

# Training and Evaluation Outline Report

**Status: Approved**

**15 Jan 2015**

**Effective Date: 30 Sep 2016**

**Task Number:** 71-9-5650

**Task Title:** Conduct Computer Network Operations (Division Echelon and Above [Operational])

**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
	JP 3-13	Information Operations	Yes	No
	JP 3-31	Command and Control for Joint Land Operations	Yes	No
	JP 6-0	Joint Communications System	Yes	Yes

**Conditions:** The command is conducting operations as a Joint Task Force (JTF) or as a Combined Joint Task Force (CJTF) headquarters. The command's headquarters receives liaison, unit, and individual augmentees. The command receives an operations order from higher headquarters. The commander issues guidance on conducting computer network operations. The command establishes communications with subordinate and adjacent units and higher headquarters. The mission command system is operational and processing information. This task should not be trained in MOPP 4.

**Standards:** The staff conducts computer network operations to attack, deceive, degrade, disrupt, deny, exploit, and defend electronic information and infrastructure 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%	<b>T</b>
			75-84%			80-90%		80-89%	<b>T-</b>
Dynamic and Complex (All OE Variables and Single Threat)	Day		65-74%	75-79%	No	65-79%	<All	<=79%	<b>P</b>
			60-64%	60-74%		51-64%			<b>P-</b>
Dynamic and Complex (<All OE Variables and Single Threat)			<=59%	<=59%	<=50%	<b>U</b>			

**Remarks:** None

**Notes:** None

**Safety Risk:** Low

**Task Statements**

**Cue:** None

**DANGER**

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

## **WARNING**

Composite 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 plans computer network operations to control the information environment and infrastructure by:	N/A	N/A	N/A
a. Reviewing theater-level computer network operations guidance.	N/A	N/A	N/A
b. Integrating computer network operations into operational planning.	N/A	N/A	N/A
c. Conducting a computer network threat assessment.	N/A	N/A	N/A
d. Providing intelligence support to computer network operations.	N/A	N/A	N/A
e. Developing rules of engagement for computer network operations.	N/A	N/A	N/A
f. Distributing rules of engagement.	N/A	N/A	N/A
g. Coordinating computer network operations plans with other capabilities to ensure unity of effort.	N/A	N/A	N/A
h. Coordinate operational-level CNO plans with other IO core, supporting, and related capabilities along with other operations to ensure unity of effort.	N/A	N/A	N/A
i. Establishing target sets for computer network operations.	N/A	N/A	N/A
j. Developing measures of performance and effectiveness to assess the computer network operations effects.	N/A	N/A	N/A
k. Determining any collateral effects of computer network operations.	N/A	N/A	N/A
l. Confirming computer network operations create desired effects on the identified targets.	N/A	N/A	N/A
m. Identifying computer network operations capabilities.	N/A	N/A	N/A
n. Verifying availability of identified capabilities.	N/A	N/A	N/A
o. Requesting support for identified computer network operations capability gaps.	N/A	N/A	N/A
p. Identifying computer network operations battle damage assessment criteria.	N/A	N/A	N/A
q. Integrating multinational forces into computer network operations in accordance with foreign disclosure policies.	N/A	N/A	N/A
r. Coordinating computer network operations with unified action partners.	N/A	N/A	N/A
+ 2. The commander directs actions to disrupt, deny, degrade, or destroy threat computer networks by:			
a. Identifying the objectives and desired effects to achieve with computer network attack.	N/A	N/A	N/A
b. Establishing measures of effectiveness and performance to assess computer network attack operations.	N/A	N/A	N/A
c. Developing collateral damage mitigation measures.	N/A	N/A	N/A
d. Implementing collateral damage mitigation measures, as appropriate.	N/A	N/A	N/A
e. Integrating computer network attack operations into the joint targeting process.	N/A	N/A	N/A
f. Coordinating computer network attack operations with other lethal and non-lethal fires.	N/A	N/A	N/A
g. Confirming computer network attack actions create desired effects on threat targets.	N/A	N/A	N/A
h. Verifying that proper authorities conduct computer network attack operations.	N/A	N/A	N/A
i. Coordinating computer network attack actions with exploitation and defense operations.	N/A	N/A	N/A
3. The staff coordinates actions to protect, monitor, analyze, detect, and respond to unauthorized activity within Department of Defense information systems and computer networks by:	N/A	N/A	N/A
a. Planning computer network defense operations to secure friendly information and information systems.	N/A	N/A	N/A
b. Assessing threat computer network operations capabilities.	N/A	N/A	N/A
c. Establishing incident handling and reporting procedures.	N/A	N/A	N/A
d. Monitoring information systems to detect intrusions and disruptions of service.	N/A	N/A	N/A
e. Responding to intrusions and disruptions of service.	N/A	N/A	N/A
f. Analyzing information system vulnerabilities to eliminate or reduce threat attack effects.	N/A	N/A	N/A
g. Employing communications, intelligence, counterintelligence, and law enforcement capabilities to defend information and computer networks.	N/A	N/A	N/A
h. Developing a continuity of operations plan with priorities for restoration of information systems.	N/A	N/A	N/A
4. The staff organizes operations and intelligence collection capabilities to collect data from threat information systems or networks by:	N/A	N/A	N/A
a. Integrating computer network exploitation operations into joint operations planning.	N/A	N/A	N/A
b. Providing intelligence resources for computer network exploitation operations.	N/A	N/A	N/A
c. Assessing the collateral effects of computer network exploitation operations.	N/A	N/A	N/A
d. Verifying that proper authorities conduct computer network exploitation operations.	N/A	N/A	N/A
e. Coordinating computer network exploitation operations to support computer network attack and defense.	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:** Never

**MOPP 4 Statement:** None

**NVG:** Never

**NVG Statement:** None

**Prerequisite Collective Task(s):**

Step Number	Task Number	Title	Proponent	Status
	71-9-5200	Assess the Operational Situation	71 - Combined Arms (Collective)	Approved
	71-9-5300	Prepare Plans (Division Echelon and Above [Operational])	71 - Combined Arms (Collective)	Approved
	71-9-5400	Control Subordinate Operational Forces (Division Echelon and Above [Operational])	71 - Combined Arms (Collective)	Approved
	71-9-6500	Provide Security for Operational Forces (Division Echelon and Above [Operational])	71 - Combined Arms (Collective)	Approved

**Supporting Collective Task(s):**

Step Number	Task Number	Title	Proponent	Status
	71-TA-5310	Conduct Operational Mission Analysis for Theater Army	71 - Combined Arms (Collective)	Approved

**OPFOR Task(s):** None

**Supporting Individual Task(s):**

Step Number	Task Number	Title	Proponent	Status
	150-LDR-5003	Use the Mission Order Technique	150 - Combined Arms (Individual)	Approved
	150-MC-2300	Perform Information Collection	150 - Combined Arms (Individual)	Approved
	150-MC-5111	Conduct the Military Decisionmaking Process	150 - Combined Arms (Individual)	Approved
	150-MC-5144	Develop a Running Estimate	150 - Combined Arms (Individual)	Approved
	150-MC-5145	Conduct Risk Management	150 - Combined Arms (Individual)	Approved
	150-MC-5200	Conduct Command Post Operations	150 - Combined Arms (Individual)	Approved

**Supporting Drill(s):** None

**Supported AUTL/UJTL Task(s):**

Task ID	Title
OP 5.6.5	Conduct Computer Network Operations

## 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. 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 FM 3-34.5 Environmental Considerations and GTA 05-08-002 ENVIRONMENTAL-RELATED RISK ASSESSMENT.

**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.