

Report Date: 23 Nov 2016  
Summary Report for Staff Drill Task  
Drill Number: 71-DIV-D5900  
Drill Title: React to Cyber Attack (Battalion through Corps)  
Status: Approved  
Status Date: 13 Nov 2014

---

**Distribution Restriction:** Approved for public release; distribution is unlimited.

**Destruction Notice:** None

**Foreign Disclosure: FD3** - This training product has been reviewed by the developers in coordination with the Fort Leavenworth foreign disclosure officer. This training product cannot be used to instruct international military students.

**Drill Data**

**Proponent:** 71 - Combined Arms (Collective)

**Drill Type:** Staff

**Approved:** 13 Nov 2014

**Obsolete:**

**Restricted Read:** No

**Route To TMD Reviewer:** Yes

**TMD Concurrence:** Yes

**TMD Comments:** Concur

**Safety Level:** Low

**Conditions:**

The command reacts to a cyber attack initiated as a drill under guidance from the Commander. The command establishes communications with higher, lower, and adjacent units, and the mission command system is operating and processing information. The commander issues guidance on coordinating cyber electromagnetic activities. Perform some iterations of this drill during limited visibility and in mission oriented protective posture 4. Some iterations of this task should be performed in MOPP 4.

**Standards:**

The command, in coordination with the Cyber Electromagnetic Activities element, detects the cyber attack and immediately imposes unit standard operating procedures. The command coordinates cyber electromagnetic activities in order to seize, retain, and exploit advantages over threat attacks in both cyberspace and across the electromagnetic spectrum while simultaneously denying and degrading the threats use of the same. The staff coordinates electronic warfare activities to protect the mission command system and ensures continual access to the cyber electromagnetic spectrum. The staff follows commanders intent and meets all cyber attack timelines established by unit standard operating procedures.

**Drill Statements:**

**WARNING**

Follow unit SOP and local policies.

**Safety:** In a training environment, leaders must perform a risk assessment in accordance with ATP 5-19, Risk Management. Leaders will complete the current Deliberate Risk Assessment Worksheet in accordance with the TRADOC Safety Officer during the planning and completion of each task and sub-task by assessing mission, enemy, terrain and weather, troops and support available-time available and civil considerations, (METT-TC). Note: During MOPP training, leaders must ensure personnel are monitored for potential heat injury. Local policies and procedures must be followed during times of increased heat category in order to avoid heat related injury. Consider the MOPP work/rest cycles and water replacement guidelines IAW FM 3-11.4, Multiservice Tactics,

Techniques, and Procedures for Nuclear, Biological, and Chemical (NBC) Protection, FM 3-11.5, Multiservice Tactics, Techniques, and Procedures for Chemical, Biological, Radiological, and Nuclear Decontamination.

**Environment:** Environmental protection is not just the law but the right thing to do. It is a continual process and starts with deliberate planning. Always be alert to ways to protect our environment during training and missions. In doing so, you will contribute to the sustainment of our training resources while protecting people and the environment from harmful effects. Refer to the current Environmental Considerations manual and the current GTA Environmental-related Risk Assessment card. Follow unit SOP and local policies and regulations.

**Cue:** The command reacts to a cyber attack.

**Coaching Point:** a. Ensure SOP is current and be prepared to revise as necessary.  
b. Continue to exercise this drill until the entire staff has mastered it.

## TASK STEPS

1. The staff responds to cyber attack in order to keep cyber disruption and destruction at less than 60% at any given time (IAW FM 6-02.53, 11.8, 5 August 2009) by:

- a. Deconflicting cyber electromagnetic activities (CEMA) mission spectrum requirements with the unit spectrum manager.
- b. Confirming that electronic warfare (EW) systems are operating without interference.
- c. Determining whether EW system emission security experiences compromise, degradation, delay, or modified operations.
- d. Evaluating EW-related interference issues.
- e. Coordinating EW-related frequency interference issues.
- f. Resolving EW-related frequency interference issues.
- g. Identifying improper maintenance of emission security.
- h. Responding to new threats through reprogramming of systems.
- i. Employing appropriate measures against friendly or enemy EW system interference.
- j. Identifying friendly vulnerabilities in the area of operations (AO) exploited by enemy actions.
- k. Identifying percent of emitters in the AO exploited by the enemy.
- l. Determining percent of friendly operations conducted in a restrictive emission control environment.
- m. Determining percent improvement of emission control procedures from previous assessments.
- n. Determining percent of successful EW system reprogramming events.
- o. Determining percent of friendly systems affected by friendly EW systems.
- p. Determining percent of friendly systems affected by enemy EW systems.
- q. Identifying the number of frequency interference issues.
- r. Identifying the number of EW systems operating on assigned frequencies.
- s. Identifying the number of EW systems detected by enemy sensors.
- t. Identifying the number of emission security violations in the AO in a given time.
- u. Identifying the number of EW system reprogramming events.
- v. Identifying the number of instances when EW system reprogramming failed.
- w. Identifying the number of systems affected by friendly or enemy EW systems.

2. The staff defeats EW attacks and ensures friendly domination of the cyber electromagnetic spectrum by:

a. Employing electronic support (ES) in the form of combat information, to provide real-time information to locate and identify adversary command and control (C2) nodes and supporting/supported early warning and offensive systems during EW attack.

b. Employing electronic attack (EA) for jamming and electromagnetic deception or destruction of adversary C2 nodes with directed-energy weapons or anti-radiation missiles.

c. Employing electronic protection, (EP), communications security (COMSEC), and transmission security (TRANSEC) in accordance with standard operating procedures.

d. Installing terrestrial line of sight (LOS) communications parallel to the forward line of troops (FLOT).

e. Employing alternate means of communications before enemy engagements.

f. Employing and reserving primary communication systems for adversary engagements.

g. Transmitting false messages and orders on communications routes experiencing interference.

3. The staff, using ES, EA, EP, and the full range of mission command electromagnetic systems capabilities, enables continual, effective communications throughout operations.

4. The staff complies with all higher headquarters' regulations and guidelines for conducting cyber threat activities.

5. The staff briefs the commander on cyber threat activities and events.

6. The staff provides cyber threat reports and summaries.

(Asterisks indicates a leader performance step.)

### **TASK MEASURES**

1. The staff responded to cyber attack in order to keep cyber disruption and destruction at less than 60% at any given time.
  2. The staff defeated EW attacks and ensured friendly domination of the cyber electromagnetic spectrum.
  3. The staff, using ES, EA, EP, and the full range of mission command electromagnetic systems capabilities, enabled continual, effective communications throughout operations.
  4. The staff complied with all higher headquarters' regulations and guidelines for conducting cyber threat activities.
  5. The staff briefed the commander on cyber threat activities and events.
  6. The staff provided cyber threat reports and summaries.
-

**Talk:**

**a.Orientation:** The object of this drill is to react to a cyber attack.

**b.Safety:** Following the SOP ensures the most efficient response to a cyber attack to limit friendly casualties and protect essential systems.

**c.Demonstration:** Conduct a staff rehearsal of concept (ROC) drill.

**d.Explanation:** Refer to performance measures and explain what each staff member must do to react to a cyber attack.

**e.Unit Instructions:** The staff is coordinating current operations and reacts to a cyber attack.

---

**Walk:**

1. Continue to rehearse to facilitate flow of information and decision-making.
  2. Update SOP as required.
- 

**Run:**

**a.Run-Through Instructions:** The staff should rehearse this drill until they can perform the drill according to the standard and without the drill book or coaching from the leader.

**b.Coaching Point:** a. Ensure SOP is current and be prepared to revise as necessary.

b. Continue to exercise this drill until the entire staff has mastered it.

**c.Performance Instructions:** When the staff can perform this drill according to the standards, the leader should evaluate them and conduct an after action review. The staff should update the SOP as required.

### Equipment (LIN)

Step ID	LIN	Nomenclature	Qty
	FA9530	Tactical Operations Center	1

### Materiel Items (NSN)

Step ID	NSN	LIN	Title	Qty
No materiel items specified				

### Support Personnel

Personnel Type	Description	School	Qty	Remarks
No support personnel specified				

### TADSS

Step ID	TADSS ID	Title	Product Type	Qty
No TADSS specified				

### Supporting Individual Tasks

Step ID	Task ID	Status	Task Title
	113-322-7017	Approved	Develop a Cyber Network Plan
	113-395-0001	Approved	Implement Performance Control Measures for a Cyberspace Network
	150-029-0007	Approved	Produce Electronic Warfare Products in Support of the Military Decision Making Process (MDMP)
	150-290-0015	Approved	Manage Cyber Electromagnetic (CEM) Working Group Outputs
	150-MC-5901	Approved	React to Cyber Attack (Battalion through Corps)

### Prerequisite Individual Tasks

Step ID	Task ID	Status	Task Title
	113-367-5000	Approved	React To Electromagnetic Spectrum Interference
	113-573-6000	Approved	React to an Electronic Attack (EA)

### Supporting Collective Tasks

Step ID	Task ID	Status	Title
	71-8-3501	Approved	Coordinate Electronic Warfare (Brigade - Corps)
	71-8-3502	Approved	Assess Electronic Warfare Operations (Brigade - Corps)
	71-9-5640	Approved	Conduct Electronic Warfare in the Joint Operations Environment(Division Echelon and Above [Operational])

### Prerequisite Collective Tasks

Step ID	Task ID	Status	Title
	71-8-5900	Approved	Coordinate Cyber Electromagnetic Activities (Brigade - Corps)

### Supporting Drill Tasks

Step ID	Drill ID	Status	Drill Title
No supporting drill tasks specified			

**OPFOR**

<b>Task Number</b>	<b>Title</b>	<b>Status</b>
No supporting OPFOR tasks specified		

**REFERENCES**

<b>Step Number</b>	<b>Reference ID</b>	<b>Reference Name</b>	<b>Required</b>	<b>Primary</b>
	ATP 2-01.3	Intelligence Preparation of the Battlefield/Battlespace (Including change 1)	Yes	No
	ATP 6-02.53	Techniques for Tactical Radio Operations	Yes	Yes
	FM 3-36	Electronic Warfare in Operations	Yes	No
	JP 3-13.1	Joint Doctrine for Command and Control Warfare (C2W)	Yes	No

## Training Setup

- a. Table(s) of organization and equipment (TOE) assigned personnel and equipment, weapons, vehicles, and communications equipment/mission command systems.
- b. All appropriate software and IT infrastructure.

## Training Facilities

Facility ID	Facility Name	Facility Type
14113	Access Control Facility	F14113-Access Control Facilities

## DODIC

DODIC	Name	Qty
No DODIC		

## Associated Documents

Media ID	Media Type	Title	Subtitle
No Associated Documents			

## GLOSSARY TERMS

Glossary Term	Definition
No glossary terms specified	

## ACRONYMS AND ABBREVIATIONS

Acronym/Abbreviation	Definition
No acronyms/abbreviations specified	