



INFORMATION-RELATED CAPABILITIES: MILITARY DECEPTION

Last Updated: 28 April 2016

[Military deception](#) (MILDEC) is defined as “actions executed to deliberately mislead adversary military, paramilitary, or violent extremist organization decision makers, thereby causing the adversary to take specific actions (or fail to take actions) that will contribute to the accomplishment of the friendly mission.”¹ Deception operations can span all levels of war and can include, at the same time, both offensive and defensive components. During planning, MILDEC can be integrated into the early [phases of an operation](#). The MILDEC role during the early phases of an operation will be based on the specific situation of the operation or campaign to help set conditions that will facilitate phases that follow. Deception can distract the adversary from legitimate friendly military operations and can confuse and dissipate adversary forces. MILDEC affects the adversary’s information systems, processes, and capabilities to create desired behavior. MILDEC planners require adversary and potential adversary decision maker analysis for a sufficiently detailed understanding of how the information environment supports the adversary’s decision-making process.

Each [information-related capability](#) (IRC) has a part to play in successful MILDEC credibility over time, so [information operations](#) (IO) facilitates close coordination with [military information support operations](#) (MISO), operations security (OPSEC), [public affairs](#) (PA), and [commander’s communication synchronization](#) (CCS) personnel within the [joint IO cell](#) or staff. Whereas MISO, PA, and CCS activities may share a common specific audience with MILDEC, only MILDEC actions are designed to mislead. There is a delicate balance between successful deception efforts and media access to ongoing operations. Inappropriate media access may compromise deception efforts. Conversely, MILDEC must not intentionally target or mislead the news media, the US public, or Congress. Deception activities potentially visible to the US public should be closely coordinated with PA operations so as to not compromise operational considerations or diminish the credibility of [PA operations](#) in the national media. Due to the sensitive nature of MILDEC plans and objectives, a strict need-to-know policy should be enforced. Additionally, approval authorities for conducting MILDEC actions are typically at the joint force commander-level or above, so the approval action may require sufficient lead time for staffing.

¹ JP 3-13.4, [Military Deception](#).



Army Field Manual 90-2, *"Battlefield Deception,"* (October 1988) revealed that the Army was revitalizing its deception capabilities, leading up to the greatest modern use of tactical deception in 1991 — Operation DESERT STORM. During DESERT STORM, a signal company mimicked traffic for the XVIII and V Corps headquarters to make it appear that they were stationary, when in fact they were moving into position for the "left hook," a flanking maneuver through the western Iraqi desert. The enemy focused on an amphibious training demonstration put on by the Marine Corps, causing Iraqi forces to reinforce the coastline, facing away from the main attack.