

Training and Evaluation Outline Report

Status: Approved

25 Mar 2015

Effective Date: 30 Sep 2016

Task Number: 71-8-5900

Task Title: Coordinate Cyber Electromagnetic Activities (Brigade - Corps)

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

Destruction Notice: None

Foreign Disclosure: FD1 - This training product has been reviewed by the training developers in coordination with the Fort Leavenworth foreign disclosure officer. This training product can be used to instruct international military students from all approved countries without restrictions.

Supporting Reference(s):

Step Number	Reference ID	Reference Name	Required	Primary
	Cyber Bulletin 16-13	Cyberspace Operations: Observations; Lessons; and Tactics, Techniques, and Procedures Cyber Bulletin No. 2	Yes	No
	FM 3-36	Electronic Warfare in Operations	Yes	No
	FM 3-38	CYBER ELECTROMAGNETIC ACTIVITIES http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/fm3_38.pdf	Yes	Yes
	JP 3-13.1	Electronic Warfare	Yes	No

Conditions: The command receives a mission order from higher headquarters and the commander issues guidance on coordinating cyber electromagnetic activities. The command establishes communications with subordinate and adjacent units, and higher headquarters. The mission command system is operational and processing information. Some iterations of this task should be performed in MOPP 4.

Standards: The staff, in coordination with the Cyber Electromagnetic Activities element, coordinates cyber electromagnetic activities in order to seize, retain, and exploit advantages over threats in both cyberspace and across the electromagnetic spectrum while simultaneously denying and degrading the threats use of the same. The staff coordinates cyber electromagnetic in accordance with the commanders intent, orders from higher headquarters, and standard operating procedures.

Live Fire Required: No

Objective Task Evaluation Criteria Matrix:

Plan and Prepare		Execute						Assess	
Operational Environment	Training Environment (L/V/C)	Training/Authorized	% of Leaders Present at	% of Soldiers Present at	External Eval	% Performance Measures 'GO'	% Critical Performance Measures 'GO'	% Leader Performance Measures 'GO'	Task Assessment
BDE & Above									
Dynamic and Complex (All OE Variables and Hybrid Threat)	Night	IAW unit CATS statement.	>=85%	>=80%	Yes	>=91%	All	>=90%	T
			75-84%			80-90%		80-89%	T-
Dynamic and Complex (All OE Variables and Single Threat)	Day		65-74%	75-79%	No	65-79%	<All	<=79%	P
			60-64%	60-74%		51-64%			P-
Dynamic and Complex (<All OE Variables and Single Threat)			<=59%	<=59%	<=50%	U			

Remarks: None

Notes:

Safety Risk: Low

Task Statements

Cue: None

DANGER

Leaders have an inherent responsibility to conduct Risk Management to ensure the safety of all Soldiers and promote mission accomplishment.

WARNING

Risk Management is the Army's primary decision-making process to identify hazards, reduce risk, and prevent both accidental and tactical loss. All Soldiers have the responsibility to learn and understand the risks associated with this task.

CAUTION

Identifying hazards and controlling risks across the full spectrum of Army functions, operations, and activities is the responsibility of all Soldiers.

Performance Steps and Measures

NOTE: Assess task proficiency using the task evaluation criteria matrix.

NOTE: Asterisks (*) indicate leader steps; plus signs (+) indicate critical steps.

STEP/MEASURE	GO	NO-GO	N/A
1. The staff coordinates cyber electromagnetic activities (CEMA) through the operations process in support of the commander's visualization, to include:	N/A	N/A	N/A
a. Cyberspace Operations.	N/A	N/A	N/A
b. Electronic Warfare (EW).	N/A	N/A	N/A
c. Spectrum Management Operations.	N/A	N/A	N/A
2. The staff coordinates CEMA in support of the overall plan.	N/A	N/A	N/A
a. Integrates CEMA with information-related capabilities to accomplish the desired objectives.	N/A	N/A	N/A
b. Determines how CEMA creates the desired effects in the unit's area of operations.	N/A	N/A	N/A
c. Identifies organic and external CEMA requirements and capabilities.	N/A	N/A	N/A
d. Determines the legal and policy compliance constraints based on higher headquarters guidance.	N/A	N/A	N/A
e. Integrates offensive and defensive CEMA capabilities with the commander's stated guidance and the unit's concept of operation.	N/A	N/A	N/A
f. Integrates CEMA, electronic warfare (EW), and electromagnetic spectrum (EMS) management with one another and the unit's other warfighting functions.	N/A	N/A	N/A
g. Coordinates to facilitate CEMA internally with subordinate units, as well as externally with supported, supporting, and adjacent units that own and/or control cyber electromagnetic resources.	N/A	N/A	N/A
3. The staff coordinates cyberspace operations.	N/A	N/A	N/A
a. Offensive cyberspace operations.	N/A	N/A	N/A
b. Defensive cyberspace operations.	N/A	N/A	N/A
c. Department of Defense information operations.	N/A	N/A	N/A
4. The staff coordinates EW operations.	N/A	N/A	N/A
a. Electronic attack.	N/A	N/A	N/A
b. Electronic protection.	N/A	N/A	N/A
c. Electronic warfare support.	N/A	N/A	N/A
5. The staff coordinates Spectrum Management Operations by managing:	N/A	N/A	N/A
a. Spectrum management.	N/A	N/A	N/A
b. Frequency assignment.	N/A	N/A	N/A
c. Host-nation coordination.	N/A	N/A	N/A
6. Integrate policy that enable the planning, management, and execution of operations within the electromagnetic operational environment.	N/A	N/A	N/A

TASK PERFORMANCE / EVALUATION SUMMARY BLOCK							
ITERATION	1	2	3	4	5	M	TOTAL
TOTAL PERFORMANCE MEASURES EVALUATED							
TOTAL PERFORMANCE MEASURES GO							
TRAINING STATUS GO/NO-GO							

ITERATION: 1 2 3 4 5 M

COMMANDER/LEADER ASSESSMENT: T P U

Mission(s) supported: None

MOPP 4: Sometimes

MOPP 4 Statement: None

NVG: Never

NVG Statement: None

Prerequisite Collective Task(s):

Step Number	Task Number	Title	Proponent	Status
	71-8-5111	Conduct the Military Decisionmaking Process (Battalion - Corps)	71 - Combined Arms (Collective)	Approved
	71-8-5144	Develop Running Estimates (Battalion - Corps)	71 - Combined Arms (Collective)	Approved

Supporting Collective Task(s):

Step Number	Task Number	Title	Proponent	Status
	71-8-3502	Assess Electronic Warfare Operations (Brigade - Corps)	71 - Combined Arms (Collective)	Approved
	71-8-6320	Perform Computer Network Defense (Brigade - Corps)	71 - Combined Arms (Collective)	Approved
	71-8-7655	Apply Knowledge Networks (Brigade - Corps)	71 - Combined Arms (Collective)	Approved

OPFOR Task(s): None

Supporting Individual Task(s):

Step Number	Task Number	Title	Proponent	Status
	011-420-0031	Implement Operations in an Electronic Warfare Environment	011 - Aviation (Individual)	Approved
	093-948-B120	Supervise Maintenance of Computer Networks and Associated Equipment	093 - Munitions and Electronics Maintenance (Individual)	Approved
	113-367-5001	Implement Network Protection Measures	113 - Signal (Individual)	Approved
	113-616-2018	Conduct Electronic Counter-Countermeasures (ECCM) Network Controller (ENC) Operations within the Defense Satellite Communications System (DSCS)	113 - Signal (Individual)	Approved
	113-642-6002	Plan for Electronic Warfare (EW) Measures	113 - Signal (Individual)	Approved
	150-029-5001	Report Electromagnetic Spectrum Interference	150 - Combined Arms (Individual)	Approved
	150-MC-2300	Perform Information Collection	150 - Combined Arms (Individual)	Approved
	150-MC-5118	Prepare an Annex	150 - Combined Arms (Individual)	Approved
	150-MC-5125	Prepare a Fragmentary Order	150 - Combined Arms (Individual)	Approved
	150-MC-5250	Employ a Mission Command Information System	150 - Combined Arms (Individual)	Approved
	150-MC-5315	Establish the Common Operational Picture	150 - Combined Arms (Individual)	Approved
	150-MC-5901	React to Cyber Attack (Battalion through Corps)	150 - Combined Arms (Individual)	Approved
	301-35Q-1100	Analyze a Computer System Architecture	301 - Intelligence (Individual)	Approved
	301-35Q-1101	Analyze a Computer Network Architecture	301 - Intelligence (Individual)	Approved
	301-35Q-1102	Produce an Assessment of a Target Network Security Posture	301 - Intelligence (Individual)	Approved
	301-35Q-1103	Determine an Exploitation Method	301 - Intelligence (Individual)	Approved
	301-35Q-1104	Analyze Digital Forensics Data	301 - Intelligence (Individual)	Approved
	301-35Q-1105	Perform Basic Analysis of Suspicious Software	301 - Intelligence (Individual)	Approved
	301-35Q-2100	Develop a Cryptologic Network Warfare Capability Requirement	301 - Intelligence (Individual)	Approved
	301-35Q-2101	Perform Intermediate Analysis of Suspicious Software	301 - Intelligence (Individual)	Approved
	301-35Q-2102	Validate an Assessment of a Target Network Security Posture	301 - Intelligence (Individual)	Approved
	301-35Q-2103	Collect Digital Forensics Data	301 - Intelligence (Individual)	Approved
	301-35Q-3100	Validate Architectural Analysis	301 - Intelligence (Individual)	Approved
	301-35Q-3101	Implement an Exploitation Method	301 - Intelligence (Individual)	Approved
	301-35Q-3102	Perform Cryptologic Network Warfare Mission Management Functions	301 - Intelligence (Individual)	Approved
	301-35Q-3103	Direct Digital Forensics Processes	301 - Intelligence (Individual)	Approved
	301-35Q-3104	Draft a Cryptologic Network Warfare Plan	301 - Intelligence (Individual)	Approved
	301-35Q-4100	Direct an Exploitation Operation	301 - Intelligence (Individual)	Approved
	301-35Q-4101	Direct a Cryptologic Network Warfare Operation	301 - Intelligence (Individual)	Approved
	301-35Q-4102	Develop a Cryptologic Network Warfare Technical Training Strategy	301 - Intelligence (Individual)	Approved

Supporting Drill(s): None

Supported AUTL/UJTL Task(s):

Task ID	Title
ART 5.9.3.4	Monitor Spectrum Management Policy Adherence
ART 5.9.3.3	Perform Host-Nation Electromagnetic Coordination
ART 5.9.3.2	Perform Frequency Assignment
ART 5.9.3.1	Perform Spectrum Management
ART 5.9.3	Conduct Electromagnetic Spectrum Operations
ART 5.9.2	Conduct Electronic Warfare
ART 5.9	Conduct Cyber Electromagnetic Activities
ART 5.9.1	Conduct Cyberspace Operations
ART 5.9.1.1 INVALID	INVALID - Conduct Cyber Warfare
ART 5.9.1.2 INVALID	INVALID - Conduct Cyber Network Operations
ART 5.9.1.4	CONDUCT CYBERSPACE SUPPORT
ART 5.9.1.5	DEVELOP CYBERSPACE SITUATIONAL AWARENESS

TADSS

TADSS ID	Title	Product Type	Quantity
No TADSS specified			

Equipment (LIN)

LIN	Nomenclature	Qty
No equipment specified		

Materiel Items (NSN)

NSN	LIN	Title	Qty
No materiel items specified			

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. .

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. .