

ART 5.10.4 Conduct Electronic Protection

Plan and implement actions such as communications avoidance or communications antijamming measures to protect personnel, facilities, and equipment from friendly and enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability. (FM 3-13) (USACAC)

NO.	Scale	Measure
01	Yes/No	Unit course of action was not compromised by enemy offensive information operations (IO).
02	Time	To develop and refine IO annex to operation order.
03	Time	For friendly information and intelligence collection sensor system managers, operators, and emergency response teams or contact teams to respond, identify, and correct system failures attributed to enemy offensive IO.
04	Time	To identify, determine appropriate response, and implement changes in response to a possible threat to information systems.
05	Percent	Of time units in the area of operations (AO) are in restrictive information operations condition.
06	Percent	Of friendly emitters in the AO known to have been exploited by an enemy.
07	Percent	Of information systems hardware, software components, and databases backed up by replacement components or backup files in case of failure or compromise.
08	Number	Of times to reprogram information system software in response to identified threats.
09	Number	Of instances of enemy offensive IO disabling, corrupting, or compromising friendly information systems and intelligence collection sensors.
10	Number	Of instances of electronic fratricide in the AO.

Supporting Collective Tasks:

Task No.	Title	Proponent	Echelon
71-9-	Conduct Electronic Warfare in the Joint	71 -	Echelons

5640	Operations Area (Division Echelon and Above [Operational])	Combined Arms (Collective)	Above Corps
71-9-6330	Employ Electronics Security in the Joint Operations Area for Operational Forces (Division Echelon and Above [Operational])	71 - Combined Arms (Collective)	Echelons Above Corps