



INFORMATION-RELATED CAPABILITIES: COUNTERINTELLIGENCE

Last Updated: 28 April 2016

[Counterintelligence](#) (CI) is defined as “information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities.”¹ Air Force Office of Special Investigation oversees all Air Force CI activities.

CI support to [information operations](#) (IO) includes identifying threats within the [information environment](#) through CI collections and analysis and assessing those threats through reactive and proactive means. Threat documentation through [intelligence, surveillance, and reconnaissance](#) (ISR) processes and CI products are the primary methods of notifying commanders. CI has the capability to neutralize and exploit threats through investigation and operations. Successful CI and [operations security](#) (OPSEC) activities deny adversaries useful information on friendly forces. CI typically has a close working relationship with [information-related capabilities](#) (IRCs) such as ISR and OPSEC but may not have the same habitual relationship with other IRCs. IO planners should ensure collaboration with CI professionals to maximize CI integration with other IRCs such as [military information support operations](#), [military deception](#), and [cyberspace operations](#).

¹ JP 2-0, [Joint Intelligence](#).