CURTIS E. LEMAY CENTER
FOR DOCTRINE DEVELOPMENT AND EDUCATION

AIR FORCE DOCTRINE PUBLICATION (AFDP) 3-10
FORCE PROTECTION

THREATS TO THE AIR FORCE MISSION (FORCE PROTECTION)

Last Updated: 19 November 2019

The threats facing the Air Force are broad and extensive. They range from powerful state actors with the full range of conventional and chemical, biological, radiological, and nuclear (CBRN) weapons delivered by sophisticated means to dangerous and ingenious non-state actors with inventive and asymmetric methods of delivering scalable harm to our forces. Such threats can create an unpredictable environment capable of inflicting catastrophic damage with or without notice. Consequently, Air Force personnel, aircraft, satellites, equipment, installations, operating locations, and, by extension, the Air Force mission are vulnerable to a wide variety of threats. This potentially daunting prospect demands force protection (FP) awareness and education at all levels and effective FP measures that are implemented through a coherent and coordinated FP command structure.

FORCE PROTECTION THREAT SPECTRUM

> Prior to the attack on Khobar Towers in June 1996, the largest terrorist strike against US forces occurred on 23 October 1983 when two large vehicle-borne improvised explosive devices (VBIEDs) struck separate buildings housing US and French military forces in Beirut, Lebanon, killing 241 US military personnel. The VBIEDs were estimated at 15,000 to 21,000 pounds of TNT equivalent. In the Khobar Towers attack, a truck laden with 20,000 pounds of TNT was detonated, destroying the building and killing 19 Americans. In another scenario in 2003, three housing complexes were simultaneously attacked in Riyadh. In this case, trucks loaded with explosives were driven behind vehicles designed to penetrate the compound defenses. In each case, the attackers appeared to have placed little priority on their own survival.

It is the commander’s responsibility to recognize threats to the Air Force and its mission across the competition continuum that encompasses the competition continuum and therefore consider the intentional objectives of threat actors. There are a variety of threats facing the Air Force. Threats may arise from terrorists or insurgents, insiders, criminal entities, foreign intelligence entities, opposing military forces, or violent activist organizations.

US forces should consider the potential of an attack from an insider threat. On 27 April 2011, an Afghan air force pilot used his pistol to kill eight Airmen and one American contractor at Kabul International Airport. After a gun battle with two US officers, the attacker was killed by Afghan quick reaction force (QRF) members. This type of insider attack, known as a green-on-blue attack, began as an adversary tactic in 2008, and hit a peak in 2012, with 44 incidents. To mitigate risk of additional green-on-blue attacks, military leaders in Afghanistan instituted the Guardian Angel program, which provides a specially trained and dedicated armed overwatch to protect military advisors and personnel from insider threats and attacks. The US casualties were supporting the Afghan government as part of a North Atlantic Treaty Organization-led International Security Assistance Force in Afghanistan.

The examples in this section demonstrate that, in addition to addressing the threats below, Airmen should continually consider "what if" scenarios to counter potential future threats. Tactics and procedures introduced in one theater could be seen again in other regions and may result in increased FP measures due to the threat of attack which could affect ongoing operations.

At approximately 2200L on 14 September 2012, 15 heavily-armed Taliban insurgents dressed in US Army uniforms breached the eastern perimeter of Camps Bastion, Leatherneck, and Shorabak in Afghanistan undetected. They split into three teams of five men each, and commenced a coordinated attack on the Camp Bastion airfield. US and coalition personnel present on the airfield responded immediately, and the US and United Kingdom (UK) QRF made contact with the enemy shortly thereafter, beginning an engagement lasting into the early hours of 15 September 2012. The resulting friendly casualties and damage included two US personnel killed in action, eight US personnel wounded in action (WIA), eight UK personnel WIA, one civilian contractor WIA, six aircraft destroyed, eight aircraft damaged, and multiple other facilities and resources damaged. The QRFs, supported by US and UK personnel and helicopters, killed 14 of the Taliban attackers and wounded the remaining attacker, who was detained and interrogated. Only heroic action by US and UK forces on the scene prevented greater loss of life and equipment.

Types of Threats

In addition to those known threats, there is the paradox of countering unknown threats. The types of threats listed below provide general categories; this list is not exhaustive, but can be used as a guide.

- ✪ **Conventional Threat**—Regular military forces supported by a recognized government including air, land, maritime, and space forces.

- ✪ **Unconventional Threat**—This threat encompasses a broad spectrum of military and paramilitary operations predominantly conducted through, with, or by indigenous or surrogate forces who are organized, trained, equipped, supported, and directed in varying degrees by an external source. It includes guerrilla warfare and other direct offensive, low visibility, covert, or clandestine operations, as well as the indirect activities of subversion, sabotage, intelligence activities, and evasion and escape networks.

- ✪ **Terrorism Threat**—This threat involves the calculated use of violence or threat of violence to instill fear and is intended to coerce or intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological. Acts of terrorism are often planned to attract widespread publicity and are designed to focus attention on the existence, cause, or demands of the terrorists, and erode public confidence in the ability of a government to protect and govern the people.

- ✪ **Criminal Threat**—Criminal activity may help predict future actions or provide advanced indications and warnings of attack. For example, theft of vehicles, military identification cards, passports, or installation entry passes are potential indicators of pending hostile action. Synthesized analysis of law enforcement and counterintelligence information is necessary to identify indicators of future attacks. Aggressive and continuous liaison efforts are needed for timely information sharing and willing cooperation from host forces.

- ✪ **Insider Threat**—This threat comes from assigned or attached personnel (military or civilian), host-country nationals (military or civilian), third country nationals (contract employees) or other persons assigned to or transiting an area of responsibility. Any of these groups of people may threaten Air Force interests by disclosing sensitive or classified information, by making decisions that favor dissident groups, or by irregular attack. They may target individuals, groups, facilities, weapon systems, or information systems. Host country forces may not provide the degree of FP anticipated or agreed to under treaty or coalition arrangements.

- ✪ **Psychological Threat**—Enemy threats target the psychological and physical well-being of Air Force personnel. The threat of CBRN attacks can hinder effective military operations as much as an actual attack. The enemy may also use deception (such as releasing harmless powder) to undermine the mission. Enemy propaganda and potentially biased media sources may also undermine coalition and public support, create civil unrest, and dangerously weaken military morale. Commanders should recognize the importance of effective communication to minimize FP risks.

- **CBRN Threats**—The CBRN threats are chemical, biological, radiological, and nuclear weapons or hazards that pose or could pose a threat to individuals. These threats may result from the deliberate employment of weapons of mass destruction by enemy forces.

- **Civil Unrest Threat**—This threat reflects country-specific concerns of violence by the population related to friendly force operations. The threat can manifest itself during protests, demonstrations, refugee and humanitarian operations, or any other local tensions that may escalate into a direct threat to US forces.

- **Information/Data Threat**—This threat results from attempts to adversely affect Air Force information systems, information-based processes, and computer-based networks. The enemy and its unconventional supporters may attempt to impact military command and control; disrupt support activities such as local, military, and civil financial institutions; and interfere with supervisory control and data acquisition systems used to control critical infrastructures.

Threat Levels

Threat Levels	Examples
Level I	**Agents, saboteurs, sympathizers, terrorists, civil disturbances**
Level II	**Small tactical units, unconventional warfare forces, guerrillas, may include significant stand-off weapon threats**
Level III	**Large tactical force operations, including airborne, heliborne, amphibious, infiltration, and major air and space operations**

Threat Levels

Enemy threats to Air Force assets take many forms and include any combination of types of threat. There are three levels of threat, depicted in the figure, "Threat Levels," and defined in JP 3-10, *Joint Security Operations in Theater*, which require security responses to counter them. These threat levels aid in performing risk assessments as well as conducting force protection planning. Each level or any combination of levels may exist in an operational area either independently or simultaneously. Emphasis on specific base or lines of communication security measures may depend on the anticipated level of threat supported by intelligence. This does not imply that threat activities will occur in a specific sequence or that there is a necessary interrelationship among the levels.

Level I Threats. Typical Level I threats include enemy agents and terrorists whose primary missions include espionage, sabotage, and subversion. Enemy activity and individual attacks may include random or directed killing of military and civilian personnel, kidnapping, and guiding special-purpose individuals or teams to targets.

Level I threat tactics may also include hijacking air, land, maritime and space vehicles for use in direct attacks; the use of improvised explosive devices (IEDs); vehicle borne IEDs (VBIEDs); or individual grenade and rocket-propelled grenade attacks. Civilians sympathetic to the enemy may become significant threats to US and multinational operations. They may be the most difficult to counter because they are normally not part of an established enemy agent network and their actions may be random and unpredictable. Countering criminal activities and civil disturbance requires doctrine and guidelines that differ from those used to counter conventional forces, and normally requires detailed coordination with external agencies. More significantly, based on political, cultural, or other perspectives, activities that disrupt friendly operations may be perceived as legitimate by a large number of the local populace. Countering Level I threats is a part of the day-to-day FP measures implemented by all commanders. Key to countering these threats is the active support of some portion of the civilian population, normally those sympathetic to US or multinational goals.

Level II Threats. Level II threats include small scale forces conducting irregular warfare that can pose serious threats to military forces and civilians. These attacks can cause significant disruptions to military operations as well as to the orderly conduct of local governments and services. These forces are capable of conducting well-coordinated, but small-scale, hit and run attacks, IED and VBIED attacks, and ambushes, and may include significant standoff weapons threats such as mortars, rockets, rocket-propelled grenades, and surface-to-air missiles.

Level II threats may include special operations forces highly trained in irregular warfare. These activities may also include operations typically associated with attacks outlined in the Level I threat including air, land, maritime and space vehicle hijacking. These forces establish and activate espionage networks, collect intelligence, carry out specific sabotage missions, develop target lists, and conduct damage assessments of targets struck. They are capable of conducting raids and ambushes.

Level III Threats. Level III threats may be encountered when an enemy has the capability to project combat power by air, land, sea, or space anywhere into the operational area. Specific examples include airborne, heliborne, and amphibious operations; large combined arms ground force operations; and infiltration operations involving large numbers of individuals or small groups infiltrated into the operational area and committed against friendly targets. Air and missile threats to bases, base clusters,[18] lines of communication, and civilian targets may also pose risks to joint forces, presenting themselves with little warning time.

Level III threats are beyond the capability of base and base cluster security forces, and can only be effectively countered by a tactical combat force or other significant force.

US Air Force Airmen successfully conducted base perimeter force protection operations 17 July 2014 to defend their operating locations when insurgents attacked an Afghanistan Air Force (AAF) air base using rocket-propelled grenades, machine guns, small arms fire, and VBIEDs. US Air Force Security Forces from the 438th Air Expeditionary Advisory Wing (AEW) took immediate action, establishing defenses and returning fire to defend the 438 AEW compound. Nearby, a USAF Special Operations Forces (SOF) Combat Aviation Advisor (CAA) team from the 6th Special Operations Squadron, assigned to a joint US SOF Advisory Group embedded with the AAF, was also taking fire. CAAs manned firing positions using their personal firearms and operating M-240 machine guns to lay down counter fire against the attackers. During the attack, the CAA Airmen also set up an initial medical aid station. The Airmen's "airmindedness" played a role in the defense, as the CAAs, working with their AAF counterparts, coordinated a combined AAF and US Air Force airpower show of force over the base. The Airmen's role in defending the base highlights the effectiveness of their FP preparation and training. The base sustained only minor damage with no friendly forces' loss of life.

[18] For information on base cluster defense operations, see Joint Publication 3-10, *Joint Security Operations in Theater*.