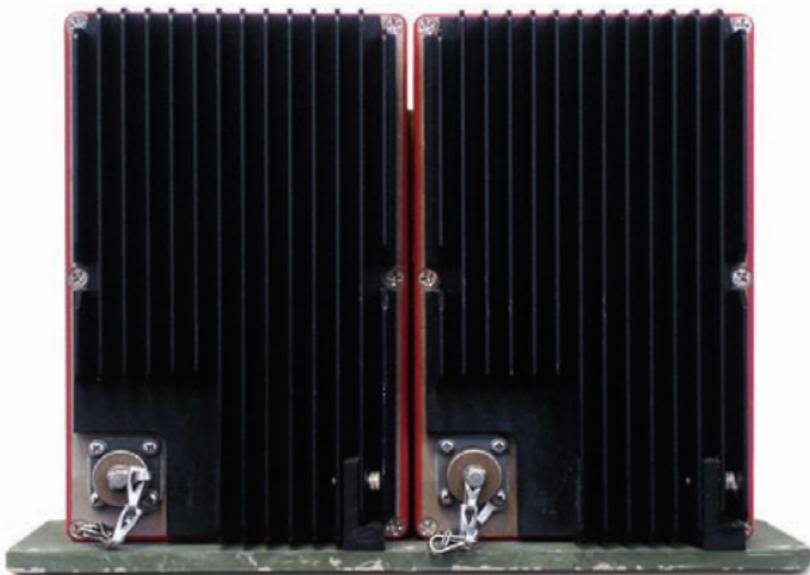


Figure 76 - Red Device

### 4.16.1 General Description

- Active jammer

### 4.16.2 Antennas

- Valcom & Smith  
*or*
- Dual Band



**ALWAYS CHECK** power cables, antenna cables, nuts, bolts and lock-washers, cable tie-downs, and security fasteners. Inspect the antenna locations for missing or broken parts.

### 4.16.3 Operator Controls & Indicators

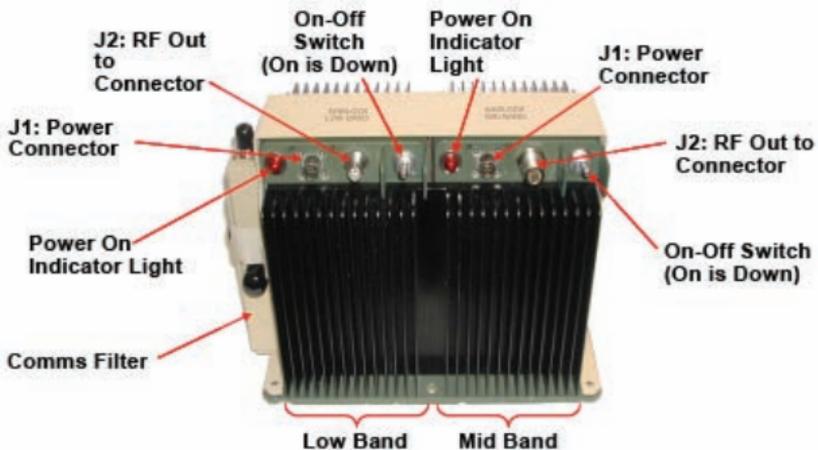


Figure 77 – Red Controls & Indicators

### 4.16.4 Device Operation

#### Turn ON Procedure

1. Let the vehicle warm up for at least 3 minutes before turning unit on.
2. Place both switches on the Low and Mid Band transmitters in the **ON** (down) position.
3. Ensure both power indicator lights are lit.
4. If not lit, inform your supervisor and/or FSR.

**Turn OFF Procedure**

1. Turn off the Red system prior to turning off the vehicle
2. Place both switches in the **OFF** (up) position
3. Ensure both power indicator lights are off

## 4.17 Red / Green Combo



Figure 78 - Red / Green Combo

### 4.17.1 General Description

- Green version 5.12 and blanking cable required
- Combination (Active & Reactive) jammer

### 4.17.2 Antennas

- 2 Dual Band  
*Or*
- Dual Band & Smith

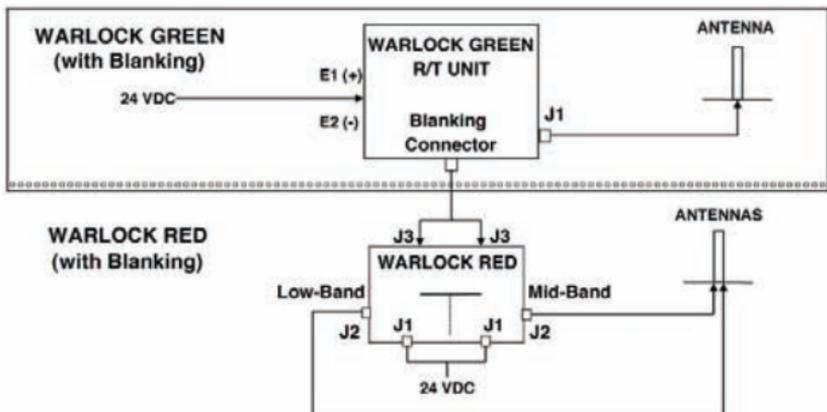


**ALWAYS CHECK** power cables, antenna cables, nuts, bolts and lock-washers, cable tie-downs, and security fasteners. Inspect the antenna locations for missing or broken parts.

### 4.17.3 Red & Green Device Connections

Note: A Red Device can only be cabled to a Green Device v5.12

1. A Red device will be connected to a Green device with a Blanking Cable.
2. When Red is cabled to a Green there will be either two DBC antennas or a DBC & a Smith antenna.
3. See Figure 79 for Red / Green combo cabling.
4. Verify a Blanking Cable is connected
5. Verify that the Dual Band antennas are connected and in upright position.



**Figure 79 - Red / Green Combo Cabling**

## 4.18 Spruce System

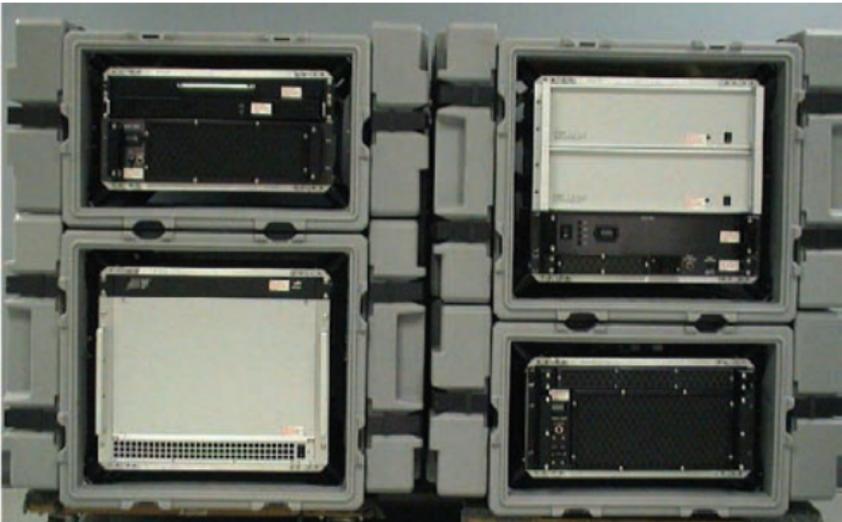


Figure 80 - Spruce Devices

### 4.18.1 General Description

- Reactive jammer

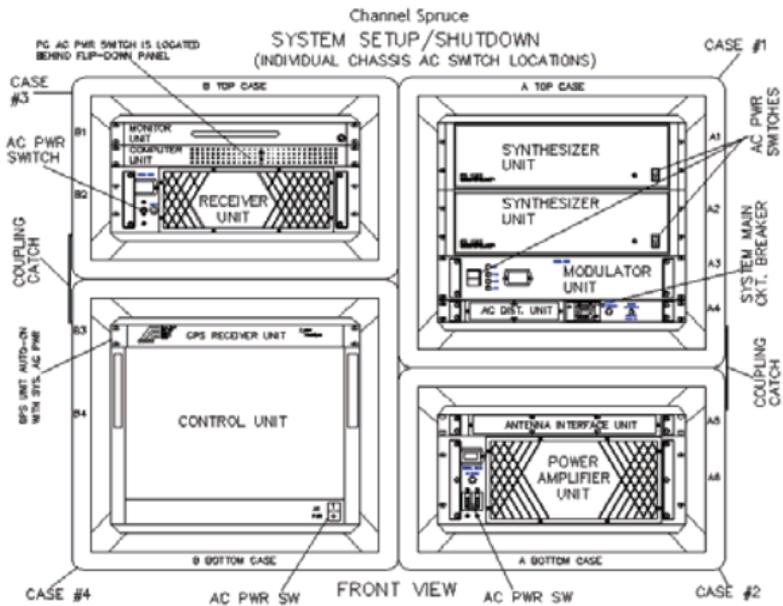
### 4.18.2 Antennas

- Bi-conical
- Discone
- GPS



**ALWAYS CHECK** power cables, antenna cables, nuts, bolts and lock-washers, cable tie-downs, and security fasteners. Inspect the antenna locations for missing or broken parts.

### 4.18.3 Operator Controls & Indicators



**Figure 81 - Spruce Chassis**

### 4.18.4 Device Operation

#### Turn ON Procedure

1. Look in Case 3 and make sure the hard drive is installed. If not, install a hard drive.
2. To apply power to the system, turn on the system main circuit breaker at the bottom of the Modulator Unit (A4).
3. Turn on the other circuit breakers in the other cases. The AC power switch for the system PC is located behind the “flip-down” panel located on the PC Unit (B1) front panel.
4. Use Figure 81 for location of all circuit breakers.

When the MAIN AC Circuit Breaker is switched to the **ON** position, the GPS Receiver Unit (B3) is also turned ON. The GPS Receiver could, per the manufacturer's specifications, require up to six (6) hours acquiring lock and determining the position of the GPS Antenna. In most situations the TFOM (Time Figure of Merit) of the GPS Receiver will require less than six (6) hours to be well within the system timing accuracy.

5. Wait for the PC to boot the Windows operating system.
6. Enter the appropriate operator or supervisor password.
7. On the Desktop, double click on Channel Spruce.
8. Once software has initialized, the laptop will establish a connection with the hardware.
9. A dialog will appear asking the user to select the mission name.
10. Select an appropriate existing mission name from the list provided on the dialog.
11. Select OK.
12. A message will be displayed notifying you that the mission has been loaded.
13. The system is now in STAND-BY mode and ready to accept commands from the user.
14. Select the Operate icon to place the system in operate mode.

## **Turn OFF Procedure**

1. After mission operations have been completed, place the system in STAND-BY mode by selecting the Standby icon.
2. Terminate the GUI application by selecting the EXIT command from the File menu or press the  icon on the GUI Main Window tool bar.
3. Turn OFF all remaining AC power front panel switches except on the AC Distribution Unit (A4).
4. Switch the system MAIN circuit breaker, located on the AC Distribution Unit (A4), to the **OFF** position.
5. Remove the hard drive and secure it in an appropriate location.

When removing power, remember to power down all circuit breakers prior to shutting off the Main Circuit Breaker.

### **4.18.5 Zeroize**

Follow Turn Off procedures.

## 4.19 SSVJ System



Figure 82 - SSVJ Device

### 4.19.1 General Description

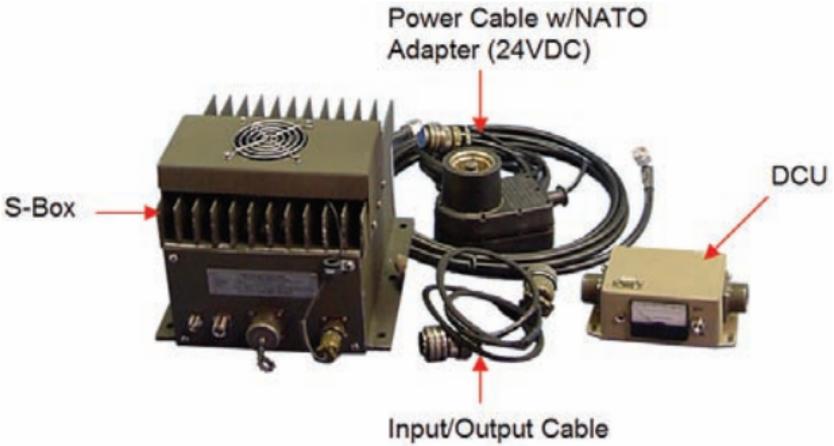
- SSVJ: Self Screening Vehicle Jammer
- Active jammer

### 4.19.2 Antenna

- Snorkel

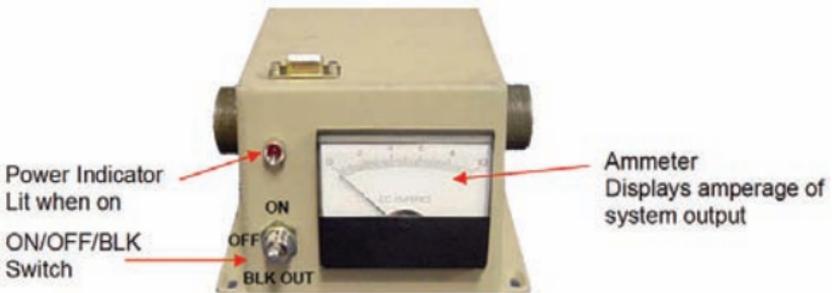


**ALWAYS CHECK** power cables, antenna cables, nuts, bolts and lock-washers, cable tie-downs, and security fasteners. Inspect the antenna locations for missing or broken parts.



**Figure 83 - SSVJ Components**

### 4.19.3 Operator Controls & Indicators



**Figure 84 - DCU Controls & Indicators**

DCU Controls	
Up	System ON
Center	System OFF
Down	System ON / BLK OUT (blackout)
Amp Meter	Nominal reading of >3.8 and < 5.3

## 4.19.4 Device Operation

### Turn ON Procedure

1. Let the vehicle warm up for at least 3 minutes before turning unit on.
2. Move the switch to the **ON** (up) position (the Power indicator illuminates bright).
3. System is transmitting in **UP** or **DOWN** position.
4. Move the switch to **BLK OUT** (down) position and verify that the Power indicator is dim.



Amp meter readings  $< 3.8$  or  $> 5.3$  indicate incorrect power to the system.

5. If the Power indicator does not come on recheck power leads. Note that the Power indicator can be green or red when illuminated.
6. If the amp meter reads low or high, contact the FSR.

### Turn OFF Procedure

1. Move the switch to the **OFF** (center) position.
2. The Power indicator should be extinguished.
3. Turn off the vehicle.

## 4.20 Warlock LX System



Figure 85 - Warlock LX Device

### 4.20.1 General Description

- Reactive jammer

### 4.20.2 Antenna

- LX system is integrated in a vehicle



**ALWAYS CHECK** power cables, antenna cables, nuts, bolts and lock-washers, cable tie-downs, and security fasteners. Inspect the antenna locations for missing or broken parts.

### 4.20.3 Operator Controls & Indicators

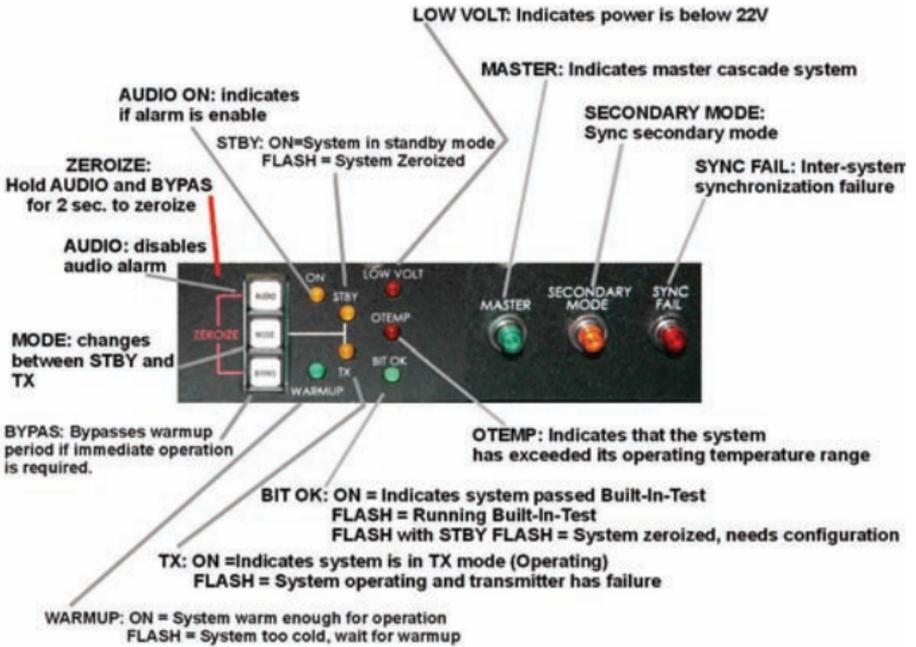


Figure 86 - LX Front Panel Controls & Indicators



Figure 87 - LX Remote Control

System State		LX Indicators						
	WARMUP	STBY	TX	BIT OK	OTEMP	LOW VOLT		
Unclassified or ZEROIZED	X	BLINK	OFF	BLINK	X	X		
Warming Up	BLINK	OFF	OFF	OFF	X	X		
Configuring or Running BIT	ON	OFF	OFF	BLINK	X	X		
Not Ready	ON	OFF	OFF	X	X	X		
Standby Mode	ON	ON	OFF	X	X	X		
Low Voltage Present	X	X	X	X	X	ON		
Over Temp Present	X	X	X	X	ON	X		

X = indeterminate, depends on other conditions (Not Blinking)  
 ON = LED is on      OFF = LED is off      BLINK = LED is blinking

## 4.20.4 Device Operation

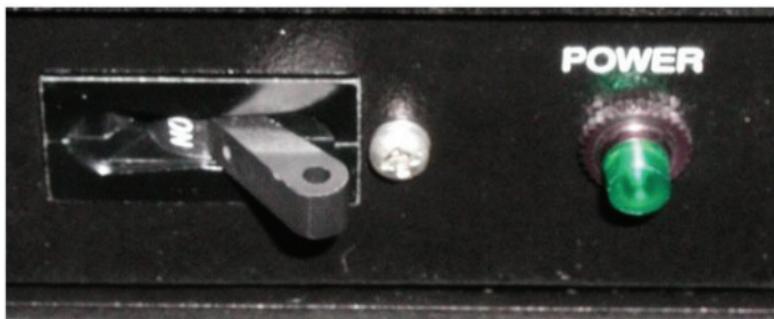


The system will not operate correctly with the chassis front panels removed.

The Warlock LX Remote Control operates exactly the same as the Front Panel interface.

### Turn ON Procedure

1. Start the vehicle engine.
2. Make sure that the LOW-Q chassis front panel is attached.
3. Turn on the circuit breaker on the front of the LOW-Q panel.



**Figure 88 - LOW-Q subsystem circuit breaker**

4. Once system power has been applied, the LEDs on the Front Panel and the Remote Control will flash on briefly.
5. The system then begins a boot-up sequence that typically ends with the system entering the Standby state and with the Built-In-Test (BIT) passing.

This condition is noted by viewing the **STBY** and **BIT OK** LEDs illuminated. This process takes approximately 40 seconds.



If the ambient temperature within the vehicle is below 0 °C, the system requires a five minute warm up period. If the system has not had adequate time to warm up, it may fail its Built-In Test (BIT). It is recommended that the system be configured following this warm-up period under these environmental conditions.

6. Connect the laptop computer.
7. Start the laptop and LX software.
8. If a file holding LX hardware settings has been created previously, open it on the laptop.
9. If the hardware settings file does not exist, create a new one using the menus.
10. Click the Configure Hardware button at the bottom of the Configuration Screen

11. Transfer the file from the laptop to the LX hardware.
12. Click the Save and Configure button to save any changes to the file.
13. Once configuration is complete, verify that the Built-In-Test has passed by checking the BIT LED on the system or the BIT lamp on the software screen.
14. If the WARMUP LED flashes, this indicates that the system requires configuration information to operate.



The engine should be running at all times that the system is powered on. If the system is run without the engine running, the vehicle BATTERIES WILL BE DRAINED

### System Bypass

1. To bypass the system warm up time press the **BYPAS** button.
2. The **BYPAS** button will bypass the warm up time and immediately configure the system for operation

### Turn OFF Procedure

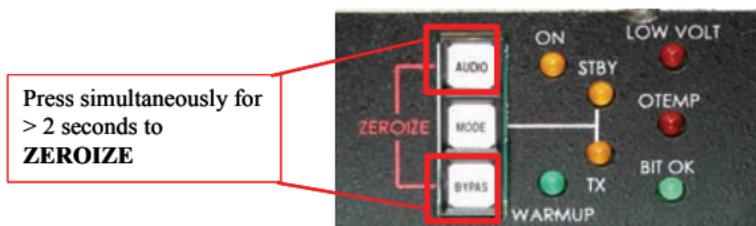
1. Zeroize the system
2. Shut down the computer and disconnect the laptop.
3. Turn off the circuit breaker.

- Turn off the vehicle.

#### 4.20.5 Zeroize / Emergency Erase

##### To Zeroize the system using the front panel

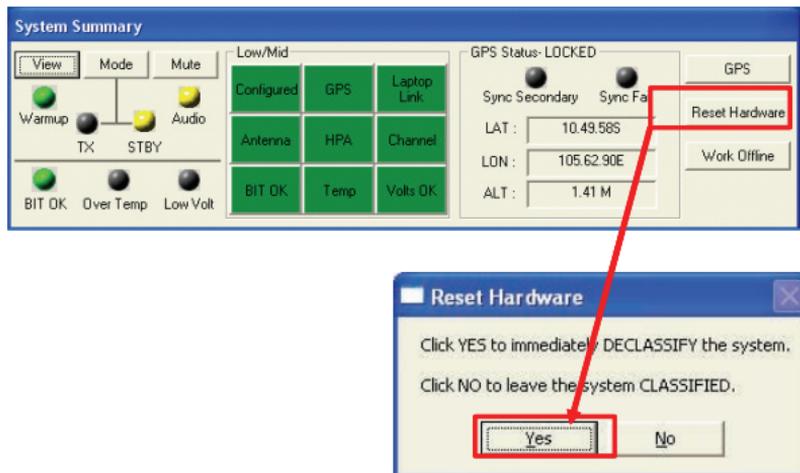
- Press the **AUDIO** and **BYPAS** buttons simultaneously for more than two seconds.
- When ZEROIZE is initiated, all classified data is purged and the system is rendered unusable until it is reconfigured with the laptop computer.
- The **BIT** and **STBY** LEDs will blink continuously once the Zeroize function is complete.



**Figure 89 - LX Zeroize Buttons**

##### To Zeroize the system using the laptop

- With the laptop connected to the LX system, go to the Windows Control Software -TW System Summary menu.
- Select Reset Hardware.
- Select YES to DECLASSIFY System, which will erase the configuration stored in the EEPROM.
- Select NO to leave the system CLASSIFIED.
- Exit the software program.



**Figure 90 - Zeroize from laptop**



**The system and laptop remain classified and must be properly handled after Zeroizing**

### What you learned in this chapter

- The different types of jammers
- Basic PMCS procedures
- How different types of CREW devices are operated

# Chapter 5

## CREW System Interoperability and Communication Alternatives

### What you will learn in this chapter

- What are interoperability considerations with CREW?
- What are some communications alternatives?

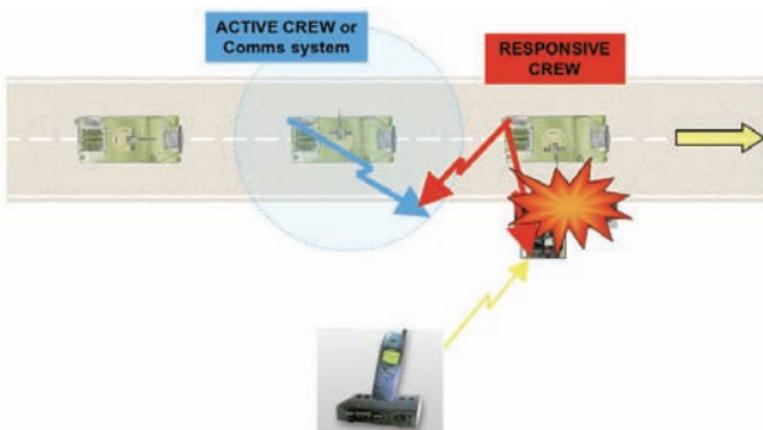
### 5.1 CREW System Interoperability

As shown in Figure 91, CREW systems may interfere with each other when they are too close. Specifically, reactive systems don't work well with active systems. Active systems don't care what other CREW systems are around; however, active CREW systems can cause reactive CREW system to respond, thereby tying up a portion of its power resources. This may cause a reactive CREW to not see and/or not be able to respond to an actual threat signal and expose you to RCIED attack.

### Why is my CREW jamming my comms?

- CREW systems will not identify any difference between legitimate comms and threat devices and will work to defeat them both.
- Turning off CREW for comms will expose you to RCIED attack.

- Good communications do not defeat RCIEDs



**Figure 91 - Interoperability**

- CREW may interfere with each other when too close.
- Refer to paragraph 1.6 Frequency De-confliction for more information.
- CREW antennas must be separated at least 36 inches from each other and other antennas (for example GPS or SINCGARS). Do not make modifications to antenna placement or place anything near the antennas as signal broadcast may be affected.
- Best advice:
  - ◆ Perform Preventative Maintenance Checks & Services (PMCS), Pre-Convoy Checks (PCC), and Pre-Convoy Inspections (PCI) on your comm gear and CREW systems.
  - ◆ OP test all your equipment together before you go outside the wire.
  - ◆ Plan your convoy using the Convoy Planning Tool, know your TTPs, and study your route and its history of IED attacks.
  - ◆ Turn CREW on, and apply your TTPs.

- The chart on the next page will help you understand when there are possible conflicts between CREW systems. It is reproduced inside the back cover of this handbook for easy reference. ALWAYS check with your S-2 / S-6 when multiple CREW systems are employed to avoid potential conflicts!

**CREW Systems Interoperability**

	Duke	Green	Red/Green	Ironwood	LX	Cottonwood	Red	SSVJ	MMBJ	mICE	Acorn	Chameleon	Hunter	Blue	Guardian
Duke															
Green															
Red/Green															
Ironwood															
LX															
Cottonwood															
Red															
SSVJ															
MMBJ															
mICE															
Acorn															
Chameleon															
Hunter															
Blue															
Guardian															

- **YELLOW** boxes indicate systems that require separation to avoid interference. See S-2 or S-6 for further information.
- **GREEN** boxes represent no known interference.

## 5.2 Communications Alternatives



**NEVER TURN OFF YOUR CREW SYSTEM UNTIL YOUR AREA IS SECURE!**

If unable to de-conflict frequencies between the CREW system and communication equipment, here are the best alternatives to restore comms:

1. Notify EWO of comms conflict. They may know of a technical solution, which may include relocation of the antenna to a different location.
2. Use FBCB2/BFT ability to transmit information as primary means of communication in accordance with Mission Execution Checklist.
3. Coordinate with Signals Officer or Comms NCO to change comms antenna type from omnidirectional to more focused transmission capability.
4. Coordinate with Signals Officer or higher for alternate means to communicate (e.g. TACSAT, HF).

When meeting another convoy determine if there is an interoperability conflict. If none, proceed with mission. If a conflict is determined:

1. Talk with the other Convoy Commander and decide who will shut down their CREW equipment.

2. If convoys have to operate in the same area, one of them must back out of range of the other jammer.

The CREW device will not identify any difference between legitimate comms and threat devices and will work to defeat them both.

### **What you learned in this chapter**

- Interoperability considerations using CREW
- Communication alternatives

# Chapter 6

## Employment Considerations

### What you will learn in this chapter

- What should you consider when planning a convoy?
- What is the Convoy Planning Tool?
- What are the CREW employment techniques?
- What should you do at an IED site?
- What should you do after a convoy?



The purpose of this chapter is to give Commanders, Leaders and Warfighters a training tool that identifies some of the considerations to be addressed before employment of CREW equipment.

## 6.1 Pre-Convoy Measures

### 6.1.1 Convoy Planning

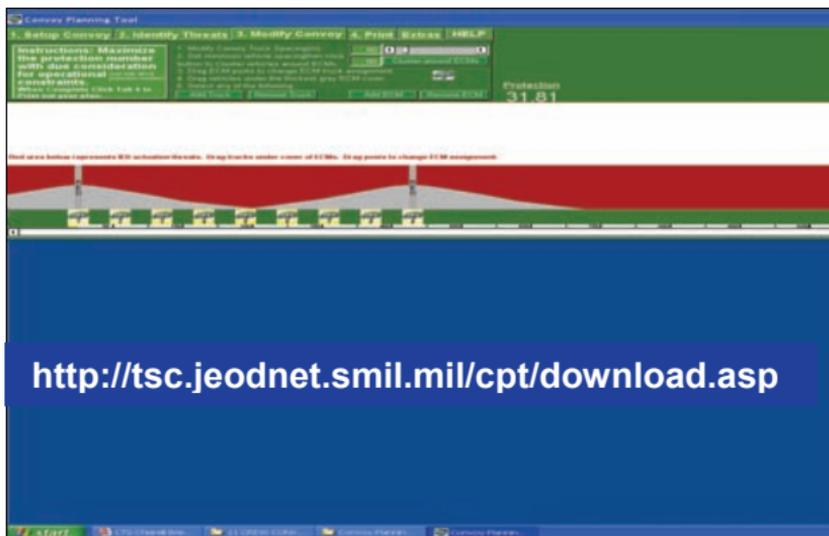
#### What is the Convoy Planning Tool (CPT)?

#### Convoy Planning Tool

The Convoy Planning Tool (CPT) is used by Commanders and Leaders to plan the placement of CREW systems within a convoy to maximize protection against RCIEDs. It is used by:

- ◆ Convoy commanders

- ◆ Vehicle drivers
- ◆ Convoy passengers



**Figure 92 – Convoy Planning Tool**

### **CPT capabilities**

- Provides Electronic Countermeasure (ECM) insight.
  - ◆ Different types of CREW equipment have varying capabilities against RCIED threats.
- Aids in selecting the CREW system that is most effective against the prevailing threat.
- Allows commanders to set up a convoy using information such as:
  - ◆ The number of vehicles in the convoy.
  - ◆ Appropriate spacing between vehicles.
  - ◆ Number of CREW systems.
  - ◆ Types of CREW systems.
  - ◆ Placement and separation of CREW equipment.
  - ◆ Known RCIED threats.

**The CPT helps plan maximum protection for everyone participating in a convoy.**

### 6.1.2 Convoy briefing

**ALWAYS BRIEF YOUR PERSONNEL!**



- Rehearse action for future contact with an IED and know everyone's duties.
- Identify local SOPs for action upon contact with an IED.
- Use secure communications.
- Identify potential conflicts between communications frequencies and the CREW equipment and plan communication alternatives.

### 6.1.3 Pre-convoy checks

- Conduct preventive maintenance checks and services (PMCS).
- Conduct communication checks with CREW off and on.
- Test all radios and GPS devices.
- Rehearse unit employment measures.
- Operators should test all systems.
- Brief on the latest IED threat intelligence.

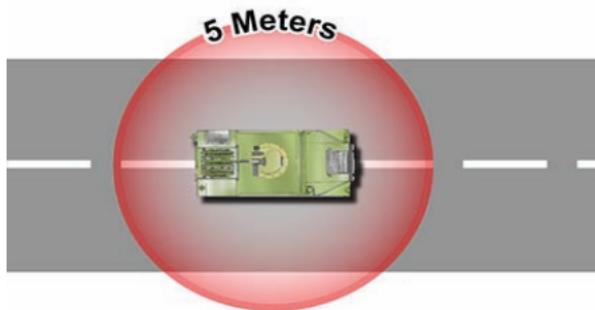
## 6.2 In-Convoy Measures

**What is the 5/25 method of surveillance?**



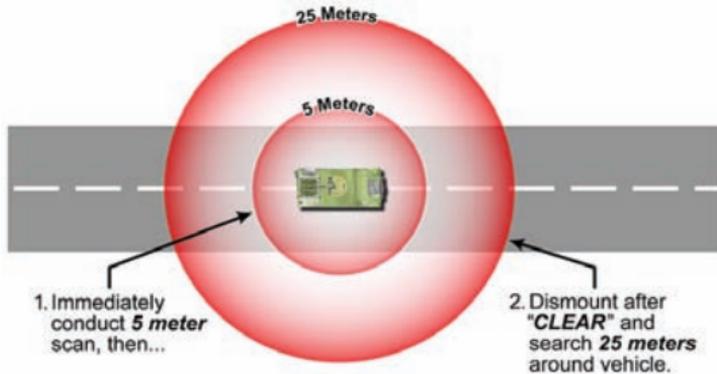
Wear personal protective equipment (vests, helmets, hearing protection and eye protection) at ALL times.

- Remain vigilant.
- Be unpredictable in the times and routes the convoy uses.
- Be extra cautious at choke points and watch flanks for IEDs if something causes the convoy to stop.
- Maintain speed and movement.
- Maintain vehicle dispersion and spacing.
- If something stops movement, survey the immediate area using the 5/25 method of surveillance.



Immediately scan 5 meters  
around vehicle for IEDs  
Give the TC "**CLEAR**"

**Figure 93 - Short Halt scan**



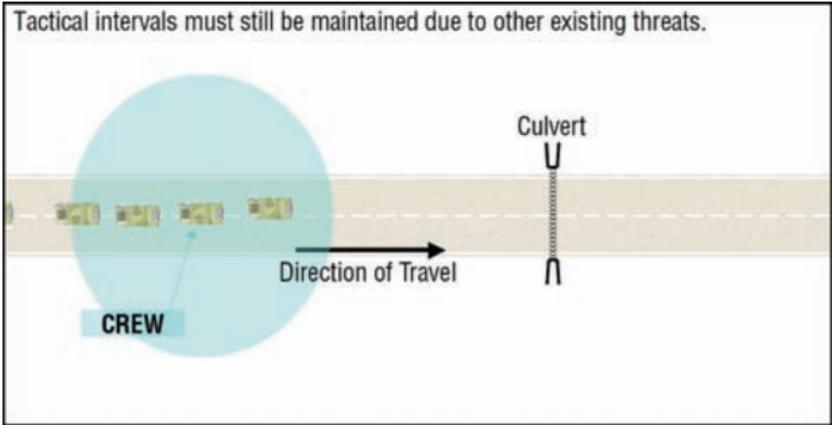
**Figure 94 - Long Halt scan**

Do NOT exit vehicle until given permission in accordance with the Unit SOP. Don't establish Long-Term Halt until 25m search has been conducted.

**The 5 meter surveillance is conducted to search for IEDs in your immediate vicinity. A 25 meter search is conducted, once "Clear" is given, to identify secondary IEDs or triggermen.**

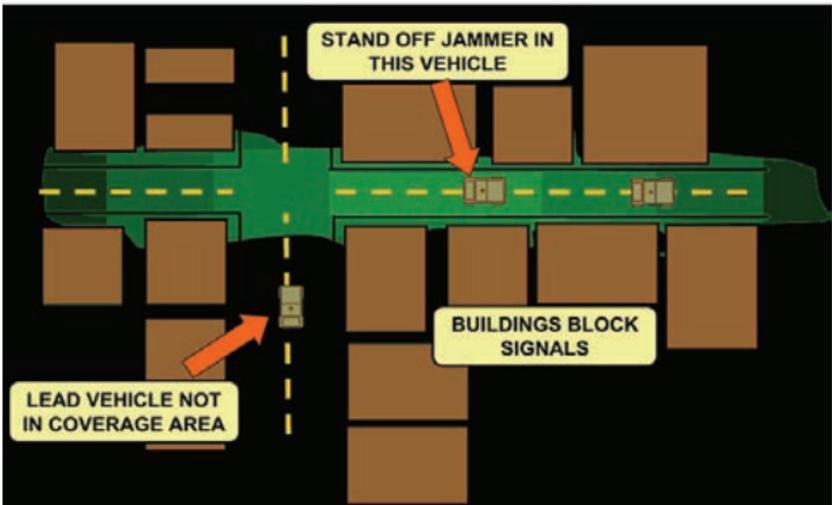
### 6.2.1 Convoy movement with CREW

- Map recon should identify most vulnerable points on the primary and alternate routes.
- Lead with CREW vehicles when approaching higher threat areas.



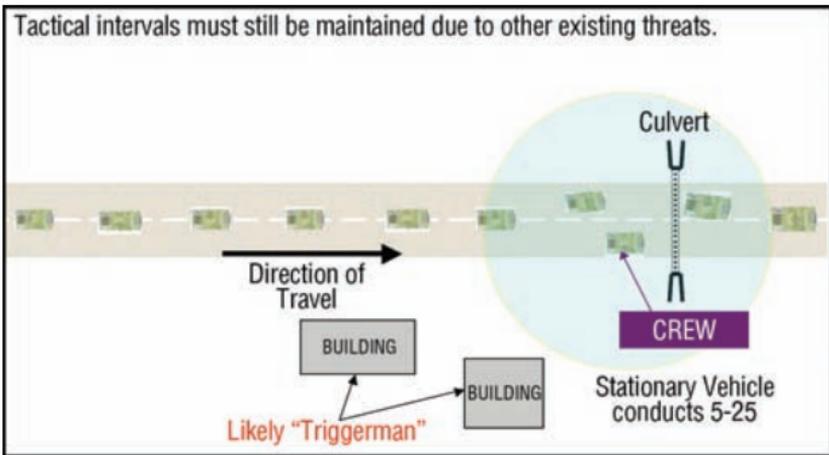
**Figure 95 - Approaching likely attack spots**

- Vehicles rounding a corner may not have CREW coverage until the vehicle with the CREW approaches the corner.
- Do NOT round off corners when making turns.



**Figure 96 - Masking in an urban area**

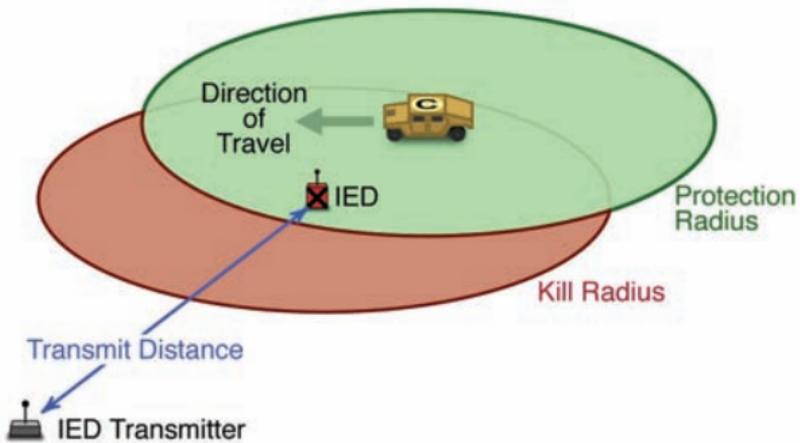
- CREW vehicle may be placed into an overwatch position where it can provide the most cover before executing the maneuver itself.
- When one CREW system is used, the patrol leader must decide whether to employ it forward at key positions.



**Figure 97 - Covering likely attack spots**

### 6.2.2 Single vehicle jamming

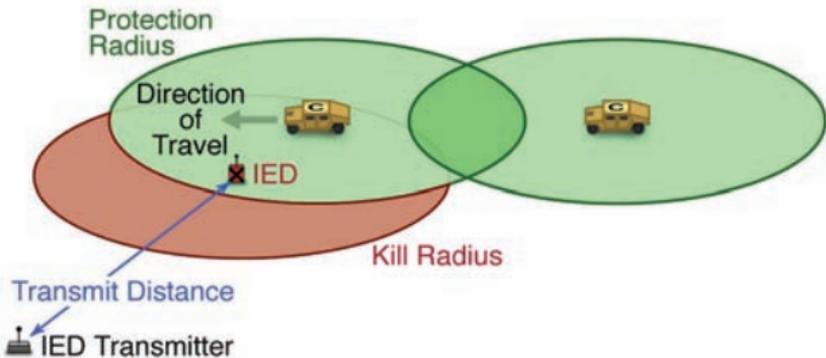
- If you are within an IED kill radius, you need CREW system protection.
- CREW jams the receiver at the RCIED, not the transmitter.



**Figure 98 - Single vehicle jamming**

### 6.2.3 Two vehicles, two jammers

- Two vehicles, both with jammers
- Overlaps in middle for additional coverage
- Check Interoperability Chart when employing multiple CREW jammers.

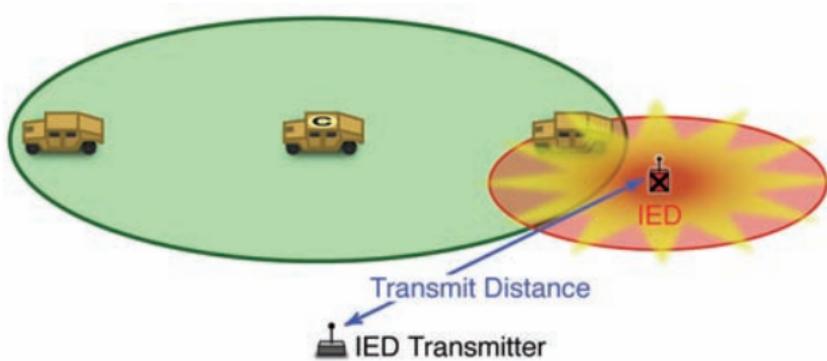


**Figure 99 - Two vehicles, two jammers**

### 6.2.4 Multiple vehicles, single jammer

- Jammer in center vehicle

- Leaves rear vehicle in the blast area as it passes the IED
- Convoy should tighten up



**Figure 100 - Multiple vehicles, single jammer**

### **6.2.5 Multiple vehicles, multiple jammers CREW coverage in urban areas**

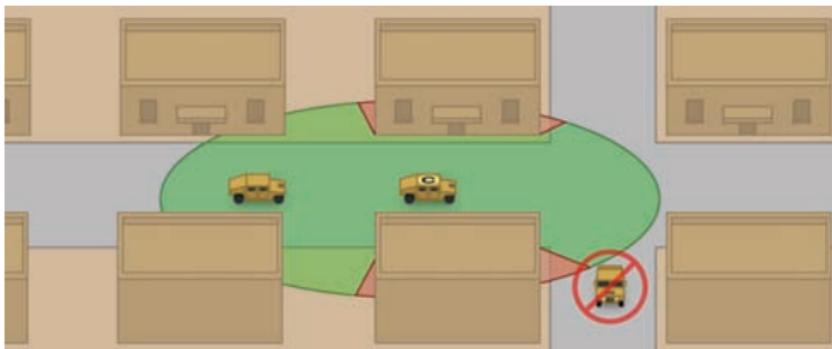
- All vehicles have a jammer
- Buildings mask the effectiveness of the jammers



**Figure 101 - Multiple vehicles, multiple jammers  
in urban area**

## 6.2.6 Multiple vehicles, single jammer in urban area

- Only center vehicle has a jammer
- Buildings limit protection area
- Lead vehicle is unprotected
- Convoy should tighten up



**Figure 102 - Multiple vehicles, single jammer in urban area**

## 6.2.7 CREW operations procedures

- Turn systems on and off when leaving and entering the FOB based on SOP.
- If communications are lost:
  - ◆ Check communications equipment.
  - ◆ Retransmit the complete report.
  - ◆ Other vehicles may hear the reply from the distant station.
- Move C2 vehicle away from the CREW vehicle.
- Utilize other means to send and receive messages.



DO NOT turn CREW off while at an IED site unless coordinated with onsite EOD team leader.

- Coordinate with QRF, EOD or other units with CREW in their patrol/convoy.
  - ♦ What kind of equipment is used?
  - ♦ Who will turn off the equipment if required?

### 6.2.8 Encountering an IED – the 5 C's



**DO NOT approach an IED!**

- Do **NOT** attempt to move the IED.
- Do **NOT** hug the curb at potential IED locations but stay in the middle of the road.
- **NEVER** drive over a suspected IED.

**What are the 5 Cs associated with suspected IEDs?**



- Scan the immediate surroundings from a 360 degree perspective.
- Use optics.

- Conduct surveillance, from a safe distance, of both the suspected IED and for a triggerman and do not attempt to move the possible IED.
- Indicate location of suspected IED using unit designated marking system.
- The first vehicle in the patrol to identify the suspected IED should attempt to alert other vehicles of the suspected IED location and mark it IAW unit SOP.
- The nearest vehicle from the IED with a radio must transmit the location of the IED to the remainder of the patrol using vehicle internal call signs and indicate the distance and direction of the threat.
- Use available hard cover to the maximum extent.
- Conduct checks of the immediate surroundings to ensure that there are no secondary devices. Use theater specific methods, such as the 5/25 method.
- Detain a suspected triggerman if one was detected.
- Call higher HQ using the 9-line EH spot report
  - ◆ Line 1, Date-Time Group. Complete this line with the date and time the item was discovered.
  - ◆ Line 2, Report Activity and Location. Complete this line with the unit and the 8-digit grid location of the EH.
  - ◆ Line 3, Contact Method. Enter the radio frequency, call sign, point of contact (POC), and telephone number.
  - ◆ Line 4, Type of Ordnance. Document whether it was dropped, projected, placed, or thrown or whether it is a possible IED. Give the number of items, if more than one.

Include as detailed a description of the item in question as possible, including the size, shape, and physical condition.

- ◆ Line 5, Nuclear, Biological, and Chemical (NBC) Contaminations. Be as specific as possible.
- ◆ Line 6, Resources Threatened. Document equipment, facilities, or other assets that were threatened.
- ◆ Line 7, Impact on Mission. Provide a short description of the current tactical situation and how the EH affected the status of the mission.
- ◆ Line 8, Protective Measures. Document any measures being taken to protect personnel and equipment.
- ◆ Line 9, Recommended Priority. Indicate whether it is immediate, indirect, minor, or no threat.
  - Immediate. Stopped the unit maneuver and mission capability or threatens critical assets vital to the mission.
  - Indirect. Stopped the unit maneuver and mission capability or threatens critical assets important to the mission.
  - Minor. Reduced the unit maneuver and mission capability or threatens non-critical assets.
  - No threat. Has little or no effect on the capabilities or assets of the unit.
- Give as much info as possible to include a safe route or approach to the ICP for EOD and other responding agencies.



- Clear all personnel from the area to a minimum safe distance of 300 meters from a potential IED.
- Vary minimum distances (beyond 300 meters) to avoid establishing predictability, because of possible secondary IED.
- Avoid using any communications or electronic equipment (other than CREW devices).
- Use mission, enemy, terrain, weather, troops and support, time available, and civilian considerations (METT-TC) factors.



- Cordon off the area.
- Position CREW devices to best protect the element.
- Direct personnel out of the danger area, allowing entry only to EOD personnel.
- Follow existing ROE procedures to question, search, and detain suspects.

In the event of larger elements personnel who are deemed non-essential for the purpose of cordoning off the area, can either use an alternate route of movement and continue the mission or return to the nearest safe area. Theater specific guidance or mission necessities may require the unit to react to the IED in different manners.

- Direct people out of the 300 meter minimum danger area.
- Check suspicious personnel exiting the cordoned-off area to suppress the enemy within the danger area.
- Identify, clear, and establish an area for an incident control point.
- Establish an ICP for follow-on agencies.
- Focus soldiers outward in cordoned positions and the ICP to provide protection and security against command-initiated IED and VBIEDs.
- Control media reporters and reduce civilian distractions.

When cordoning IEDs, position CREW vehicle(s) between likely triggerman location(s) and friendly forces.

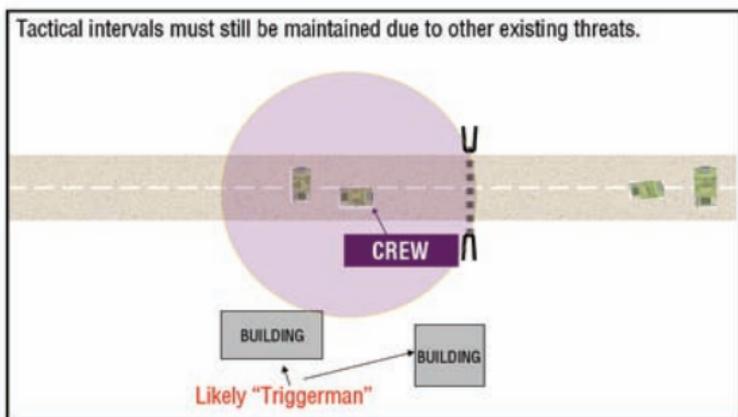


Figure 103 - Cordoning IEDs



- Check the immediate area for secondary devices from the ICP or cordoned positions.
- Conduct 5-meter and 25-meter checks, and 100-meter (if possible) of the area for IED materials, indicators, and equipment that may lead to other IEDs flanking the unit.



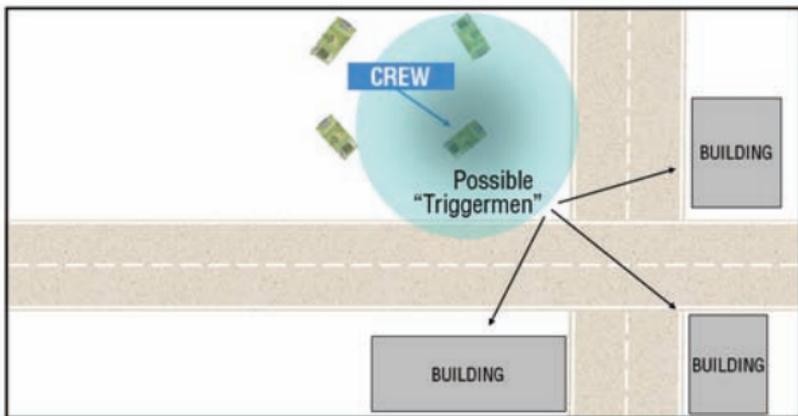
**Figure 104 - Notify higher HQ**



- Control the area inside the cordon to ensure only authorized access.
  - ◆ Allow only authorized emergency vehicles to enter the cordoned area.

- ◆ Ensure all personnel and vehicles enter and exit the cordoned area through the ICP.
- Scan for other enemy indicators such as a cameraman, triggerman, or any other observer.

When establishing a security perimeter, place CREW vehicle(s) to 'cover' likely triggerman locations



**Figure 105 - CREW covering**

**The 5 Cs are Confirm, Clear, Cordon, Check, and Control.**

## 6.3 Post-Convoy Measures

### 6.3.1 Convoy debriefing

#### **ALWAYS REPORT ANY IED ACTIVITY!**



- IED sightings
- IED locations
- Things that seemed out of the ordinary

### 6.3.2 Post-convoy checks

- ◆ Conduct post-convoy PMCS
- ◆ Immediately notify FSR or appropriate personnel of any equipment damage or failure.
- ◆ Ensure CREW equipment is secure.

#### **What you learned in this chapter**

- What you should consider before a convoy
- What is the Convoy Planning Tool
- The CREW employment techniques
- What you should do at an IED site
- What you should do after a convoy

## Additional Sources of Information

The following Web sites can provide more information and assistance in convoy planning and current threat.

- JCREW Web Portal  
<https://ieddefeat.jfcom.smil.mil>  
<http://ieddefeat.jfcom.mil>
- PM CREW and Warlock Training  
[http://arat.army.smil.mil/SEPS\\_WARLOCK](http://arat.army.smil.mil/SEPS_WARLOCK)
- Knowledge and Information Fusion Exchange  
<https://knife.jfcom.smil.mil>
- Convoy Planning Tool (CPT)  
<http://TSC.jeodnet.smil.mil/cpt>
- WARLOCK and CHANNEL Systems Training Site  
<http://tsc.jeodnet.smil.mil/CREW/>
- CFLCC Mine Info Center:  
[http://www.swa.arcent.army.smil.mil/sections/c7/mine\\_infocenter.html](http://www.swa.arcent.army.smil.mil/sections/c7/mine_infocenter.html)
- CJTF-7 Antiterrorism/Force Protection  
[http://148.35.250.12/sections/anti\\_terrorism/atfpweb/index.htm](http://148.35.250.12/sections/anti_terrorism/atfpweb/index.htm)
- Mine & Explosive Ordnance Info Coordination Center (MEOICC)  
<http://148.35.250.12/sections/ENG/meoicc/>
- Countermine & Booby Trap Center  
<http://148.124.179.178/cmcbtc/index.asp>
- Dept of Army – Intelligence Information Services  
<http://dadpm.inscom.army.smil.mil/index.asp>
- Nat'l Ground Intel Center – Energetic Materials  
<http://www.ngic.army.smil.mil/>

**Additional Sources of Information (cont'd)**

- Electronics Attack Weapons School  
[http://eaws.nmci.navy.smil.mil/eaws\\_web/index.htm](http://eaws.nmci.navy.smil.mil/eaws_web/index.htm)
- Combined Explosive Exploitation Cell (CEXC):  
<http://cexc.s-iraq.centcom.smil.mil/>
- HQ Dept of Army IED Task Force  
<http://iedtaskforce.army.smil.mil/>
- Marine Corps Center for Lessons Learned (MCCLL)  
<http://www.mccll.usmc.mil>  
<http://www.mccll.usmc.smil.mil>
- Joint IED Defeat Organization (JIEDDO)  
<http://releasable.portal.inscom.army.smil.mil/jieddo/default.aspx>
- Joint Information Operations Center  
<http://www.jioc.smil.mil/index.cfm?CFID=1022901&CFTOKEN=41801464>
- Navy Lessons Learned  
<http://www.naidc.navy.smil.mil/NLLS/NLLWeb/default/>
- Army Training and Support Command  
<http://www.train.army.mil>

While deployed, you can contact the Joint IED Task Force Field Team in theater for up-to-date developments.

This handbook has been reviewed and released for publication by JIEDDO; questions or requests for distribution should be directed to the Training Officer at 703-601-2392 (DSN: 329-2392), or by email to [training@jieddo.dod.mil](mailto:training@jieddo.dod.mil)

## Acronyms

AC	Alternating Current
AO	Area of Operation
ARAT	Army Reprogramming Analysis Team
BFT	Blue Force Tracker
BIT	Built-In-Test
C2	Command and Control
CB	Circuit Breaker
CEXC	Combined Explosive Exploitation Cell
CPT	Convoy Planning Tool
CREW	Counter RCIED Electronic Warfare
CWIED	Command Wired IED
DCU	Dashboard Control Unit
EA	Electronic Attack
ECM	Electronic Counter Measure
EOD	Explosive Ordnance Disposal
EP	Electronic Protection
ES	Electronic Support
EWO	Electronic Warfare Officer
FBCB2	Force Battle Command, Brigade and Below
FOB	Forward Operating Base
FSR	Field Service Representative
GPS	Global Positioning System
HQ	Headquarters

**FOR OFFICIAL USE ONLY**

**Acronyms (cont'd)**

HZ	Hertz
ICE	IED Countermeasure Equipment
ICP	Incident Control Point
IED	Improvised Explosive Device
JIEDDO	Joint IED Defeat Organization
LED	Light Emitting Diode
LOS	Line Of Sight
LRCT	Long Range Cordless Telephone
MCM	Mobile Countermeasures
METT-TC	Mission, Enemy, Terrain, Troops available, Time, and Civilian considerations
MHz	Megahertz
mICE	Modified IED Countermeasure Equipment
MMBJ	Mobile Multi-Band Jammer
OEF	Operation Enduring Freedom
OIF	Operation Iraqi Freedom
OP	Observation Post
PCC	Pre-Convoy Checks
PCI	Pre-Convoy Inspection
PDA	Personal Digital Assistant
PDU	Power Distribution Unit
PIR	Passive Infrared
PMCS	Preventative Maintenance Checks and Services
PMU	Power Monitor Unit
QRF	Quick Reaction Force

**FOR OFFICIAL USE ONLY**

**Acronyms (cont'd)**

RCIED	Radio Controlled IED
RCU	Remote Control Unit
RF	Radio Frequency
SINGCARS	Single-Channel Ground and Airborne Radio System
SOP	Standard Operating Procedure
SSVJ	Self Screening Vehicle Jammer
TACSAT	Tactical Satellite
TFOM	Time Figure of Merit for GPS receivers
TTP	Tactics, Techniques and Procedures
UDM	User Data Module
UXO	Unexploded Ordnance
VBIED	Vehicle Borne IED
VOIED	Victim Operated IED
VSWR	Voltage Standing Wave Ratio
WIT	Weapons Intelligence Team

## Acknowledgements

The JCREW Quick Reaction Team wishes to acknowledge the following organizations for providing exceptional support to the process of development, printing and distribution of the Joint Counter Radio Controlled Improvised Explosive Device Electronic Warfare (JCREW) Handbook:

- Joint Centers of Excellence (JCOE)
- Department of Defense (DoD)
- Joint IED Defeat Organization (JIEDDO)
- Joint Test and Evaluation (JT&E)
- Naval Explosive Ordnance Disposal Technology Division (NAVEODTECHDIV)
- Program Manager Signals Warfare (PM SW)
- Systems Documentation, Inc. (SDI)
- SENTEL Corporation
- Communications Electronics Command (CECOM) Software Engineering Center (SEC)
- Joint Forces Command (JFCOM)
- PEO-LMW PMS-408
- OPNAV N85
- Joint CREW Composite Squadron 1 (JCCS-1)
- Multinational Force 1 (MNF-1)
- Task Force Troy
- Task Force Paladin
- Camp Victory
- Training and Doctrine Command (TRADOC)
- United States Army Intelligence Center (USAIC)
- Marine Corps Center for Lessons Learned
- United States Central Command (CENCOM)
- Fort Irwin
- Fort Huachuca

**FOR OFFICIAL USE ONLY**

**Acknowledgements (cont'd)**

- Fort Monmouth
- Fort Leavenworth, Electronic Warfare Division
- Army HQDA G3 Electronic Warfare Division

## Table of Figures

Figure 1 - Components of Electronic Warfare .....	2
Figure 2 - Typical Communication.....	3
Figure 3 - Jamming Simplified.....	4
Figure 4 - CREW Jamming.....	5
Figure 5 - Line-Of-Sight.....	6
Figure 6 - Stand-Off Vehicle Jammer in Urban Area.....	7
Figure 7 - Antenna Coverage Comparison .....	8
Figure 8 - Transmission Power.....	10
Figure 9 - Command Wire Detonator.....	15
Figure 10 - Vehicle Borne Detonator .....	15
Figure 11 - Radio controlled detonation.....	16
Figure 12 - High & Low Power Devices .....	17
Figure 13 - Masked Devices.....	18
Figure 14 - Baited Attack.....	19
Figure 15 - Attack using OP.....	20
Figure 16 - Broken Down Vehicle Attack.....	20
Figure 17 - Typical Attack.....	21
Figure 18 - EW Process Flow .....	23
Figure 19 - Acorn Device.....	45
Figure 20 - Acorn with Remote Switch .....	46
Figure 21 - Acorn without Remote Switch .....	47
Figure 22 - Remote Switch.....	47
Figure 23 - Beech Device.....	49
Figure 24 - Beech Controls & Indicators.....	50
Figure 25 - Blue Device .....	52
Figure 26 - Blue Controls & Indicators.....	53
Figure 27 - Proper cable alignment.....	55

**FOR OFFICIAL USE ONLY**

**Table of Figures (cont'd)**

Figure 28 - Cloning.....	56
Figure 29 - Zeroizing.....	57
Figure 30 - Mobile Countermeasures (MCM) Unit..	58
Figure 31 - Remote Control Unit (RCU) .....	59
Figure 32 - Master MCM Switch .....	60
Figure 33 - Remote Screen .....	61
Figure 34 - Jammer is ON.....	62
Figure 35 - Jammer status is OFF.....	63
Figure 36 - ECM Fault Screens .....	64
Figure 37 - Lost ECM Fault Screen.....	65
Figure 38 - System jamming OK.....	66
Figure 39 - Fault but still jamming .....	67
Figure 40 - Fault and not jamming .....	67
Figure 41 - Master ON/OFF.....	68
Figure 42 - Rear Panel.....	68
Figure 43 - Erase using RCU.....	70
Figure 44 - MCM Erase Button .....	70
Figure 45 - Cottonwood Device .....	71
Figure 46 - User Front Panel .....	72
Figure 47 - Remote Control.....	73
Figure 48 - Battery Box.....	74
Figure 49 - PDU Connections & Breakers.....	75
Figure 50 - Power Monitor Unit (PMU) .....	76
Figure 51 - Unclassified Shutdown.....	79
Figure 52 - Duke Device.....	81
Figure 53 - Duke Primary Unit Controls & Indicators.....	82
Figure 54 - Duke Remote Control Unit Controls & Indicators.....	85
Figure 55 - Guardian D (QRD) System .....	95

**Table of Figures (cont'd)**

Figure 56 - Assault Pack .....	96
Figure 57 - Typical Guardian Device (with battery pack) .....	96
Figure 58 - Guardian Controls & Indicators .....	97
Figure 59 - BB/UBI2590 Battery .....	98
Figure 60 - Green Device .....	102
Figure 61 - Green Controls & Indicators .....	103
Figure 62 - Floating Star indication .....	103
Figure 63 - Traveling Star indication .....	104
Figure 64 - Green Force Jam Mode .....	106
Figure 65 - Hunter Remote Control Unit .....	109
Figure 66 - Ironwood Device .....	113
Figure 67 - Front Panel .....	114
Figure 68 - Ironwood Remote Control .....	114
Figure 69 - Low and High Band subsystem circuit breaker .....	116
Figure 70 - mICE Device .....	119
Figure 71 - mICE Controls & Indicators .....	120
Figure 72 - MMBJ Device .....	122
Figure 73 - MMBJ Controls & Indicators .....	123
Figure 74 - Pecan Device .....	125
Figure 75 - Pecan Controls & Indicators .....	126
Figure 76 - Red Device .....	129
Figure 77 - Red Controls & Indicators .....	130
Figure 78 - Red / Green Combo .....	132
Figure 79 - Red / Green Combo Cabling .....	133
Figure 80 - Spruce Devices .....	134
Figure 81 - Spruce Chassis .....	135
Figure 82 - SSVJ Device .....	138
Figure 83 - SSVJ Components .....	139

**Table of Figures (cont'd)**

Figure 84 - DCU Controls & Indicators.....139

Figure 85 - Warlock LX Device .....141

Figure 86 - LX Front Panel Controls & Indicators  
.....142

Figure 87 - LX Remote Control.....142

Figure 88 - LOW-Q subsystem circuit breaker.....144

Figure 89 - LX Zeroize Buttons.....147

Figure 90 - Zeroize from laptop.....148

Figure 91 - Interoperability .....150

Figure 92 - Convoy Planning Tool.....156

Figure 93 - Short Halt scan.....158

Figure 94 - Long Halt scan.....159

Figure 95 - Approaching likely attack spots.....160

Figure 96 - Masking in an urban area.....160

Figure 97 - Covering likely attack spots.....161

Figure 98 - Single vehicle jamming.....162

Figure 99 - Two vehicles, two jammers.....162

Figure 100 - Multiple vehicles, single jammer .....163

Figure 101 - Multiple vehicles, multiple jammers in  
urban area .....163

Figure 102 - Multiple vehicles, single jammer in  
urban area .....164

Figure 103 - Cordoning IEDs.....169

Figure 104 - Notify higher HQ.....170

Figure 105 - CREW covering.....171



**FOR GUIDANCE ONLY!  
ALWAYS CHECK WITH S-2 OR S-6 WHEN USING  
MULTIPLE SYSTEMS**

**CREW Systems Interoperability**

	Duke	Green	Red/Green	Ironwood	LX	Cottonwood	Red	SSVJ	MMBJ	mICE	Acorn	Chameleon	Hunter	Blue	Guardian
Duke	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green
Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green
Red/Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green
Ironwood	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green
LX	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green
Cottonwood	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green
Red	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green
SSVJ	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green
MMBJ	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green
mICE	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green
Acorn	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green
Chameleon	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green
Hunter	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green
Blue	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green
Guardian	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green

- **YELLOW** boxes indicate systems that require separation to avoid interference. See S-2 or S-6 for further information.
- **GREEN** boxes represent no known interference.

**FOR OFFICIAL USE ONLY**

# Resource Phone Directory

FSR Baghdad (Victory)	DSN 318-992-2988
FSR Balad (Anaconda)	DSN 318-992-0562 x8038
FSR Tikrit (Speicher)	DSN 318-242-1721
FSR Mosul (Marez)	DSN 318-987-6966 x5801
FSR MEF (Fallujah)	DSN 318-340-1418
FSR Fielding Operations Office (Victory)	DSN 318-822-2774
PM CREW Office (Ft. Monmouth)	DSN 312-992-2988
Joint CREW Field Operations Officer (Paladin)	DSN 318-231-3010
KnIFE 24 Hour Watch	DSN 312-668-0777

**FOR OFFICIAL USE ONLY**