



COUNTERTHREAT OPERATIONS (FP)

Last Reviewed: 13 August 2014

Counterthreat operations (CTO) are defined as the employment of [AFOSI](#) capabilities to find, fix, track, and neutralize enemy threats in order to create a sustained permissive environment for [air](#), [space](#), and [cyberspace](#) operations.¹ CTO are essential in detecting, assessing, denying, and responding to threats affecting Air Force operations. CTO are [intelligence, surveillance, and reconnaissance](#) (ISR)-driven operations using information derived from multiple intelligence and [counterintelligence](#) sources providing tactical situational awareness to forewarn or preempt enemy or adversarial attack. CTO activities include counterintelligence collection, analysis, and investigation; surveillance; and countersurveillance. These activities provide excellent sources of intelligence that assist [force protection](#) (FP) operations. The base defense forces should use ISR to aggressively eliminate threats. The ability to acquire and analyze suspicious activity reports for indications and warning of possible terrorist pre-attack activities is a critical component of counterintelligence support to the force protection mission. Terrorists have the advantage of choosing the time and venue for their attacks, but normally have to conduct extensive pre-attack preparations to maximize their chances of success. The pre-attack phase of a terrorist operation, however, is the period of greatest vulnerability to the terrorist group, since it must surface to collect intelligence and conduct physical surveillance and other activities of the target. Therefore, an effective system, such as CTO, for detecting terrorist pre-attack activities is a high priority task for the intelligence community, law enforcement, security elements, and local community authorities.

¹ See AFTTP 3-10.3, [Integrated Base Defense Counterthreat Operations](#), for more information on CTO.