ATP 3-37.15

FOREIGN SECURITY FORCE THREATS

JANUARY 2020

INCORPORATING CHANGE 1, MAY 2025

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

HEADQUARTERS, DEPARTMENT OF THE ARMY

This publication is available at the Army Publishing Directorate site (https://armypubs.army.mil) and the Central Army Registry site (https://atiam.train.army.mil/catalog/dashboard).

Change No. 1
Army Techniques Publication
No. 3-37.15

Headquarters
Department of the Army
Washington, D.C., 23 May 2025

Foreign Security Force Threats

1. Change 1 to ATP 3-37.15, 30 January 2020, replaces all occurrences of the term “gender” with the term “sex” in accordance with Executive Order 14168, dated 20 January 2025.

2. A plus sign (+) marks modified content.

3. ATP 3-37.15, 23 May 2025, is changed as follows:

Change Version Page(s)	Change Description
Page 2-5	Replaces “genders” with “sexes”
Page 3-7	Replaces “same-gender” with “same-sex”
Page 3-7	Replaces “mixed-gender” with “mixed-sex”
Page 3-8	Replaces “gender” with “sex”
Page 3-11	Replaces “mixed-gender” with “mixed-sex”

4. An updated Authentication page has amended the prior authentication reflected in the rear of this publication.

DISTRUBUTION RESTRICTION: Approved for public release; distribution is unlimited.

This page intentionally left blank.

Army Techniques Publication
No. 3-37.15

Headquarters
Department of the Army
Washington, DC, 30 January 2020

FOREIGN SECURITY FORCE THREATS

Contents

Page

PREFACE ..... **iii**

INTRODUCTION ..... **v**

Chapter 1 **FOREIGN SECURITY FORCE THREAT FUNDAMENTALS** **1-1**
Characteristics of the Foreign Security Force Threat 1-1
Causation 1-3

Chapter 2 **FOREIGN SECURITY FORCE THREAT PREVENTION AND RESPONSE FRAMEWORK** **2-1**
Five Functions 2-1
Prevent 2-1
Deter 2-12
Defeat 2-15
Exploit 2-16
Recover 2-18

Chapter 3 **FOREIGN SECURITY FORCE THREAT TRAINING PROGRAM** **3-1**
Training to Prevent 3-1
Training to Deter 3-2
Training to Defeat 3-4
Training to Exploit 3-6
Training to Recover 3-12

Chapter 4 **FOREIGN SECURITY FORCE PLANNING AND OPERATIONS** **4-1**
Planning Considerations 4-1
Preparation 4-6
Assess 4-7

SOURCE NOTES ..... **Source Notes-1**

GLOSSARY **Glossary-1**

REFERENCES **References-1**

INDEX **Index-1**

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

Figures

Figure 2-1. The predictive classification concept 2-8
Figure 2-2. Defense in depth 2-14
Figure 2-3. Point of dominance 2-15

Tables

Table 3-1. Threat detection and neutralization 3-3

Vignettes

The Soviet Union in Afghanistan 1-2
Jordanian Soldier Kills Three U.S. Soldiers 1-3
Attacker Motivated by Family Member's Detention 1-4
Desecration of Religious Materials Inspires Attack 1-5
Corrupt Officer Attacks U.S. Air Force Advisors 1-6
Taliban Co-opts Afghan Border Policeman 1-7
Attacker Motivated by Abuse 1-8

Preface

ATP 3-37.15 provides fundamental principles and techniques for preventing and defeating foreign security force threats. It is based on lessons learned from several years of persistent, limited contingency operations.

The principal audience for ATP 3-37.15 is all members of the profession of arms. Commanders and staffs serving as joint task force or multinational headquarters should also refer to applicable joint or multinational doctrine concerning the range of military operations and joint or multinational forces. Trainers and educators throughout the Army can also use this publication.

Commanders, staffs, and subordinates ensure their decisions and actions comply with applicable United States (U.S.), international, and, in some cases, local laws and regulations. Commanders at all levels ensure that their Soldiers operate in accordance with the law of war and the rules of engagement. (See FM 6-27.)

ATP 3-37.15 implements elements of NATO Standardization Agreement (known as STANAG) 6513 and NATO Allied Tactical Publication (known as ATP)-3.16.1 into U.S. Army doctrine.

ATP 3-37.15 uses joint terms where applicable. Selected joint and Army terms and definitions appear in both the glossary and the text. The term for which ATP 3-37.15 is the proponent publication (the authority) is presented in italics and bold font in the text and is marked with an asterisk (*) in the glossary. When first defined in the text, the term for which ATP 3-37.15 is the proponent publication is boldfaced and italicized, and the definition is boldfaced. When first defining other proponent definitions in the text, the term is italicized and the number of the proponent publication follows the definition. Following uses of the term are not italicized. This publication uses the acronym *FSF* for foreign security force (singular). This differs from the joint acronym *FSF* which stands for foreign security forces (plural).

ATP 3-37.15 applies to the Active Army, Army National Guard/Army National Guard of the United States, and United States Army Reserve unless otherwise stated.

The proponent of ATP 3-37.15 is the United States Army Combined Arms Center. The preparing agency is the Combined Arms Doctrine Directorate, United States Army Combined Arms Center. Send comments and recommendations on DA Form 2028 (*Recommended Changes to Publications and Blank Forms*) to Commander, United States Army Combined Arms Center and Fort Leavenworth, ATTN: ATZL-MCD (ATP 3-37.15), 300 McPherson Avenue, Fort Leavenworth, KS 66027-2337; by email to usarmy.leavenworth.mccoe.mbx.cadd-org-mailbox@mail.mil; or submit an electronic DA Form 2028.

Acknowledgements

The copyright owners listed here have granted permission to reproduce material from their works.

Quote from Bill Roggio's "Taliban Promise Suicide Assaults, 'Insider Attacks' in this Year's Spring Offensive." *Foundation for the Defense of Democracies Long War Journal*. 29 April 2013. Copyright © 2007 – 2019. Multimedia Inc.

The predictive classification concept is adapted from the Department of Energy's *Predictive Modeling for Insider Threat Mitigation*, 2009.

Paraphrased courtesy Oriana Pawlyk, "Questions Remain As Families Mourn Victims of 2011 Green-On-Blue Kabul Attack," *AirForceTimes.com*, 27 April 2018. © 2019 Sightline Media Group.

Paraphrased courtesy Bilal Sarwary, "Anatomy of an Afghan 'Turncoat' Killer," from *BBC News* at bbc.co.uk/news, October 21, 2011. Copyright © 2019 BBC.

"Securing the Security Force Assistance Advisors in Afghanistan" by Pete Escamilla and Eric Lopez is reprinted from *Small Wars Journal* per the Creative Commons license granted upon its https://smallwarsjournal.com/jrnl/art/securing-the-security-force-assistance-advisors-in-afghanistan.

Introduction

A foreign security force threat is the potential for violence posed by foreign security forces (FSFs) working with, or granted access to, U.S. Service members, civilians, or contractors. Previously referred to as green-on-blue attacks, persistent limited contingency and stability operations have revealed the vulnerabilities inherent in multi-partner environments. These operations require close integration and partnership with FSFs, thereby increasing the risk that an enemy will exploit this access to attack U.S. forces. These attacks threaten to undermine the cohesion and trust necessary for unified action partners to shape, prevent, and ultimately win in a volatile and complex environment. This threat is not bound by time or geography and, as U.S. forces will continue to work alongside FSFs in future operations, it will likely persist.

ATP 3-37.15 clearly addresses the FSF threat, distinguishing it from the related, but distinct, insider threat. The term "insider threat" as derived from the 2017 National Defense Authorization Act means, with respect to the Department of Defense, a threat presented by a person who has, or once had, authorized access to information, a facility, a network, a person, or a resource of the Department; and wittingly, or unwittingly, commits an act in contravention of law or policy that resulted in, or might result in, harm through the loss or degradation of government or company information, resources, or capabilities; or a destructive act, which may include physical harm to another in the workplace. Insider threats and attacks can occur both at home and abroad, while FSF threats occur primarily in expeditionary environments during contingency operations. (For more information on insider threat prevention and response, see AR 381-12.)

This publication provides tactics, techniques, and procedures for providing personnel security, increasing survivability, and preventing and defeating the FSF threat. Although completely eliminating the threat is unlikely, units and organizations can apply the measures herein to better position themselves to prevent, deter, defeat, exploit, and recover from FSF attacks. Defeating the FSF threat requires discipline, awareness, teamwork, and training. This is particularly important for units executing security force assistance or stability operations, as they are under a significantly increased risk of attack. These units develop unit training plans, battle drills, and standard operating procedures designed to increase survivability and to prevent and defeat the FSF threat.

ATP 3-37.15 provides the doctrinal foundation for units to build a comprehensive survivability, threat prevention, and defeat program. It defines key terms, examines motives and methods behind FSF attacks, and explores the context behind previous incidents. It also outlines potential threat indicators that aid early detection. Furthermore, it presents the Army FSF threat prevention and response model and offers training and techniques to prevent and defeat FSF threats. Finally, ATP 3-37.15 provides planning considerations for units at all levels to incorporate into their operations.

ATP 3-37.15 contains four chapters:

- **Chapter 1** defines key terms, provides context for previous FSF attacks, and explores the methods and causations behind these attacks.
- **Chapter 2** presents the Army FSF threat prevention and response model. It details how units can prevent, deter, defeat, exploit, and recover from an FSF attack. The tactics, techniques, and procedures presented are designed to protect units and Soldiers operating alongside multinational partners.
- **Chapter 3** examines training requirements for an effective FSF threat prevention and response program. Soldiers can incorporate techniques into unit training before or during a deployment requiring close cooperation with FSF.
- **Chapter 4** reviews planning considerations for incorporating FSF threat mitigation measures into operations at all levels. This chapter offers planning considerations that assist units in properly addressing the FSF threat when incorporated during troop leading procedures and the military decision-making process.

This page intentionally left blank.

Chapter 1
Foreign Security Force Threat Fundamentals

This year's spring operation, in accordance with its combat nature, will consist of special military tactics…while successful insider attacks, to eliminate foreign invaders, will be carried out by infiltrating Mujahideen inside enemy bases in a systematic and coordinated manner.

Islamic Emirate of Afghanistan
Spring 2013 Offensive Statement

The foreign security force (FSF) threat is not a new phenomenon; however, during recent limited contingency operations, U.S. forces experienced a sharp increase in the number of attacks perpetrated by FSFs. This chapter introduces the FSF threat by exploring its context, causation, and methods. It also facilitates shared understanding and dialogue by defining relevant terms. Armed with this knowledge, Soldiers and leaders will be better positioned to properly implement the threat prevention and defeat techniques described in subsequent chapters.

CHARACTERISTICS OF THE FOREIGN SECURITY FORCE THREAT

1-1. A FSF threat is the potential for violence posed by FSFs working with, or granted access to, U.S. Service members, civilians, or contractors. An FSF threat attack is a violent act perpetrated against a U.S. Service member, civilian, or contractor by a FSF member or members who have access to U.S. Service members, civilians, or contractors. *Foreign security forces* are those forces, including, but not limited to military, paramilitary, police, and intelligence forces; border police, coast guard, and customs officials; and prison guards and correctional personnel, that provide security for a host nation and its relevant population or support a regional security organization's mission (FM 3-22). FSFs may belong to the host-nation government, belong with a paramilitary organization, or consist of a third party's contribution to a multinational operation. When operating in an expeditionary, multi-partner environment, the potential for a violent attack by FSFs increases significantly since they operate alongside U.S. Service members and civilians. This threat has proven particularly challenging during protracted limited contingency operations in which U.S. forces work with FSFs to stabilize a fragile state by advising and assisting its security or police forces.

1-2. Often referred to as green-on-blue violence or an inside the wire attack, FSF attacks are characterized by speed, surprise, shock, opportunity, and violence. The attacks often occur quickly and without warning intending to shock both local security forces and a wider audience through their brazen nature. The opportunity for these attacks exists once FSFs have access to U.S. forces or facilities and can operate closely with them.

1-3. Whether successful or not, FSF attacks seek to directly kill or injure U.S. Service members or civilians. These attacks can take many forms such as assassinations, mass shootings, suicide bombings, and vehicle-borne improvised explosive device (also called VBIED) attacks. Often notable for their brazen and irrational nature, attackers show little regard for their own safety or the threat of capture.

1-4. An attacker often has intended victims and will seek them out during an attack. However, attackers will also accept targets of opportunity and will likely continue the attack after finding intended victims. As such, an attacker will often continue attacking throughout buildings or compounds until stopped by U.S. forces, FSFs, or suicide.

1-5. FSF attacks generally target U.S. forces during periods of perceived security. Attackers often intend to use the element of surprise to exploit vulnerable Soldiers and maximize lethality. Attacks often occur at locations where U.S. Service members believe they are safe and have little reason to expect an enemy attack. Potential locations for FSF attacks include U.S. or FSF bases, host-nation government buildings, or intergovernmental or nongovernmental organization facilities. Attacks may also occur at training events, such as at a small arms range or during combined operations.

1-6. FSF attacks serve multiple purposes for an enemy force. At the strategic level, these attacks are a form of messaging. They communicate to an international audience that U.S. efforts are failing and lack the support of either the host-nation or multinational partners. This messaging may be an effort to undermine national will by upsetting the U.S. domestic population and influencing decision makers to adjust or abandon strategic objectives. In the past, these attacks have undermined national will by persuading foreign leaders to alter national policy. For example, in 2012, an FSF attack in Afghanistan that killed four French soldiers resulted in the French government temporarily suspending all partnerships and training operations in Afghanistan. At the operational level, threats use these attacks to degrade or impede interoperability by altering the acceptable level of risk requisite for multinational operations. Tactically, FSF attacks erode the trust and cohesion necessary for U.S. Service members to work alongside FSFs to achieve common objectives.

The Soviet Union in Afghanistan

The foreign security force threat is not a recent phenomenon. It has been employed throughout history by disadvantaged military forces attempting to defeat a stronger enemy force. In March 1979, Ismail Khan, a captain in the Afghan Army, orchestrated the murder of 50 Soviet military advisors and 300 of their family members in Herat Province, Afghanistan. After beheading many of his victims, Khan placed the severed heads on spikes and paraded them through the city as a warning to both the Soviet Union and the local population. The atrocity served as an impetus for the Soviet Union's full-scale invasion of Afghanistan in December of that year.

1-7. The FSF threat primarily exists in expeditionary environments, posing the greatest risk to those units and personnel performing security force assistance (SFA), stability, or counterinsurgency operations. These operations require close contact and integration with FSFs, thereby expanding a threat force's opportunity to attack. They also require an extensive amount of cross-cultural communication, compromise, and understanding, increasing the potential for personal or cultural conflict. In these environments, attackers often seek opportunities where U.S. forces are particularly exposed, where senior leaders are present, or where ceremonies or key events occur (to make a strategic statement). Key leader engagements (KLEs), graduation ceremonies, parades, and high-profile training events illustrate potential high-value targets (also called HVTs) for an FSF attack. A *high-value target* is a target the enemy commander requires for the successful completion of the mission (JP 3-60).

1-8. FSF attacks often target senior leaders to draw additional attention to an attack by elevating its profile. The presence of leaders may entice an attacker to act. Units planning for KLEs and similar events consider risks and accommodations.

1-9. Historical evidence reveals the FSF threat is most prevalent during stability operations. During these operations U.S. forces work closely with FSFs to re-establish security and essential services, often presenting a greater opportunity for an attack. Between 2008 and 2017, 96 FSF attacks were carried out against U.S. or multinational forces conducting stability operations in Afghanistan. These attacks resulted in approximately 152 U.S. or multinational deaths and over 200 wounded personnel. However, this does not mean that attacks are limited to specific missions or phases; instead, the potential for an FSF threat exists anytime U.S. forces are partnered with FSF and can occur during operations to shape, prevent, or win during large-scale combat operations.

Jordanian Soldier Kills Three U.S. Soldiers

In November 2016, three U.S. Soldiers were shot and killed by a Jordanian soldier as their vehicle approached the entry control point at the King Faisal Airbase in southern Jordan. The Soldiers were returning to the base in a four-vehicle convoy after completing a training mission as part of the U.S. effort to defeat the Islamic State in Iraq and Syria. The attacker, Marik al-Tuwayha, claimed he believed the convoy presented a threat; however, in video footage recovered from the scene he is seen reloading his weapon after the Americans identified themselves as friendly. Although his motive was unclear, al-Tuwayha was found guilty of voluntary manslaughter, violating military orders, and insulting the dignity and reputation of the Jordanian armed forces. In July 2017 he received a life sentence.

This incident is an important reminder that foreign security force (FSF) threats are not limited to counterinsurgency or stability operations and can occur anytime U.S. forces partner closely with FSFs. This includes during operations to shape or prevent, where an enemy may exploit the perceived lack of an active threat to surprise U.S. forces.

CAUSATION

1-10. The Army uses six categories to classify FSF attacks: personal, ideological, reactionary, criminal, enemy, and general. These categories assist in understanding the motives behind FSF attacks and can aid in detecting a potential threat. The categories are not mutually exclusive, and an attack can often be classified in two or more categories at once. For example, an FSF member may have a dispute with a U.S. Service member (personal) while simultaneously beginning to sympathize with an extremist organization and its cause (ideological). There are many reasons why FSFs may decide to attack; however, they are usually motivated by a trigger that falls into one of the categories listed in paragraphs 1-11 through 1-27.

PERSONAL

1-11. A personal attack occurs when an FSF member acts intentionally yet independently as an individual attacker, without direct guidance, command, or preplanning from external entities. Such attacks account for most violent incidents between U.S. Service members and FSFs, and they are often motivated by personal grievances, cultural animosity, or misunderstanding. A personal attack may also be caused by a specific grievance with U.S. or partnered forces; this is particularly true when U.S. forces kill or detain a host-nation soldier's family member, relative, or close friend.

1-12. A study conducted during protracted contingency operations in Afghanistan found that many FSF attacks were motivated by personal grievances, cultural animosity, or disrespect. The study revealed that these attacks usually occurred once an FSF member became belligerent after a disagreement or perceived socio-cultural transgression committed by a U.S. Service member. It also indicated that attacks may be caused by simple personality conflicts, disparate standard operating procedures (such as disarming FSF members when they enter a U.S. base or not allowing FSF vehicles to pass U.S. convoys), or the use of offensive language.

1-13. Offensive language—even when not directed at an FSF member, unit, or nationality—may upset an FSF member enough to prompt an attack. Soldiers need to start and maintain relationships with FSF members by demonstrating positive behaviors. Ethnocentric behavior or xenophobic attitudes may intensify tensions originating from operational disparities that cannot be adjusted. Effective leaders ensure their Soldiers conduct themselves as professionals by respecting foreign cultures when operating alongside FSFs. This is best accomplished by treating FSFs as peers and partners, not subordinates.

1-14. Combat stress can escalate seemingly trivial personal disputes into violent attacks. This is particularly true for host-nation security forces (HNSF) experiencing combat in their homeland. Often, these soldiers are additionally stressed as their families, friends, and relatives experience the privations of combat. U.S. Service

members must recognize this by showing empathy for host-nation soldiers and their challenges of fighting a war in their homeland.

1-15. Personal attacks may be prevented by proactive and engaged leaders. Effective leaders identify personality conflicts or disputes between Soldiers and FSF members and proactively work to resolve conflicts. Leaders should also remove or transfer Soldiers who lack the interpersonal skills, maturity, or emotional intelligence to work alongside FSFs. A comprehensive cultural awareness training program will help Soldiers understand how to behave alongside both FSFs and the local population. This training can be provided by FSFs and may serve as a healthy cultural exchange between partnered units. Finally, leaders look for and recognize the signs of combat stress in both their Soldiers and partnered forces, ensuring that Soldiers receive adequate rest and relaxation to mitigate the effects of combat.

Attacker Motivated by Family Member's Detention

On September 29, 2008, one U.S. Soldier was killed and two were injured at an Afghan National Police station when an Afghan National Policeman attacked their patrol in Paktia Province. The incident occurred after the patrol gained access to the station and Soldiers were conducting security force assistance operations. The attacker opened fire without warning but was quickly killed by U.S. Service members. It was later determined that the attacker's brother was a member of the Taliban and had recently been captured by U.S. forces. The Soldiers' quick reaction, awareness, and aggressive posture likely prevented additional casualties.

IDEOLOGICAL

1-16. An ideological attack occurs when an FSF member is radicalized by an extremist ideology that encourages attacks for religious, political, or other ideological reasons (see ATP 3-37.2 for additional information on ideological considerations and categories). The individual may exhibit intense hatred of those who do not ascribe to their belief system and may focus their attention on the more radical or extreme elements of their ideology. Ideologically motivated threats are similar to personal threats in that an individual may adopt them without external support. However, an individual will likely be influenced by extremist media or propaganda during the radicalization process.

1-17. Ideologically motivated attackers may demonstrate indicators of their potential for violent action as they progress through the radicalization process. An indicator is a behavior, action, or event that precedes an attack. Individuals undergoing radicalization may become so consumed by their extremist ideology that they cannot conceal the changes associated with it and often present behavioral indicators. Potential indicators of an ideologically motivated threat include individuals complaining about other nations, religions, or cultures; defending radical groups or ideologies; and isolating themselves from the group or unit. (See paragraphs 2-29 through 2-33 for additional behavioral indicators.)

REACTIONARY

1-18. A reactionary attack occurs when an FSF member responds to a local, regional, or international event by attacking U.S. or partnered forces. FSF members may react violently to any number of events or issues. They may take offense to a U.S. policy decision or statement towards their country, region, or tribe. Culturally inflammatory acts like the desecration of religious materials or sites can also trigger an attack. Likewise, threats or insults to religious leaders may spark violence. Finally, a culturally offensive incident that occurs outside the joint operations area but resonates personally may become cause for an attack. However, civilian casualties attributed to U.S. or partnered forces are often the greatest motivation for reactionary attacks. Leaders and Soldiers must be aware that such events may trigger an attack and adjust their protective posture to mitigate the increased risk.

Desecration of Religious Materials Inspires Attack

On February 12, 2012, Afghan National Police Lieutenant Abdul Saboor killed two U.S. officers at the Ministry of the Interior in Kabul, Afghanistan. He shot both officers in the head while they worked at their desks in the ministry. Although the office doors were equipped with cypher locks, the officers enjoyed cordial relations with their Afghan counterparts and left their door open to encourage others to enter. After the incident, Lieutenant Saboor claimed that he attacked the officers in response to an inadvertent Koran burning that occurred earlier in the year. The attack resulted in the International Security Assistance Force Afghanistan (known as ISAF) withdrawing its advisors from the Ministry of the Interior for several weeks. Lieutenant Saboor's attack may have been prevented had the officers followed proper force protection protocols by closing and locking their office door.

CRIMINAL

1-19. Criminal attacks occur when an FSF member is at risk of being discovered in the planning or commitment of a criminal act. An FSF member may also attack in an effort to safeguard an ongoing criminal enterprise from discovery or interruption. Effective leaders and Soldiers understand that extreme corruption is a crime, and corrupt FSF members may turn to violence to protect corrupt practices or the benefits accrued from them. (See FM 3-39 for additional information on criminal threats and crime's effects on an operational environment.)

Corrupt Officer Attacks U.S. Air Force Advisors

On April 27, 2011, Colonel Ahmed Gul, an Afghan National Air Force pilot with over twenty years of military service, had a verbal dispute with his United States Air Force (USAF) advisors that resulted in the death of eight advisors and one U.S. civilian. The argument erupted when Colonel Gul was denied the personal use of government aircraft by his USAF advisors. After the argument became increasingly hostile, and the advisors refused to allow him to use the aircraft, Colonel Gul left the room. Upon return, he drew his service pistol, disarmed the USAF advisors, and proceeded to shoot and kill all nine personnel. Five Afghan National Security Force (known as ANSF) soldiers were wounded and one was killed as they fled by jumping out of windows to escape. A quick reaction force responded to the incident, but Colonel Gul committed suicide before it could neutralize the attack. The Taliban later claimed responsibility for the attack; however, no evidence of Taliban influence or cooperation was discovered.

This incident has characteristics of both a criminal and personal attack. The incident is criminal in that Colonel Gul was attempting to violate Afghan National Air Force regulations by using government aircraft for personal use, and he was so incensed by objections to this practice that he decided to attack eight USAF advisors. The incident is personal because it arose out of a verbal disagreement between U.S. Service members and foreign security forces (FSFs). Of the nine victims, four were majors and one was a lieutenant colonel. At the time, this single attack accounted for over half of all USAF deaths in Afghanistan.

Although it is difficult to discern when a dispute will evolve into an attack, had the USAF advisors recognized the escalatory nature of the disagreement and intervened by disarming Colonel Gul, the incident may have had a different outcome. It is also possible that Colonel Gul was offended by being countermanded by subordinate officers. In these instances, U.S. advisors should recognize the nuances associated with partnering between different ranks, and they should be sensitive to the potential for embarrassment and humiliation when senior FSF officers have disagreements with lower ranking U.S. advisors. If possible, these disagreements should occur behind closed doors and with as small an audience as possible.

ENEMY

1-20. Enemy attacks occur when a FSF member is influenced by, or is a member of, an enemy organization. This type of attack often occurs when conducting counterinsurgency operations, as an insurgent force may attempt to co-opt, infiltrate, or impersonate FSFs to gain and exploit access to U.S. forces. These attacks may also occur when FSF members believe the current security situation favors enemy forces, and they switch sides out of self-interest.

1-21. ***Co-option*** **is a process an enemy, insurgent, or terrorist organization uses for recruiting an existing foreign security force member**. Recruiting an existing FSF member is appealing as it may circumvent the initial screening and vetting required for new recruits. Recruitment may occur by or through ideological pressure, financial incentives, intimidation, or social ties. An enemy force may also co-opt FSF members by capitalizing on an existing grievance an individual may have with U.S. forces. Co-option can take a grander form in which accommodation or cooperation exists between entire FSF units and enemy or insurgent forces.

1-22. An enemy force may recruit potential attackers without completely co-opting them into an enemy or insurgent organization. This recruitment is often driven by financial incentives, not ideological underpinnings, as an enemy force may simply pay an FSF member to attack U.S. forces. This is perhaps the

most difficult threat to detect because an FSF member acting for financial gain may not show any behavioral indicators.

Taliban Co-opts Afghan Border Policeman

On November 29, 2010, Ezatullah Wazirwal, an Afghan border policeman, attacked U.S. Soldiers in Nangarhar Province. The Soldiers were training on a small arms range with an Afghan border police unit when the attack occurred. Wazirwal waited until lunch, when the Soldiers removed their personal protective equipment (PPE), to launch his attack. He fired on a group of Soldiers and killed six before he was killed by return fire. Wazirwal and his brother joined the Afghan border police three years earlier in response to Taliban actions in their home province. He even went so far as to relocate his family to an urban area to avoid Taliban intimidation. Wazirwal had an impeccable service record and demonstrated no indicators prior to the attack. However, he had recently returned from leave, and while at home he spent time with his uncles who had fought with the Taliban. It is believed that Wazirwal's family co-opted him to use his position of trust to attack U.S. forces. The proper wear of PPE and the use of armed security overwatch or guardian angels may have prevented or mitigated the results of this attack. Units are also encouraged to carefully observe foreign security force members for threat indicators after they return from leave.

1-23. In addition to co-option, an enemy force may infiltrate FSFs to gain access and conduct attacks. Infiltration occurs when an existing enemy fighter clandestinely joins an FSF through the standard recruitment process. However, infiltration removes a fighter from the enemy's ranks and puts that fighter at risk during recruitment, vetting, and training. As such, a successful infiltrator is likely to be much more competent and experienced than an average recruit and may be used in a more effective manner by an enemy force. Although infiltrators may still conduct singular attacks, they may use their experience and training to collect information on U.S. forces or to target senior leaders over time. Assessing the level of possible infiltration in an organization is difficult, as infiltrators will seek to remain undetected until they attack.

1-24. An enemy soldier may also impersonate an FSF member to gain access and attack U.S. forces. Impersonation occurs when existing enemy soldiers pose as FSF members to circumvent force protection or access control measures and gain access to U.S. forces or facilities. Enemy soldiers may simply dress in FSF uniforms and present counterfeit badges at access control points. Impersonation is often more effective and easier to accomplish than co-option or infiltration since FSF uniforms and identification credentials may be easily replicated. Co-option may accompany impersonation if actual FSF members assist an enemy with obtaining uniforms or badges. Impersonation rarely occurs without some level of facilitation, complicity, or awareness by FSF members. This facilitation may include providing an identification badge, escorting an individual onto a base, or simply knowing of the attacker's intentions to target U.S. forces. Biometric screening at access control points may prevent enemy forces from successfully impersonating FSFs and gaining access to U.S. forces.

GENERAL

1-25. An FSF attack may occur for reasons that do not easily fit within a single category. An underlying mental illness or drug addiction may cause an otherwise sound actor to attack. However, mentally ill people may exhibit many indicators before they commit an attack. These symptoms can include various psycho-social impairments including severe stress or anxiety. The most prominent symptoms include unwarranted angry outbursts, isolation, or dramatic changes in behavior.

1-26. Tensions within FSF rank structure may also serve as the motive for an attack. At times lacking a robust noncommissioned officer corps, an FSF may be plagued by tensions between officers and enlisted personnel stemming from inequality, disrespect, or a lack of pay. At worst, senior FSF officers may abuse, extort, or steal from their enlisted members, exploiting the trust necessary for a unit to function effectively. These issues may originate from (or be exaggerated by) tribal, political, or familial factions that compete

with each other for limited resources, power, or influence in a particular region. If U.S. forces fail to address these excesses, or are believed to be facilitating them, attackers may turn their frustrations against U.S. forces in the form of violence. Units operating in security environments where corruption is prevalent must recognize its potential to undermine leadership and cause an attack.

1-27. Disparities and tension may also exist between various branches of a nation's security apparatus, with friction rife among military, paramilitary, and police organizations. These conflicts may stem from the inequitable distribution of resources or equipment among the organizations. They may also arise out of jurisdictional disputes between organizations, with varying units competing to be the dominant force in an area or region. In these instances, it is imperative that U.S. forces proactively attempt to resolve the conflict by bridging the divide between disputing FSF units. Failing to do so may lead to animosity between FSF units being redirected against U.S. forces. If animosity exists between a partnered unit and another FSF organization, then units conducting SFA operations may be targeted for an attack simply by their association with the partnered unit. This is particularly true if an FSF unit believes U.S. forces show favoritism to their partnered unit while the other organization receives little assistance.

Attacker Motivated by Abuse

On November 2, 2009, an Afghan National Policeman in Helmand Province fired on International Security Assistance Force Afghanistan (ISAF) soldiers, killing five British soldiers and wounding six other ISAF members. The attack occurred immediately after a serious dispute with ISAF forces. The attacker escaped on a motorcycle and was not located during subsequent operations. Afterwards, it was learned that the policeman had been abused, sodomized, and sexually molested by a senior Afghan National Police officer that he believed was protected by the British soldiers. The policeman had also expressed frustration with inadequate and inconsistent pay.

Chapter 2

Foreign Security Force Threat Prevention and Response Framework

This chapter presents the FSF threat prevention and response framework. It provides tactics, techniques, and procedures (TTP) for units to prevent and defeat FSF threats in an expeditionary environment. Preventing and defeating these threats requires training, discipline, vigilance, and teamwork. Although it may be impossible to completely eliminate the threat posed by FSFs, the TTP herein are designed to protect units and Soldiers operating alongside multinational partners. These TTP compile the best practices captured from years of limited contingency operations.

FIVE FUNCTIONS

2-1. The FSF threat prevention and response framework consists of five functions: prevent, deter, defeat, exploit, and recover. Prevention and deterrence occur continuously, whereas the defeat, exploit, and recover functions occur once a threat evolves into an attack. Each function includes several components that, when applied in concert, better position the unit to prevent and respond to an FSF threat.

2-2. Prevention and deterrence are complementary functions that occur throughout operations. Prevention consists of the internal processes and behaviors employed by units to increase threat awareness and reduce the likelihood of an attack. Deterrence includes the active measures employed by a unit to discourage a potential attacker from acting and, should an attack occur, to reduce the consequences of the attack. Distinguishing between the two is a matter of perspective. Prevention should be understood from a unit or Soldier perspective; it consists of the behaviors, TTP, and practices designed to preclude an attack by inhibiting the emergence of a threat. Deterrence is best understood from an attacker's perspective. What practices will make FSF threats believe their attack will fail? This internal and external construct enables a comprehensive approach to threat prevention.

2-3. Conversely, the defeat, exploit, and recover functions occur sequentially. Defeat consists of the immediate response procedures executed to neutralize an attack and restore local security. The exploit function is transitional and consists of actions to collect information about the attack, consolidate lessons learned, and share this information with other units. Effective Soldiers apply lessons learned to prevent, deter, and defeat future threats. Exploitation and recovery may occur simultaneously; however, they serve different purposes. The recover function consists of the steps taken to regain trust and cohesion with the partnered FSF, resume pre-attack operations, and manage the wider consequences of an attack.

PREVENT

2-4. Prevention consists of internal processes and behaviors employed by units to increase threat awareness and reduce the likelihood of an attack. It promotes a unit culture conducive to working alongside FSFs and capable of detecting threats. As such, prevention seeks to deny a potential attacker the motive, will, or opportunity to attack. Prevention requires awareness, discipline, and teamwork to be successful, all of which can be developed through a comprehensive unit training program.

CULTURAL AWARENESS AND PROFESSIONALISM

2-5. Respecting the cultural norms of both partnered FSFs and the local population is a critical component of FSF threat prevention. Lessons from OPERATION ENDURING FREEDOM reveal that violating cultural norms can be a significant point of tension between U.S. Service members and FSFs. Soldiers are encouraged

to respect cultural norms that do not interfere with mission accomplishment or the safety and security of U.S. Service members. They must recognize that continually violating cultural norms will often prove more detrimental to mission success in the long term than the perceived security benefit gained by violating them in the short term. Cultural awareness training is an important first step to ensuring Soldiers understand and respect foreign cultures.

2-6. Leaders and Soldiers also maintain the utmost level of professionalism during all interactions with FSFs and the local population. This is particularly important when conducting SFA and counterinsurgency operations since frustrations inherent in these missions are often compounded by the challenges of cultural differences and language barriers. Failing to maintain professionalism only exacerbates tensions and may foster personal grievances that become the impetus for an attack. This principle applies to U.S. Service members' interactions with the local population as well. HNSF may take extreme offense to U.S. Service members' disrespect for the local population or disregard for cultural norms. This is a matter of pride for HNSF members; they may be humiliated and embarrassed when their U.S. partners fail to show respect to the local culture. Ultimately, maintaining professionalism is a leader's responsibility. Soldiers achieve professionalism by watching their leaders' example and by refusing to tolerate unprofessionalism or immaturity within the organization.

2-7. Key components of cultural awareness and professionalism include these behaviors:

- Avoid derogatory or vulgar language. Whether this language is directed at an individual, a nationality, or an ethnicity, it may be offensive to FSFs or the local population. This principle applies regardless of the perceived language barrier since common, repetitive, or emotional words and phrases are often quickly understood across cultures.
- Intervene early to resolve personality conflicts and disputes. Allowing personal animosity to build may lead to additional conflict that erodes cohesion between U.S. forces and FSFs. Leaders practice their conflict resolution skills to mitigate potential issues before they escalate.
- Avoid discussing potentially provocative or emotional subjects, such as politics or religion, in a critical or demeaning manner.
- Do not slander, disparage, or demean FSFs or the local population.
- Do not aggressively touch or assault FSF members during exercises or training.
- Always show gratitude for host-nation and FSF hospitality.
- Attempt to understand FSF and host-nation cultural sensitivities; if unsure, ask for clarification through an interpreter.
- Always treat FSF members as peers and partners. Avoid treating them as inferiors or subordinates.
- Always show proper customs and courtesies to senior ranking partners.
- Avoid correcting FSF leaders in public or in front of their soldiers.
- Manage personal disputes and disagreements in private.
- Treat FSFs with respect.

BUILD AND MAINTAIN RAPPORT

2-8. Effective rapport is a relationship between people founded on mutual trust, understanding, and respect. Establishing effective rapport with partnered FSFs can prove challenging but is often necessary for success during SFA or stability operations. This is largely because U.S. forces usually lack direct authority over FSFs and, instead, must rely on personal relationships to accomplish their mission. They establish effective rapport that allows them to motivate their partnered FSFs to achieve desired objectives despite their lack of authority.

2-9. Establishing effective rapport provides protection at multiple levels. Many cultures protect friends, and politeness is usually an important part of any culture. FSFs and the local population are much more likely to discuss difficult matters, such as suspicious individuals, with those they trust. Effective leaders emphasize and focus on building close and trusted relationships with partnered forces. They should approach partnered forces as peers and treat them with the same respect they would fellow Service members.

2-10. Building initial rapport with partnered FSFs may begin before Soldiers meet their FSF counterparts. Studying the culture, society, and military of the partnered force provides a foundation from which dialogue and a future relationship can be built.

2-11. Maintaining effective rapport over time requires demonstrating competence as a Soldier and advisor. Partnered FSF members must believe their U.S. counterparts to be professionally competent enough to provide sound advice. If an FSF member does not believe the partnered Soldier or advisor is competent, that FSF member may quickly lose the trust and confidence necessary to work effectively on a multinational team.

2-12. Maintaining effective rapport is also accomplished through leadership by example. Leaders demonstrate to their subordinates how to maintain rapport. They share sacrifices with the partnered force and respect, not only cultural norms, but the opinions, concerns, and beliefs of the FSFs they partner with. Given the frustrations inherent in cross-cultural advising, leaders patiently work with their FSF counterparts and take the time to explain the reason and intent behind activities the FSFs may not understand. Soldiers avoid setting different standards for themselves and their partnered forces; they act as their leaders act. Maintaining effective rapport does not compromise force protection, rules of engagement (ROE), or operations security. Leading by example also reinforces competence.

2-13. Maintaining effective rapport may also require compromising with FSFs. Seeking compromise may encourage FSFs to take a personal stake in mission success or may be necessary to prevent FSFs undue humiliation or embarrassment. Achieving compromise becomes easier when partners build relationships on mutual trust and the reciprocal respect shown between professionals, regardless of nationality.

2-14. An important part of building and maintaining rapport is including partnered FSFs in patrol briefs, debriefs, and after action reviews (AARs). However, leaders ensure that including partnered FSFs in these forums does not violate force protection protocols or operations security.

2-15. Soldiers avoid forcing their partnered FSFs into action, as this may jeopardize existing rapport or become the impetus for greater conflict. Soldiers discuss disagreements in private and avoid engaging in a public disagreement or dispute with their FSF counterparts. Instead they find a way to encourage or motivate FSF members to participate in the desired action.

2-16. Building and maintaining rapport with FSFs is a deliberate activity that requires engagement and planning. Successful units attempt to engage with their partnered FSFs outside of operational requirements. This can include activities like sharing meals, participating in or watching sporting events, and joining in holidays or celebrations. This does not mean that units should disregard force protection or FSF threat prevention protocols during these events. Instead, units incorporate threat prevention protocols into rapport building events.

MAINTAIN ACCOUNTABILITY

2-17. U.S. forces advising or assisting FSFs maintain accountability of their weapons, munitions, and uniforms to prevent a potential threat from using these items in an attack. Enemy forces can use U.S. or FSF uniforms to impersonate friendly forces and gain access to U.S. bases or facilities. Soldiers and FSF members return non-serviceable uniforms to the unit supply officer for proper disposal. The supply officer follows standard operating procedures (SOPs) to discard those uniforms. SOPs specify that units never discard uniforms locally. FSFs that lack a system for exchanging or returning non-serviceable uniforms should destroy them.

2-18. Leaders and Soldiers also maintain accountability of their fellow Soldiers and team members. Although most attacks involve violence, an FSF member may attempt to capture a U.S. Service member or civilian. The unit, squad, and team regularly maintain accountability during all partnered operations, exercises, and engagements. A resilient communications plan supports accountability by ensuring Soldiers maintain contact with their leaders or team members. This plan includes primary, alternate, contingency, and emergency means of communications.

2-19. Soldiers operate in pairs or teams at all times to prevent becoming isolated and susceptible to capture. Team members remain in visual contact with each other while also maintaining a safe interval. They develop a habit of covering each other's flanks and observing entryways and avenues of approach. Team members must maintain situational awareness for each other and be ready to rapidly react to an attack. Leaders enforce the use of pairs and teams during mundane or routine activities like KLEs, physical training, or when working

in combined command posts. Leaders ensure that teams can support each other as much as possible, even if only as an immediate response force.

2-20. U.S. forces advising and assisting HNSF must also maintain awareness of HNSF members who have taken extended periods of leave or have gone absent without leave. These soldiers may have been co-opted by enemy, insurgent, or terrorist groups, and they may present a threat to U.S. forces upon their return. Leaders alert U.S. forces when these soldiers return to their units. HNSF that return after prolonged absences may require observation or investigation to determine whether they have been co-opted by enemy forces. Commanders may revoke their access to U.S. bases or facilities until this determination is made.

KNOW THE ENVIRONMENT

2-21. An important part of detecting FSF threats and preventing an attack is knowing the physical and human environment. The physical environment includes natural and man-made terrain, including the layout of buildings, compounds, and villages. The human environment consists of FSF members with whom units partner on a regular basis, FSF leadership, and key civilian leaders in the unit's area of operations (AO). It may also consist of FSF associates or civilian employees regularly present in FSF bases or facilities. Awareness of the human environment and physical terrain enables Soldiers to establish a baseline for their surroundings. A baseline is the sum of conditions normally encountered in a certain area or among a population. Once established, this baseline helps Soldiers detect anomalies, or indicators, of a potential FSF threat.

2-22. Aside from regular interaction and partnership, units can develop aids to help Soldiers understand the population in their environment. Biographical cards, with pictures and background information on the FSF members with whom Soldiers regularly interact, can assist new units or Soldiers as they develop a baseline for their AO. These cards can provide context and facts on their FSF partners so Soldiers can understand, engage with, and build rapport through dialogue. The cards also help Soldiers to quickly distinguish between the FSF members they regularly partner with and new or unrecognized FSF members. A biographical card on an FSF partner may include the following:

- Picture.
- Name (with a pronunciation aid).
- Rank.
- Unit.
- Position.
- Additional duties.
- Ethnicity.
- Age.
- Place of birth.
- Languages and fluency levels (written and spoken).
- Education level.
- Religion.
- Stance on U.S. forces (pro, against, neutral, or unknown).
- Phone numbers (personal and office).
- Email.
- An assessment of the FSF member's competence, loyalties, and position towards U.S. forces.
- Notable engagements.
- Previous incidents of concern.

2-23. Knowing the physical environment requires establishing a baseline awareness of the terrain and then regularly referencing that baseline to identify changes or discrepancies. Soldiers look for changes from day-to-day or previous visits and question the significance of noticeable changes. They may question significance by asking these questions:

- Could a threat use the changes to attack U.S. forces?
- Are the changes indicative of an FSF threat?

Examples of physical changes that can indicate a threat include different ingress and egress routes at FSF bases or denied access to previously utilized defensible areas within an FSF compound. Leaders identify and prompt Soldiers to recognize noticeable changes to their surroundings. This guidance and mentoring helps Soldiers develop an environmental baseline, scan for anomalies, and then assess conditions for the existence of a threat.

2-24. When replacing a U.S. unit already partnered with FSFs, an important first step to knowing both the physical and human environments is a thorough relief in place. The relief in place includes both the U.S. unit and the partnered FSF to help establish a relationship between the new forces. Departing units share FSF threat information, intelligence, and experiences during the relief in place; they also identify and discuss potential vulnerabilities or suspect individuals.

DETECT FSF THREATS

2-25. In tactical operations, *detection* is the perception of an object of possible military interest but unconfirmed by recognition (JP 3-11). As a continuous process, detection requires the active participation of all Soldiers. A systematic approach to detection helps units interpret complex and ambiguous environments. Soldiers constantly assess their environment and FSF partners to recognize threats not detected by traditional screening methods. Because of this, detection rests on vigilance and establishing a baseline for both the physical and human environments. Soldiers can then assess changes or anomalies to this baseline as potential threat indicators. Recognition and timely reporting of threat indicators enables preemptive action and can be used to drive intelligence at all echelons. Staffs ensure the rapid dissemination of threat warnings across the force to promote a shared understanding of the environment.

2-26. Leaders and Soldiers aware of the indicators associated with an FSF threat are better positioned to detect, deter, and defeat an attack. Identifying a threat early allows leaders to take proactive steps to neutralize the threat or better protect the unit. Threats often present numerous warnings before an attack. All leaders ensure their subordinates know threat indicators and reporting procedures. An indicator is a behavior, action, or event that precedes an attack. Threat indicators can be environmental, physiological, or behavioral.

Environmental Indicators

+ 2-27. The environment consists of the sights, sounds, smells, feel, and mood of a particular area. The disposition of the local population towards U.S. forces is also an important component of the environment. Once Soldiers have established a baseline for their environment, they can more easily identify environmental anomalies indicative of a potential threat. This includes the manner in which groups express themselves and the art, symbolism, and customs common in a particular area. Flags, posters, and graffiti are all potential indicators of a changing environment. An environmental anomaly or change to an established baseline may be the only indicator of a pending attack. Other environmental shifts can include sudden changes to normal routines, patterns, or behaviors by the local population, or the presence of abnormal activity such as—

- A usually noisy and raucous place is quiet and calm.
- A typically crowded area is empty.
- An area that normally contains people of all ages and sexes is devoid of a certain demographic (for example, the absence of women or children).
- Civilian attitudes towards U.S. Service members differs markedly from usual (hostility or avoidance).
- Unfamiliar vehicles or individuals are present.
- Anti-American graffiti is noticeable on walls and buildings.
- FSFs or local workers fail to report to work.
- Newspaper or radio broadcasts are markedly critical of U.S. forces or policies.
- Businesses or shops normally open are closed.
- Film crews or cameramen are noticed in the area.

Physiological Indicators

2-28. Physiological indicators are the body's observable and measureable reactions to stress. They are the body's chemical response to external stimuli and quite difficult to suppress. A threat preparing to attack will likely be under a great deal of stress and may present physiological indicators. Physiological indicators include excessive sweating, shaking, flushing, or having dilated or constricted pupils. Attackers may also use illicit drugs to enhance their stamina, focus, or mental state to carry out an attack. Either stimulants or depressants, these drugs often produce a physiological response. Diligent Soldiers observe FSFs for lethargy, apathy, excitability, or belligerent behavior, as these may indicate attackers under the influence of narcotics. Physiological indicators may be particularly noticeable in an attacker who has no plan for surviving an attack, such as a suicide bomber.

Behavioral Indicators

2-29. Behavioral indicators are changes to an individual's emotional state, social interactions, or expressions that may indicate a potential threat. Behavioral changes are the easiest to detect and intervene. Often Soldiers observe behavioral changes as the first indicators of an emerging FSF threat. While a single indicator may not warrant action, Soldiers still report observed indicators to their chain of command. Sometimes those Soldiers need to act quickly to mitigate a threat when multiple indicators are present. A threat may gradually evolve from minor behavioral changes to more alarming or observable indicators as a threat grows closer to committing an attack. Observable indicators allow Soldiers and leaders the opportunity to intervene before the threat evolves into an attack. As such, behavioral indicators are classified into three escalatory categories.

Category 1

2-30. Soldiers closely monitor FSFs exhibiting category 1 indicators. Soldiers ask these FSFs about potential changes to their personal lives and inform fellow U.S. Service members of the behavioral changes. Soldiers include these indicators in mission debriefs and report them to the chain of command. Category 1 indicators include—

- Complaining about other nationalities, ethnicities, or religions.
- Advocating violence beyond the accepted norm.
- Shifting abruptly in behavior, personality, or performance.
- Desiring control or authority beyond the scope of their duty position.
- Expressing frustration with U.S. forces.
- Demonizing others.
- Lacking positive identity with the unit or country.
- Becoming suddenly reclusive and withdrawn when others are engaged and involved.
- Abusing drugs or alcohol.
- Intimidating, being belligerent, harassing, bullying, or behaving aggressively.
- Showing signs of depression.
- Encouraging disruptive behavior or disobedience.
- Making statements indicating desperation over family, financial, or other personal problems.

Category 2

2-31. In addition to the measures applied for FSF exhibiting Category 1 indicators, Soldiers refer individuals exhibiting Category 2 indicators to their chain of command and notify the U.S. intelligence staff. Individuals demonstrating Category 2 indicators may require close observation and supervision. Category 2 indicators include—

- Defending radical groups or ideologies.
- Speaking about seeking revenge.
- Associating with extremist individuals or groups.
- Demonstrating intolerance for other nations, ethnicities, groups, or religions.

- Being personally connected to a host nation or FSF grievance with a U.S. unit, individual, policy, or operation.
- Isolating self from unit, family, or friends.
- Possessing extremist propaganda or reading material.
- Expressing approval for the use of violence to resolve a personal or professional problem.
- Bragging or joking about belonging to a terrorist or enemy organization.
- Viewing websites that promote terrorist acts or acts of defiance to undermine legitimate authority.
- Stating delusional or paranoid ideas.

Category 3

2-32. Category 3 behavioral indicators are the most severe. They require immediate action to address the threat. Soldiers deny these individuals access to weapons. Leaders direct that Soldiers constantly supervise or detain such individuals to prevent them from attacking. Category 3 indicators include—

- Advocating the use of unlawful violence or force to achieve political, religious, or ideological goals.
- Shifting suddenly from upset to normal behavior or from normal to upset behavior.
- Making suspicious travels or having unauthorized absences.
- Collecting excessive and unauthorized munitions or weapons.
- Expressing open hatred for U.S. forces.
- Expressing a sudden interest in U.S. headquarters, facilities, or living quarters.
- Attempting to gain unauthorized access to U.S. headquarters, facilities, or living quarters.
- Making open threats or gestures to U.S. forces.
- Making statements identifying with, or expressing sympathy for, enemy or extremist organizations.
- Espousing extremist ideological rhetoric.
- Attempting to recruit others to an extremist or subversive cause.
- Being repeatedly unwilling to comply with rules and regulations regarding weapons handling, force protection procedures, or access control measures.
- Expressing openly a hatred of American society, culture, or government.
- Obtaining sudden and unexplained wealth or a significantly improved financial situation.
- Expressing a duty to engage in violence against U.S. forces.
- Displaying evidence of training with or attendance at terrorist or enemy training facilities.
- Identifying with family members or other close associates with ties to the enemy or extremist organizations.
- Posting online comments that promote violence against the United States or U.S. forces.
- Having a physical altercation with a U.S. Service member or civilian.
- Damaging or destroying U.S. or FSF equipment or property.

2-33. Every Soldier has a duty to report observed behavioral indicators to unit leaders, intelligence staff members, and fellow Service members. Leaders ensure that FSF partners are aware of the potential threat indicators and know how to detect a threat within their ranks. In a multi-partner environment, units provide training to those forces that lack a mechanism for identifying and reporting threats.

Predictive Classification Concept

2-34. The predictive classification concept provides a model for how indicators may evolve and manifest over time. Figure 2-1 on page 2-8 presents the predictive classification concept. The concept demonstrates how an FSF threat may be detected through routine data and, after focused observation, additional indicators or behaviors may reveal a potentially dangerous threat. As such, it is a useful tool for determining the severity of a threat and discerning an actual threat from an individual experiencing the frustrations of combat.

2-35. Progressing from data to behaviors, the predictive classification concept presents a comprehensive approach to threat detection and classification. For example, a commander may notice an FSF member having a cultural misunderstanding with U.S. forces. Although not an actionable indicator, this incident should warrant further observation. Later, when a Soldier observes the same individual repeatedly arguing with U.S. advisors, the likelihood that that individual is a threat increases and action may be warranted. Finally, when a Soldier observes the individual making threatening gestures and comments about U.S. forces, the unit steps up to take action as that individual's behavior indicates an imminent threat. Individuals may display threat indicators for many reasons, only some of which involve the intent to attack. The predictive classification concept provides Soldiers a means of distinguishing unusual behavior or the stresses of combat from a genuine threat.

2-36. The data that form the basis of the predictive classification concept are generally open information and may be available in many forms. Statements to fellow FSF members, correspondence, reading material, and access attempts are all forms of data that units can use to identify a potential threat. However, the model does not suggest that all detection begins with data. Sometimes a Soldier initially detects an FSF threat through indicators or behaviors, with supporting data identified after the staff conducts an investigation. Commanders report the discovery of questionable data to the intelligence staff.

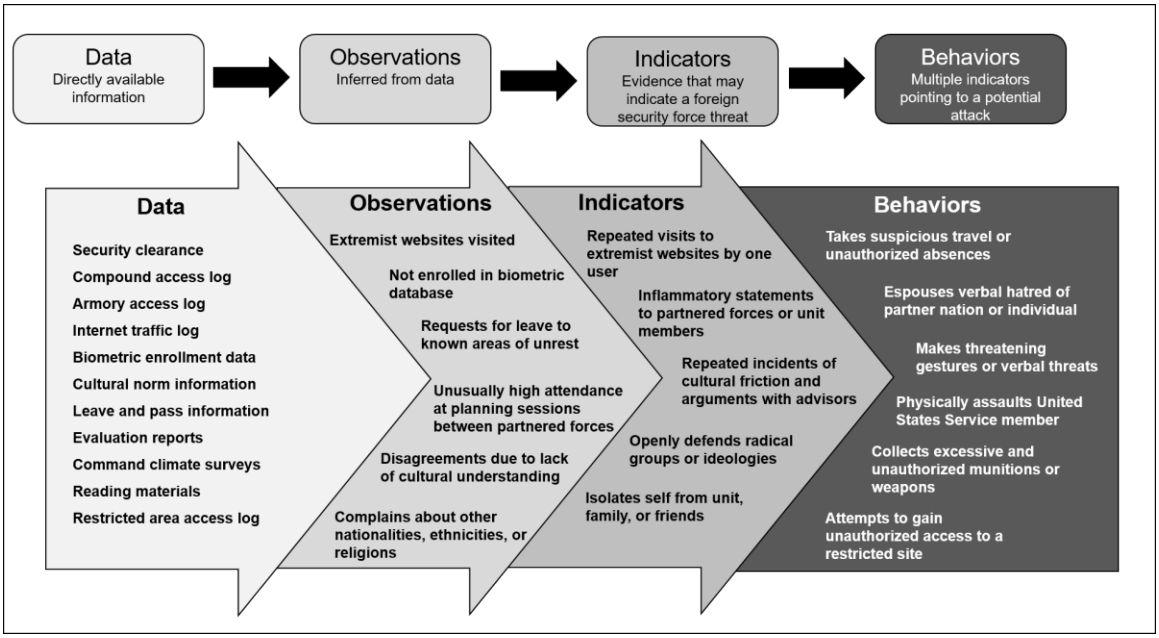


Figure 2-1. The predictive classification concept

ASSESS THREAT, VULNERABILITY, AND RISK

2-37. *Risk management* is the process to identify, assess, and control risks and make decisions that balance risk cost with mission benefits (JP 3-0). Incorporating FSF threat considerations into operational planning and preparation requires comprehensive risk management. The potential for an FSF attack exists during all combined operations, and leaders must continually exercise risk management to prevent, deter, and defeat the FSF threat. Risk management requires identifying and assessing the threat, criticality, vulnerability, and ultimately risk. As a continuous process, it results in the implementation of control measures to actively combat the FSF threat and protect U.S. forces while enabling mission success.

Types of Assessments

2-38. Units use four assessments: threat, criticality, vulnerability, and risk. An FSF member with the intent to attack may possess motive and capability, but an attack requires opportunity to be successful. Soldiers

identify intent and capability through threat assessments, but they identify opportunity using a vulnerability assessment.

Threat Assessments

2-39. Threat assessments focus on an enemy force's capability and intent. Intelligence staffs can provide intelligence on potential threats for units in their AO based on information about their partnered FSF. Units may also collect threat information from the local population or trusted FSF members. However, for this information to be actionable, units and Soldiers working alongside FSFs must report it to the intelligence staff.

Criticality Assessments

2-40. Criticality assessments help commanders identify mission-essential vulnerable areas and potential high-risk targets. Criticality assessments for units executing tactical operations focus on identifying the most critical (decisive) aspect of the mission that must be protected and on determining the specific friendly forces most important to mission success. Criticality assessments during SFA and stability operations also consider FSF security requirements, the local government, and the civilian population. Units use criticality assessments to initiate a vulnerability assessment. Command posts, local police stations, or government offices all illustrate potentially mission-essential vulnerable areas.

Vulnerability Assessments

2-41. The protection cell staff performs vulnerability assessments to determine the magnitude of a threat against personnel, an installation, a unit, an exercise, a facility, or some other site. It identifies the areas of improvement necessary to withstand, mitigate, or deter attacks.

2-42. Preventing FSF attacks requires mitigating identified vulnerabilities. Vulnerability is the risk variable over which commanders can exert the most control. A proper vulnerability assessment enables commanders to plan appropriate defensive countermeasures or change the operational parameters to reduce vulnerability to an acceptable level. However, this is particularly challenging when assessed against the FSF threat, as an attacker often relies on the element of surprise to be successful. Because of this, a vulnerability assessment must seek to identify how, when, and where a threat can achieve local surprise and how to prevent it.

2-43. A vulnerability assessment identifies a vulnerable friendly unit and the specific threat weapon or tactic it is vulnerable to. This weapon-target pairing is critical to understanding a unit's vulnerability. Some units may be more vulnerable than others. The vulnerability assessment considers unit protection levels and their operational profiles. For example, a provincial reconstruction team or elements from a security force assistance brigade may routinely operate separate from the main body, possibly making them more susceptible to an FSF attack.

2-44. A vulnerability assessment anticipates environmental triggers that could motivate an FSF member to attack. The transition from vulnerability to attack may be event driven, time oriented, or location driven. This is the most difficult part of a vulnerability assessment, and it requires a thorough understanding of the operational environment (OE) and the population. Assessments incorporate the expertise of experienced small-unit leaders to determine the points in time and space where and when a unit is most vulnerable. Such attacks are often reactionary, and they may be triggered by local, regional, or international events. Civilian casualties, significant U.S. policy decisions, or culturally offensive incidents may all trigger reactionary attacks. Attacks may also be seasonal or associated with certain holidays or historically significant dates.

Risk Assessments

2-45. Risk assessments examine threats, criticality, and vulnerability to gauge probability and impact. Commanders use risk assessments to identify and implement control measures to reduce the likelihood and mitigate the consequences of an attack. Commanders, staffs, and subordinate leaders understand an assessment's value in identifying and mitigating risk both in fixed locations and while operating. Examples of control measures designed to mitigate the FSF threat include physically separating U.S. and FSF living quarters at shared bases, identifying defensible rally points at frequently visited sites, and using guardian angels during KLEs or other high-profile events. Other control measures include communication and

consensus building with partnered forces, physical security measures at entry control points, and the use of screening procedures when granting access to U.S. facilities.

Note. An important part of risk management during partnered operations is ensuring that the control measures implemented to prevent, deter, or defeat an FSF threat do not place Soldiers at undue risk. If control measures designed to defeat an FSF threat inadvertently put Soldiers at greater risk through exposure, isolation, or a lack of adequate resources, leaders intervene by carefully weighing the mission's importance against the potential risk to forces.

Biometric Screening and Verification

2-46. Relying on a threat to display suspicious behavior before an attack cedes initiative to the enemy. Instead, Soldiers have other measures available they can use to prevent FSF attacks. Biometric screening can be used to detect and prevent impersonation and infiltration, as the data used to verify an individual's identity cannot be altered. *Biometrics* is the process of recognizing an individual based on measurable anatomical, physiological, and behavioral characteristics (JP 2-0). Effective commanders take advantage of available biometric systems and databases to positively identify FSFs granted access to U.S. installations and personnel. Unfamiliar or newly arrived FSFs undergo biometric screening, credentialing, and badging before a unit grants them access to U.S. facilities, units, or personnel. Identification badges created by biometric devices are more difficult to counterfeit than locally produced alternatives. Failing to screen, credential, and badge FSFs affords enemy forces an opportunity to infiltrate U.S. bases using false identification. (See ATP 2-22.85 for more information on utilizing biometric screening with FSF partners.)

2-47. Biometric data collection is an important component of the overall intelligence, targeting, and force protection architecture. When properly analyzed, the data form a system that enables force protection personnel to identify and defeat threat networks across the joint operations area. Locally, it enables Soldiers to confirm the identity of those with whom they partner and detect impersonators or infiltrators.

2-48. Biometric screening is particularly important when conducting HNSF recruitment. During initial enrollment, units screen data collected from applicants against an existing database that contains biometric data or forensic evidence associated with confirmed hostile actors or enemy actions. If a unit detects a match, U.S. forces can deny, detain, or arrest the individual attempting to join the HNSF. However, for this to occur, leaders must ensure that units regularly update and synchronize biometric devices and data with their respective databases or networks. Collecting data without sharing or synchronizing does little to defeat the FSF threat. (See ATP 2-22.82 for more information on using biometrics to place suspect individuals on watch lists.)

2-49. In addition to being a critical step during initial vetting, intelligence professionals can use the data collected during biometric enrollment to identify threats that may not have been radicalized or disillusioned during their initial enrollment. This occurs when forensic evidence gathered at the scene of an attack is uploaded into the biometric database and matched against an FSF member.

Disseminated Warnings and Shared Information

2-50. Rapid dissemination of threat warnings ensures that all personnel are informed of credible threats identified by the intelligence community. On receipt of threat warnings, commanders reassess vulnerabilities and residual risks and, where necessary, take action in accordance with their respective TTP and SOPs. Leaders ensure that staffs disseminate warnings throughout their units.

2-51. Commanders ensure that staffs share FSF threat information collected by their unit both within and outside their organization. Commanders and their staffs are often the primary means of information exchange laterally. They ideally share information about potential threats with units working in their AO or operating alongside the FSF unit with which they typically partner. Mission debriefs and AARs often contain valuable information that units need to share with other organizations and the intelligence staff for further analysis and dissemination.

2-52. At the theater level, commanders and staff share information with HNSF when U.S. forces release their detainees. Providing the identity of these detainees to the host nation may prevent the detainees from infiltrating the HNSF once released.

2-53. In addition to information about potential threats, commanders and staffs share FSF threat prevention and response TTP with other organizations. Outside the joint operations area, the Center for Army Lessons Learned is the Army's central repository for lessons learned. This center collects, analyzes, and rapidly disseminates applicable TTP across the force. Commanders and investigating officers provide relevant lessons learned to the Center for Army Lessons Learned. They can upload lessons learned to the Center for Army Lessons Learned at https://call2.army.mil or to the Joint Lessons Learned Information System at www.jllis.mil.

Enforced Access Control Measures

2-54. Rigorous enforcement of security measures is essential to denying access to those not authorized to enter U.S. installations or facilities. Threats may try to infiltrate facilities by impersonating FSF or U.S. Service members. To prevent infiltration, U.S. personnel enforce security measures and access protocols at all times. This includes practices such as the use of badges to access U.S. or combined compounds and bases. Units may employ biometric toolkits to produce access or identification badges for vetted FSF members. The Biometric Automated Toolset System and the Hand-held Interagency Identity Detection Equipment systems create badges that are difficult to counterfeit. Security forces thoroughly search FSFs who lack proper badges yet seek access to U.S. installations or facilities. After security forces search the FSF member for weapons, munitions, or contraband, they allow the member entry only after the local security or intelligence officer clears them.

2-55. Maintaining accountability of badges and access credentials prevents lost or stolen badges from being used by enemy forces to gain unauthorized access. This applies to U.S. Service member's badges, badges generated by U.S. forces for FSF, and FSF-generated badges. The unit registers lost or stolen badges in an access control database and notifies security personnel. Checkpoint personnel notify security personnel, if an individual presents such a badge at an entry control point. Checkpoint personnel deny entry and detain the individual presenting the badge for questioning.

2-56. FSF members only receive access to locations on U.S. facilities or bases where their presence is required. Units take particular care to ensure that FSF do not have open access to U.S. forces' living quarters, command posts, or headquarters where sensitive information or leaders may be present. If required access to one of these locations, an armed U.S. Soldier escorts the FSF member at all times.

2-57. Although access control measures should ensure that only authorized personnel enter restricted locations, units should not employ them as stand-alone security measures. All personnel remain alert to the possibility that an unauthorized person may gain access to a location where U.S. personnel work or live. It is incumbent on all Soldiers to remain vigilant and have the courage to challenge and report anyone who appears out of place. Each facility, compound, or base develops and publicizes reporting procedures so tenants know which persons have authorized access and how to report suspicious activity.

2-58. U.S. and combined facilities, bases, and compounds conduct periodic security patrols to ensure unauthorized FSFs have not gained access. These internal patrols verify the identity and access credentials of all FSFs on the facility. Security patrols disarm and detain FSFs without authorized access for further questioning. Units execute security patrols before high-profile events such as KLEs, ceremonies, or training academy graduations. These patrols not only verify that the FSFs present are authorized, but also that the location is free of unauthorized weapons, munitions, and improvised explosive devices.

2-59. While security always trumps cultural sensitivity, some procedures, such as searching or disarming FSFs at entry control points, may be modified for recognizable FSF leaders to prevent embarrassment or disrespect. Ultimately, a commander determines any modifications to the force protection condition or access control measures.

DETER

2-60. *Deterrence* is the prevention of action by the existence of a credible threat of unacceptable counteraction and/or the belief that the cost of an action outweighs the perceived benefits (JP 3-0). Deterrence complements prevention and occurs throughout operations. Deterrence relies on actively discouraging an enemy from attacking by demonstrating U.S. preparations and the ability to rapidly defeat an attack. Deterrence is not possible without preparation, as it requires making individuals and units difficult targets to attack. It also positions units to better respond and defeat an attack should it occur. Deterrence starts with leaders. Leaders demonstrate the vigilance and discipline required to deter an FSF threat and ensure friendly units employ appropriate protection protocols in accordance with local policies and the threat level. Deterrence consists of three components: force protection, posture, and defense in depth.

FORCE PROTECTION

2-61. *Force protection* refers to the preventive measures taken to mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities, and critical information (JP 3-0). Force protection measures present a visible posture, presence, and profile that can deter both opportunist and planned attacks. These measures provide a mix of direct protection (such as armed guards and physical security measures) and indirect protection (such as training and rehearsals). Indirect protection mitigates threats by decreasing the likelihood an attack will be successful. As such, force protection is a critical component of deterrence.

2-62. Understanding FSF threats and their potential courses of action (COAs) enables commanders to develop tailored protective measures that address the most likely and most dangerous threats. Based on the criticality, vulnerability, and risk, units can implement specific force protection measures that will reduce unit vulnerabilities to the threat COAs. By developing defensive measures tailored to the specific threat COAs, commanders can provide relevant and focused force protection measures.

2-63. Effective staffs continually assess and occasionally adjust force protection measures to prevent complacency and deny enemy forces the ability to easily target U.S. forces. Such adjustments include avoiding set patterns, adjusting meeting locations, and changing routes used to move to and from engagements and recurring events.

2-64. Implementing specific, relevant, and focused force protection measures, including policies regarding personal protective equipment (PPE) and arming status, is a central element of FSF threat deterrence. These policies address whether FSFs have access to weapons while on U.S. or combined bases. They also provide a framework for the status of both U.S. and FSF weapons in accordance with the threat and the force protection condition level. (See ADP 3-37 for more information on force protection and the protection warfighting function.)

POSTURE

2-65. Posture, presence, and profile are critical to deterring FSF attacks. Posture is a unit's readiness to prevent and defeat an attack. Perception, garnered by demonstrated ability, plays an important part in establishing a unit's posture. Posture determines whether a threat perceives a unit as easy or difficult to attack. A disciplined unit, whose Soldiers are trained and ready to prevent and respond to an attack, may deter an enemy from attacking.

2-66. A combination of vigilance and discipline is critical in presenting a hard target to FSF threats. Discipline requires a commitment by all Soldiers to operations security and force protection protocols. Vigilance demands that Soldiers remain aware of their surroundings and pay attention to the attitudes and behaviors of FSFs and the local population. These attributes establish the organization's posture and contribute significantly to whether the unit is viewed as susceptible to an attack.

2-67. Weapon status and arming policies are critical components of a unit's posture that directly affect its ability to deter potential threats. Arming policy directives mitigate risk based on an identified vulnerability or threat. Elevating a unit's weapon's status or arming policy can also project the appearance of a hard target. Although often directed by higher echelon headquarters in accordance with the force protection condition

framework, adherence to the prescribed weapon status and arming policies presents the appearance of a disciplined and ready unit.

2-68. Wearing PPE not only ensures the safety of U.S. Service members, but it is also a key component of a unit's posture. Although often used to refer to the protective equipment worn by Soldiers to operate in a hazardous or contaminated environment, PPE includes equipment like helmets and body armor. Soldiers operating alongside FSFs in an expeditionary environment wear their prescribed PPE in accordance with local or theater policy. This helps the unit maintain its image as a hard target while also protecting Soldiers from the consequences of a potential attack. Commanders take special care when downgrading the wearing of PPE during KLEs or similar events. Unless performing their duties covertly, guardian angels and security personnel maintain their prescribed PPE through the duration of their duties.

DEFENSE IN DEPTH

2-69. Maintaining an active, layered defense is the most important step a unit can take in deterring and defeating an FSF attack. Vigilant Soldiers, working in pairs or teams and tasked with maintaining a piece of the security or protection infrastructure, not only discourage an enemy force from attacking but position the unit to rapidly respond to and defeat an attack. The defense in depth framework primarily applies when units execute SFA or stability operations at a combined base, FSF compound, or host-nation location. However, elements of a defense in depth can be integrated into the larger force protection framework at U.S. bases or compounds frequented by FSFs.

2-70. The defense in depth framework consists of five layers: external security, mobile security, internal security, a reserve, and guardian angels. A noncommissioned officer, either a team leader or squad leader, leads and supervises each layer. The patrol leader has responsibility for overall security and mission accomplishment. If the patrol leader is engaged with other mission tasks, units may use a sergeant of the guard to manage the overall security framework. Each layer should have the ability to communicate with the rest of the patrol, and Soldiers should always maintain visual contact with at least one other member of the security force. Units periodically rotate guards to prevent complacency and fatigue.

2-71. External security consists of the security element charged with protecting the compound, facility, or site from external attack or compromise by an FSF threat. Due to operational constraints, this layer may be integrated with FSFs; however, U.S. forces present at all entry control points ensure FSFs enforce proper access control measures while U.S. personnel are present. The external security layer guards against infiltration and impersonation, ensuring that FSFs seeking access to the site are vetted prior to entrance. Effective U.S. forces observe the external environment for anomalies or signs of an attack, such as the absence of women and children or the presence of a cameraman observing the site.

2-72. Mobile security consists of teams assigned to patrol within a compound who observe for indicators of a potential FSF attack. These teams observe FSFs for suspicious activity and weapon status violations while also guarding against FSFs gaining unauthorized entry to sensitive areas within a compound. Mobile security patrols operate in pairs or teams, and they sometimes relieve other elements of the security infrastructure to prevent complacency. The sergeant of the guard or security force noncommissioned officer in charge may be a member of the mobile security element to simultaneously monitor the unit's overall security posture and ensure appropriate work and rest rotations.

2-73. Internal security consists of Soldiers assigned with guarding a sensitive area within a compound to prevent unauthorized individuals from gaining access and attacking potentially vulnerable U.S. forces or leaders. As FSF threats often target U.S. forces when they are advising or meeting with their partners, units position internal security forces in a location where they can effectively neutralize a threat before it gains access to the building or room in which the engagement is occurring.

2-74. If available, the patrol leader may designate assigned personnel to form a reserve or quick reaction force capable of responding to an FSF attack or other contingency. This team can rapidly respond and defeat an attack. Team members wear or have their PPE readily accessible, have their weapons at the ready, and maintain communication with the rest of the security force throughout the operation. Units position the quick reaction force or reserve element where it can best respond to a threat without disrupting the operation or offending the FSFs. Commanders can also use this element to support other security force members should

they identify a threat. The quick reaction force or reserve element can assist with de-escalating, disarming, searching, and detaining a suspected FSF threat. The defense in depth framework is presented in figure 2-2.

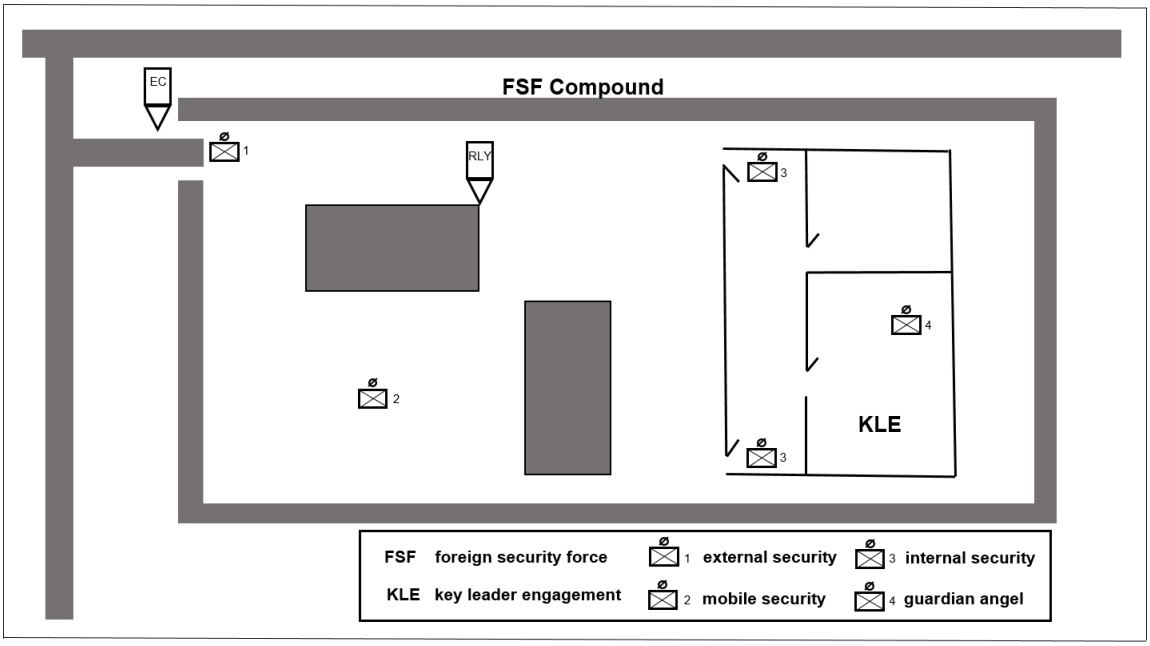


Figure 2-2. Defense in depth

GUARDIAN ANGELS

2-75. Similar to a personal security detail, guardian angels comprise the innermost layer of security for U.S. forces conducting FSF engagements, training events, or SFA operations. Guardian angels are designated, armed U.S. Service members who protect key leaders or other personnel who may be vulnerable to an FSF attack. They may operate as individuals, pairs, or small teams to protect individuals who, because of their status or mission requirements, are particularly exposed to an attack. Guardian angels provide close security overwatch during KLEs, high-profile meetings, or training events. They avoid downgrading their PPE and maintain their weapons in a ready status in accordance with local policy and regulations. Aside from presenting a strong deterrent, guardian angels provide an immediate response mechanism to neutralize a threat.

2-76. Soldiers performing duties as guardian angels have no other mission requirements or tasks as they only provide close security overwatch to personnel engaging, training, or partnering with FSFs. They must concentrate on securing assigned personnel and avoid being distracted by conversations or training occurring around them. However, commanders take care to ensure the use of guardian angels does not jeopardize the trust and confidence of the FSFs.

2-77. Units employ guardian angels at any location where U.S. forces operate alongside FSFs with access to weapons and ammunition. This includes at partnered locations where Soldiers and FSFs cohabitate and are only separated by physical security measures. Units take special care at these locations; commanders may use guardian angels to protect Soldiers' sleeping or dining areas. However, when FSF leadership meets with U.S. advisors or leaders on a secure U.S. facility, the use of guardian angels may not be necessary.

2-78. During static engagements or meetings with FSFs, guardian angels establish points of dominance in the room where they can observe and defend ingress and egress points. They maintain a clear line of sight on their fellow Soldiers and all the participating FSFs. A guardian angel accounts for furniture, obstacles, and windows when establishing a point of dominance. Furniture should not interfere with a guardian angel's ability to engage potential targets, and windows must be accounted for as potential vulnerabilities, ingress

points, and egress points. They should also avoid silhouetting themselves in front of windows. Guardian angels enter a room first and exit it last. Figure 2-3 depicts guardian angels establishing points of dominance.

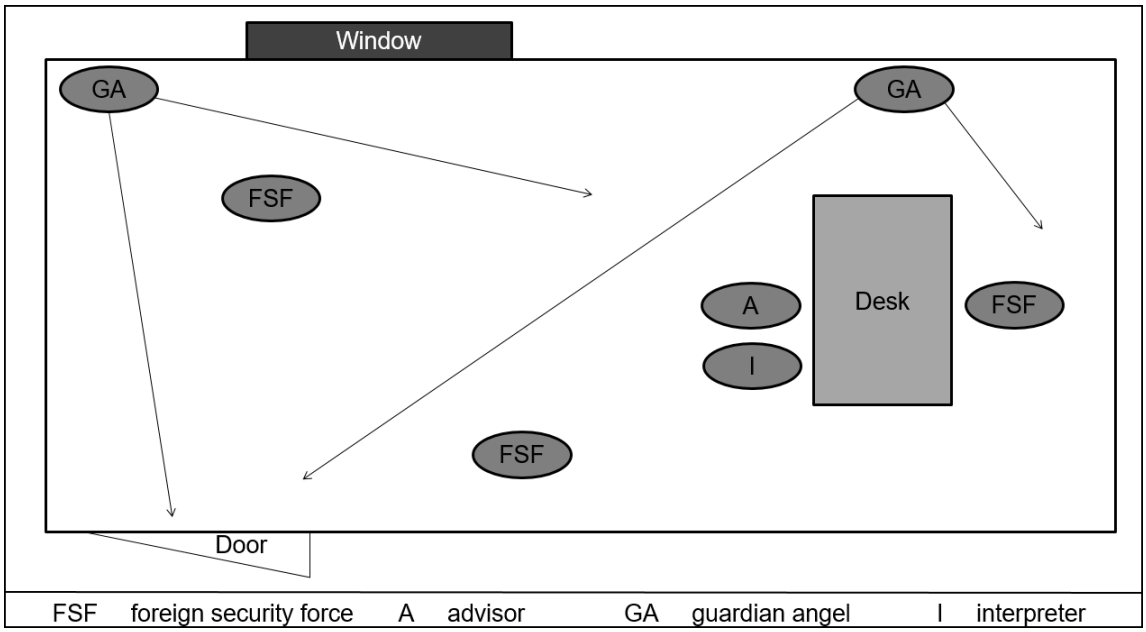


Figure 2-3. Point of dominance

2-79. Units also use guardian angels during dismounted, mobile engagements with FSFs, such as when U.S. leaders visit a local compound, base, or urban area. These engagements may require more personnel designated as guardian angels than during static, indoor engagements. During these operations, FSF leaders may employ their own personal security detail, and guardian angels may integrate with them to provide additional overwatch.

2-80. Guardian angels are particularly important when executing training with FSFs that involves live munitions, such as small arms ranges. Guardian angels remain in full PPE and position themselves in locations where they can observe the entirety of the training. Multiple guardian angels may be necessary for these training events.

Note. Units take special care to ensure that security measures, such as the use of guardian angels, are not seen as culturally offensive or disrespectful. Commanders may need to explain that their higher echelon headquarters requires these measures. Commanders should compare these measures to using a personal security detail common to many foreign militaries.

DEFEAT

2-81. If prevention and deterrence fail, an FSF threat may evolve into an attack. Defeat consists of the immediate response procedures executed to neutralize an attack and restore local security. Units accomplish defeat by implementing established and rehearsed TTP, drills, and SOPs. These rehearsed action plans ensure the fastest possible response while offering the best means of neutralizing the threat. Defeating an FSF attack requires rapidly neutralizing the threat, consolidating forces and gaining control of the situation, warning and reporting, and conducting a combined response.

NEUTRALIZE THE THREAT

2-82. When an attack occurs, Soldiers gain and maintain contact as quickly as possible to neutralize the threat. This prevents an attack from expanding and limits potential casualties. While guardian angels often

provide the first line of defense, all Soldiers remain prepared to react decisively to neutralize a threat. FSF attacks are not confined to areas where guardian angels are assigned. Attackers may even target members of the security force. In these situations, the reserve or quick reaction force must respond rapidly to neutralize the attacker. If a reserve or quick reaction force is not available, Soldiers performing duties as internal or mobile security form fire teams and respond immediately.

2-83. An FSF attack may be part of a larger, complex attack supported by enemy reinforcements. Enemy forces may seek to exploit the surprise and confusion caused by the initial attack to launch a larger assault on a unit or compound. Because of this, units maintain external security during this initial response to defeat enemy reinforcements, prevent the attacker or accomplices from fleeing, and assist with regaining control of the situation.

2-84. An attack initiated against a unit's security force may result from early detection, and the security force may not be the attacker's intended target. Until security forces neutralize the threat, guardian angels continue performing their duties unless otherwise directed by their commander.

CONSOLIDATE FORCES AND GAIN CONTROL

2-85. The confusion, speed, and shock of an attack may to lead to a temporary loss of control. Rapidly regaining the initiative through clear communication, deliberate maneuver, and disciplined target identification is critical to defeating the threat. Once security forces neutralize the threat, the unit meets at a predetermined rally point to gain control, conduct accountability, and further assess the situation. Leaders choose a rally point that is defensible and provides the cover necessary to provide initial casualty care. Leaders at all levels need to account for their subordinates as they coordinate response efforts. Units maintain external security as they consolidate forces at the rally point.

2-86. Unless required to depart to evacuate casualties, units secure the area to prevent a follow-on attack and to facilitate exploitation. If necessary, units cordon the scene of the attack to preserve evidence and detain potential accomplices for questioning. Elevating force protection measures and restricting access to the area facilitates a unit regaining control and initiative.

WARN AND REPORT

2-87. Leaders and Soldiers rapidly communicate pertinent information regarding an attack to all members of the unit as soon as possible. Once the security situation allows, units report information to their higher echelon headquarters and, if necessary, request follow-on support to secure and exploit the site. If the attacker escapes, the unit warns other forces in the area. The unit can coordinate support and response efforts with other forces.

CONDUCT A COMBINED RESPONSE

2-88. When possible, units coordinate with FSFs to conduct a combined response to an attack. Bringing all capabilities to bear may assist in regaining control and initiative, especially if multiple actors coordinated the attack. FSFs may assist in regaining control by identifying attackers and communicating with wounded or panicked civilians. If a unit must depart to evacuate casualties, FSFs may be the only option to secure the scene and preserve evidence for exploitation. Conversely, if the attacker escapes, FSFs may be better positioned to pursue the attacker if U.S. forces must secure the scene or evacuate casualties. Responding units assume a supporting relationship to the attacked unit until friendly forces restore local security. A combined effort by all partners and agencies strengthens the overall response and lays the foundation for recovery operations.

EXPLOIT

2-89. Exploitation commences as soon as the on-scene commander is satisfied that the unit neutralized the threat and established a secure local environment. *Exploitation* is taking full advantage of any information that has come to hand for tactical, operational, or strategic purposes (JP 2-01.3). Exploiting an attack transforms the initiative gained during the response phase into momentum to drive follow-on operations. It capitalizes on the attacker's exposure to further develop an understanding of the threat network and allow

units to assess and refine their force protection and threat TTP. Properly exploiting an FSF attack establishes the foundation for actions in the recover function and ensures information gathered directly supports lessons learned.

2-90. Exploiting an attack involves gathering information and evidence that contributes to an understanding of the attackers, their affiliations, and their motives. To target the FSF threat and prevent future attacks, forces that conduct exploitation also pursue, preserve and investigate, and collect and share intelligence and lessons learned.

PURSUE

2-91. Pursuit operations involve capturing and detaining individuals who were either involved in an attack or had prior knowledge of an attack. This includes attackers, accomplices, and potentially, depending on the circumstances, the attacker's family and associates. Pursuing escapees and accomplices may yield information that drives follow-on operations and results in wider successes against threat networks. Soldiers treat individuals detained as part of an attack in accordance with the law of war and rules for the use of force (known as RUF). While tactical questioning immediately following the incident may provide actionable information, only human intelligence personnel trained and certified to conduct interrogations can perform additional questioning for intelligence.

PRESERVE AND INVESTIGATE

2-92. Once operational circumstances allow, Soldiers treat an incident as a crime scene to preserve and investigate evidence. This treatment includes securing the immediate area of the attack; bodies of victims, attackers, or bystanders; detained individuals; and weapons or equipment used in the attack. Until investigative authorities arrive and assume the scene, the responsible unit establishes a cordon and controls ingress and egress through a central point. Most often a unit gains that control by posting guards and using engineer tape to mark a rough perimeter. The unit limits access to only those personnel required to render the scene secure, preserve sensitive equipment or information, and provide aid to the wounded. Personnel who enter the scene make every effort to avoid disturbing it; they only move equipment or weapons that pose a safety or security hazard. Successfully preserving evidence is a key step in exploiting threat networks and collecting lessons learned.

2-93. After the unit secures the scene and preserves evidence, forces conduct site exploitation (SE) to collect the information necessary to further expose, identify, and defeat threat networks. *Site exploitation* is a series of activities to recognize, collect, process, preserve, and analyze information, personnel, and/or material found during the conduct of operations (JP 3-31). Tactical SE is a series of methodical actions taken to ensure that material at the scene of an attack is detected, collected, and processed. SE may collect actionable information to potentially drive future operations, deny enemy forces resources, or help the unit better understand an OE.

2-94. Proper SE requires preparation and training. Units prepare by maintaining an SE kit with the equipment required to thoroughly exploit the scene of an attack. The kit includes items like bags and tags for evidence, a camera, permanent markers, tape, chalk, and spray paint. Preparation also requires developing an SE SOP that provides a systematic method for searching, documenting, and collecting evidence. Units search the scene of an attack methodically and mark, photograph, and diagram all rooms searched. In addition to weapons used in the attack, units secure the attacker's electronic devices, computers, notebooks, identification items, and cell phone, as these items may yield pertinent information concerning the attacker's motivation and a wider threat network.

2-95. SE may also extend to the attacker's barracks, home, or unit headquarters if the attack did not occur at one of these locations. Units need to thoroughly search the attacker's personal effects to yield a complete picture of the threat network, the motive behind the attack, and the attacker's preparations. U.S. forces may have to work closely with the FSF command to gain access and conduct SE at these locations. (See ATP 3-90.15 for additional information on SE.)

2-96. In addition to exploiting the scene of an attack, units prepare to thoroughly investigate and debrief personnel involved. Military police, intelligence staff, and higher echelon headquarters may all conduct investigations and request to interview U.S. forces and FSF members. Authorities may also wish to speak

with the attacker's friends, family, or members of the attacker's unit. The unit ensures that partnered FSFs present for the attack are documented and remain at the scene until interviewers have arranged to interview the FSFs as part of the investigation. Commanders make every effort to facilitate these activities. While an investigation can include numerous agencies, commanders may also initiate their own investigation into an attack. Commanders can refer to AR 15-6 to capture and codify lessons learned from an incident and refine unit TTP and SOPs to effectively mitigate future threats.

COLLECT AND SHARE

2-97. After the unit and responsible agencies complete their investigations of an incident, the findings are collected and shared with the higher headquarters and other units. Through careful study and analysis, leaders identify points in the operation where practices or lapses made the unit vulnerable to attack. From this, leaders identify or recommend changes to TTP, SOPs, drills, and training programs to prevent future incidents and address vulnerabilities. Units may also learn vital lessons from internal AARs or debriefs. Commanders ensure the lessons learned from investigations or AARs are implemented across their formations and shared with other units in the joint operations area. To ensure the widest dissemination, staffs share lessons learned from FSF attacks with the Center for Army Lessons Learned.

RECOVER

2-98. The recover function consists of four simultaneous and overlapping tasks that aim to stabilize the situation so that operations may return to pre-incident levels. As a whole, recover consists of the actions taken to regain trust and cohesion with partnered FSFs, to resume pre-attack operations, and to manage the wider consequences of the attack. Until recovery occurs, leaders consider adjusting operational requirements that must continue in the immediate aftermath of an attack. For example, leaders may adjust the length of guard duty or rotate Soldiers through posts more frequently. After a particularly destructive attack, commanders may consider adjusting subordinate unit partnerships or AOs. Commanders may also consider temporarily suspending operations to provide Soldiers opportunities for rest and relaxation. The four tasks discussed in paragraphs 2-99 through 2-102 provide a general framework for the recover function; however, it is ultimately the unit commander's decision when to return operations to pre-incident levels.

MANAGE CONSEQUENCES

2-99. One task in the recover function is consequence management, a critical task after any attack involving partnered FSFs. The enemy often exploits attacks as part of an information campaign or strategic communication effort. Because of this, units work proactively with public affairs officers (PAOs) to manage consequences and control the narrative. Identifying factors that precipitated an attack, detailing the response, and highlighting steps taken to prevent future attacks are essential in dispelling rumors and de-escalating heightened emotions. Managing consequences requires messaging at every level be coherent and responsive while providing a narrative that debunks potential enemy claims without divulging information that could compromise future operations. Messaging assures partners that U.S. forces are taking the necessary steps to determine the cause of an attack and prevent future attacks from occurring. Consequence management reaffirms the importance of U.S. relations with partners and helps maintain the operational tempo with as little disruption as possible.

ENGAGE PARTNERS

2-100. Following an attack, relationships between multinational partners may be strained. Leaders quickly engage with partnered FSFs to explain the attack, the response, and the future. Strong unit cohesion, good rapport, and an effective combined response can significantly ease tensions and speed the return to normalcy. When possible, units include partnered FSFs in recovery operations. Units may share lessons learned from the investigation with FSFs so long as this does not compromise unit security or future operations. This may promote buy-in, trust, and cohesion between U.S. forces and FSFs. Units may also conduct a coordinated messaging or public affairs campaign with partnered forces to promote the perception of unity and restore the public's confidence in the operation and its objectives.

REINFORCE MORALE

2-101. Morale may be damaged as the result of an FSF attack. Part of the recover function involves reinforcing unit morale. This is especially true if the attack was committed by an FSF unit that had an enduring and trusted relationship with U.S. forces. Good leaders understand the importance of rebuilding morale among their Soldiers and multinational partners. Communication is key to reinforcing morale. Commanders inform Soldiers of pertinent information related to an attack, the status of the investigation, and any measures implemented to prevent future attacks. After an attack, Soldiers may seek counseling from behavioral health professionals or chaplains to assist in coping. Commanders strive to accommodate these requests, since counseling can help improve morale across the organization. If possible, commanders may offer these services to FSF partners affected by the attack.

RESUME OPERATIONS

2-102. The last task of the recover function is resume operations. Commanders and units resume their missions as rapidly as possible after an attack. Attacks are operationally ineffective once activity returns to pre-incident levels. Resuming operations is a sign of normalcy. It signals renewed trust, and it is an indication of restored confidence between U.S. forces and their FSF partners. Furthermore, it demonstrates the Army's commitment to mission accomplishment, and it is a testament to a unit's courage and cohesion. Resuming operations may also boost morale still lagging from the disruption caused by an attack.

This page intentionally left blank.

Chapter 3

Foreign Security Force Threat Training Program

This chapter provides guidance for incorporating FSF threat prevention and response techniques into unit training programs. The techniques offered can be incorporated into unit training before or during a deployment requiring close cooperation with FSFs.

TRAINING TO PREVENT

3-1. Commanders are responsible for ensuring units conduct FSF threat prevention training. FSF threat prevention training includes personnel selection and cultural awareness training.

PERSONNEL SELECTION

3-2. Training to prevent the FSF threat begins with assessing and selecting appropriate personnel to partner with FSFs. Many FSF attacks stem from personal disputes, cultural animosity, or disagreements between FSF and U.S. Service members. Because of this, Soldiers who work closely with FSFs should be mature, possess strong interpersonal communications skills, have high emotional intelligence, and demonstrate patience when working with peers and teammates. Soldiers working alongside FSFs need to possess conflict resolution skills and the cultural adaptability to operate in a multi-partner environment. Culturally adaptable Soldiers demonstrate awareness, interaction, skillful rapport-building, respectfulness, self-reflection, and self-control.

3-3. Leaders at all levels should know their subordinates, including a general knowledge of their strengths and weaknesses. Not everyone has the aptitude to work alongside people from different cultures. Commanders have a responsibility to identify those individuals and avoid placing them in advisory roles. In advisory roles, these individuals can invite undue risk on themselves, others, and the mission.

3-4. Commanders also consider individual rank and standing when considering partnerships with FSFs. They partner U.S. advisors with FSF members of similar rank, as significant differences between advisors and their partners may become a source of tension. When U.S. advisors are junior in rank to their FSF counterparts, their guidance may cause embarrassment or humiliation, especially if offered in public. Over time, the tension this causes may escalate into violence. An unbalanced partnership can make the underlying advisory mission exceedingly difficult, as the FSF partner may reject guidance provided by a junior ranking U.S. Service member.

CULTURAL AWARENESS TRAINING

3-5. Training to prevent includes cultural awareness training. Cultural misunderstandings may result in grievances that, if combined with other tensions, can lead to an attack. Commanders can mitigate these tensions by conducting cultural awareness and sensitivity training before and during deployment. Cultural awareness training not only informs Soldiers of acceptable and unacceptable norms and behaviors, but it also promotes respect for the different cultures, ethnicities, and nationalities units may encounter during their deployment.

3-6. Pre-deployment cultural awareness training consists of both classroom instruction and practical exercises to condition Soldiers for the diversity they may encounter during a deployment. Classroom training provides the context and background necessary for Soldiers to recognize acceptable and unacceptable norms and behaviors. Trainers then incorporate these norms and behaviors into a live training environment so Soldiers can practice demonstrating respect without compromising security or mission objectives. Commanders can use these training events to assess Soldiers for cultural adaptability.

3-7. Commanders use cultural awareness training while deployed to build on the foundation provided during pre-deployment training. This secondary training refines cultural sensitivities to the precise location, ethnicity, or nationality with which a unit is partnered. This training is often best provided by HNSF, and it can serve as a tool for building rapport and increased understanding between U.S. forces and FSFs. Commanders may also consider this training opportunity as a forum for HNSF to provide feedback to the unit on its cultural sensitivity and areas for improvement with the local population. In addition to HNSF, local national interpreters often prove invaluable for providing cultural awareness training and feedback while deployed.

TRAINING TO DETER

3-8. Units train to deter an FSF attack by developing and rehearsing TTP, SOPs, and battle drills that make the unit difficult to attack and demonstrate to a potential attacker the unlikelihood of carrying out a successful attack. Training to deter promotes a culture of vigilance and discipline within the unit and ensures Soldiers can identify and mitigate a threat before the unit is compromised. As such, this training reinforces the Soldier's ability to detect and respond to a threat without ceding initiative to the enemy. Training to deter consists of detection, escalation of force, and biometric toolkit training.

DETECTION

3-9. The threat of detection is a strong deterrent; attackers may be unwilling to follow through with an attack if they believe it will be unsuccessful or costly. Training to detect consists of instructing Soldiers on the environmental, physiological, and behavioral indicators of an FSF threat and then challenging them to identify, communicate, and rapidly react to those indicators in accordance with the unit's TTP, SOPs, and battle drills.

3-10. Training to identify potential threat indicators is an important step in detecting FSF threats. Effective Soldiers know the indicators listed in paragraphs 2-25 through 2-33. Leaders employ the predictive classification concept discussed in paragraphs 2-34 through 2-36 to monitor suspected threats. Incorporating indicators into live training environments enhances Soldiers' abilities to identify an FSF threat. Effective leaders brief role players on these indicators and include role players in exercises conducted at combat training centers and mobilization training centers prior to deployment.

3-11. Training to detect includes detecting counterfeit credentials. Leaders train Soldiers to recognize FSF badging and access credentials, so Soldiers can quickly recognize inauthentic or unauthorized badges. Trained Soldiers can identify FSF uniforms and ranks as well as render the proper customs and courtesies due senior ranking FSF members.

3-12. Units train to assess their OE before and during deployments. Training to know the environment, identify anomalies, and detect potential threats can be easily incorporated into live training environments. Leaders coach Soldiers to constantly scan and interpret their surroundings. They challenge their Soldiers to identify vulnerabilities or locations from which an enemy could mount an attack. Leaders vary the training environment to present Soldiers with indicators of a potential threat, such as a deserted market place that is normally crowded.

3-13. Effective commanders continue training to detect indicators and anomalies while deployed. This training starts with leaders helping Soldiers establish a baseline for their OE. During missions, leaders discuss the environment with their Soldiers, identifying notable characteristics of locations the unit regularly visits. Afterwards, leaders discuss what specific changes to these environments indicate a potential threat.

ESCALATION OF FORCE

3-14. Although all Soldiers generally receive escalation of force training, because of their requirement to continually assess, identify, and defeat potential threats, this skill is especially important for Soldiers performing duties on a security force or as guardian angels. Escalation of force measures provide Soldiers with an actionable framework for discerning and neutralizing a threat. Generally, once a perceived threat is identified, Soldiers employ escalation of force measures that progress from audible and visual warnings, through less-than-lethal force to lethal force until the threat is neutralized. Escalation of force training consists

of classroom instruction and situational training exercises that require Soldiers to identify and react to threats in accordance with the prescribed escalation of force measures. During escalation of force training, trainers vary the threat so that Soldiers are required to both progress through each of the steps and, at times, escalate rapidly through the steps to address a significant threat. Units conduct escalation of force training before and during deployments and often include it in pre-mission briefs and rehearsals. Table 3-1 presents a basic threat detection and neutralization framework that can be used in conjunction with escalation of force measures to stop a threat. However, commanders ensure Soldiers are trained on the rules for the use of force and escalation of force measures applicable to the theater in which they operate.

Note. Commanders, staffs, and subordinates ensure their decisions and actions comply with applicable United States, international, and, in some cases, local laws and regulations. Commanders at all levels ensure that their Soldiers operate in accordance with the law of war and the ROE. (See FM 6-27.)

Table 3-1. Threat detection and neutralization

Step	*Action*
Identify the threat.	Visually scan foreign security forces (FSFs) looking for concealed weapons, odd mannerisms, and demeanor. Start with the hands and move up and down the body. Scan for bulky protrusions or odd shapes concealed under clothing.
Stop the threat.	If a threat is detected, begin with a verbal warning and then use escalation of force to stop their movement and gain time and space.
Disarm and search the threat.	If possible, have other FSFs disarm and search the suspected individual for concealed weapons or explosives. United States forces should observe this search and provide armed overwatch to ensure thoroughness and security.
Verify identity.	Trusted FSF leadership verify the suspected individual's identity. Verify security badges for authenticity and authorization to access the facility.
Communicate.	Disseminate updates about the security situation to the patrol and request additional support if necessary.
Neutralize the threat.	If the suspected individual refuses to comply with commands, act decisively to neutralize the threat. In accordance with rules for the use of force, the law of land warfare, and the rules of engagement, apply the lowest level of force necessary to stop the threat.

3-15. To properly conduct escalation of force, Soldiers are trained and proficient with common host-nation and FSF key words and phrases. Commanders can use interpreters, HNSF, and FSFs to assist in teaching and rehearsing common words and phrases necessary for Soldiers to conduct basic escalation of force. (See additional language training resources at the Army Training Requirements and Resources System at https://www.atrrs.army.mil and the Defense Language Institute Foreign Language Center at http://www.dliflc.edu.)

BIOMETRIC TOOLKIT TRAINING

3-16. When leaders train Soldiers to detect, they include training on biometric toolkits and devices. Soldiers use these devices in theater to enroll and screen enemy fighters, FSFs, and local contractors in threat databases. Training covers how to verify identities with the devices, how to screen for threats, and how to upload and download data. If a unit's mission requires recruiting and screening HNSF, Soldiers also train on how to create identification badges with biometric devices.

3-17. In addition to technical training on biometric toolkits, Soldiers are trained and proficient with the unit's communications equipment. The decentralized nature of SFA operations often requires Soldiers to operate in small teams and security elements away from the main body. Because of this, all Soldiers learn to effectively communicate across the patrol and to higher headquarters in support of critical activities. Trained Soldiers can load, fill, and transmit on all of the unit's organic communications systems.

TRAINING TO DEFEAT

3-18. Defeating FSF attacks requires developing, training, and rehearsing unit TTP and drills designed to posture a unit to rapidly respond to an attack. Effective TTP and drills are codified in unit SOPs. These TTP and drills address current enemy tactics. Staffs update and refine TTP and drills as enemy forces adapt.

3-19. Developing and rehearsing FSF threat prevention and response TTP enhances an organization's preparedness and improves its security posture. In addition to establishing and rehearsing standard TTP and drills, such as casualty evacuation or react to contact, units develop TTP and drills that directly address the FSF threat. Examples of effective TTP and drills include the use of guardian angels, consolidation and accountability drills, and the identification of teams and methods for inspecting locations for threats before key events.

3-20. During deployment, units can construct training aids to rehearse their threat response TTP and drills in an environment that closely mimics conditions they encounter when operating. Constructing "glass houses" that replicate the compounds and buildings a unit frequents provides a realistic environment for rehearsing TTP and drills. Reacting to an FSF attack, rehearsing casualty evacuation, and practicing ingress and egress drills on terrain that accurately replicates conditions in an OE improves a unit's ability to rapidly defeat an attack.

GUARDIAN ANGEL TRAINING PROGRAM

3-21. A comprehensive guardian angel training program is the foundation of FSF defeat. Training Soldiers to serve as guardian angels starts with specialized selection. Like SFA advisors, guardian angels possess the maturity, cultural adaptability, and endurance to operate alongside FSFs for prolonged periods. Commanders select Soldiers with a keen sense of awareness, the discipline to stay focused in distracting or confusing environments, and the ability to rapidly detect threats and make decisions. Soldiers selected to serve as guardian angels demonstrate a high proficiency with their assigned weapons. Often, the best guardian angels are experienced Soldiers and junior noncommissioned officers.

3-22. Units train guardian angels to perform their duties both overtly and covertly. They train on establishing points of dominance in rooms where they can best counter a possible threat while safeguarding assigned personnel. This training includes observing and safeguarding ingress and egress points, managing obstacles and furniture, and maintaining clear lines of sight throughout engagements.

3-23. Soldiers selected to perform duties as guardian angels are assigned weapons and optics designed for use at close quarters instead of those designed for engagements at distance. For example, weapons like the M-249 Squad Automatic Weapon are not appropriate for Soldiers performing duties as guardian angels. Soldiers performing duties as guardian angels are issued a rifle and sidearm if available. Additionally, not all Soldiers are experienced with a pistol and units train pistol proficiency before and during a deployment. Guardian angels also wear discreet communications equipment such as the Multiband Inter-Intra Team Radio with ear pieces that do not interfere with or distract from their primary mission.

3-24. More information relevant to guardian angel training can be found in ATP 3-39.35 (law enforcement restricted). Soldiers designated to perform duties as guardian angels are encouraged to attend the high-risk personnel protection course at Fort Leonard Wood, Missouri. The course provides specialized training to Soldiers, regardless of military occupational specialty, who are assigned to conduct high-risk personnel security operations.

WEAPONS TRAINING

3-25. Weapons handling and advanced marksmanship training are critical components of an effective guardian angel training program. Normal weapons proficiency training is often insufficient for Soldiers designated to serve as guardian angels. These attacks often occur in close quarters and crowded spaces, and they may develop rapidly without warning. Guardian angel training shifts away from a qualification-centric weapons training strategy in favor of one that emphasizes dynamic shooting engagements at closer ranges. Advanced weapons training and marksmanship is required to enhance speed of response and accuracy in close quarters. Guardian angel weapons training includes advanced marksmanship, close-quarters marksmanship (CQM), and stress shooting exercises to build Soldiers' confidence in their ability to

accurately identify and engage targets at close range. This training is conducted in a progression from pre-marksmanship instruction and dry fire training, to simulations based training, and, ultimately, advanced live-fire exercises. Commanders exercise discretion in tailoring their CQM training strategy to the unit's mission by considering multiple sources of information and TTP. Guardian angel weapons training includes the following fundamentals:

- Pistol training:
  - Stance.
  - Grip.
  - Sight picture and sight alignment (aiming).
  - Drawing the pistol.
  - Trigger control.
  - Follow through.
  - Breathing.
  - Weapon positions.
  - Loading and press check.
  - Safety and decocking procedures.
  - Unloading.
  - Reloading.
  - Malfunctions.
  - Post-engagement sequence.
  - Support-side weapon manipulation.
- Rifle training:
  - Stance.
  - Grip.
  - Length of pull and buttstock position.
  - Sight alignment.
  - Trigger control.
  - Weapon positions.
  - Reloading.
  - Transitions.
  - Malfunctions.
  - Immediate action.
  - Remedial action.
  - Support side weapon manipulation.
  - Post-engagement sequence.
  - Scanning.
  - Asymmetrical shooting positions.

Dry Fire Training

3-26. Dry fire training consists of weapons familiarization and training without live rounds, but it may include simulated dummy rounds. Soldiers build on the fundamentals taught during pre-marksmanship instruction by incorporating sight alignment, trigger control, and weapons handling with rapid reloading, immediate action drills, and weapons transition drills. Units train Soldiers on these skills under progressively demanding time constraints to build proficiency and confidence. If trained properly and repetitively, these skills transfer to live-fire training. Dry fire weapons training requires little additional equipment, can be trained virtually anywhere, and offers a cost-effective means for Soldiers to practice their weapons handling skills.

Simulations Based Training

3-27. The Engagement Skills Trainer and other simulation-based training aids are important progressions in a CQM training strategy, and they offer a viable alternative when live-fire training resources are unavailable. Leaders use the feedback provided by these simulations to assess and correct marksmanship fundamentals. These training aids are also used to conduct more advanced threat identification and target acquisition training through "shoot" and "don't shoot" scenarios that cannot be replicated in a live-fire environment.

3-28. If allocated, units conduct simulations based training with blank rounds or simunitions as an intermediate step in a CQM or advanced marksmanship training progression. This training is used to familiarize and rehearse the tasks, conditions, and standards required during live-fire training. If possible, this training is conducted at the same range, "shoot house," or facility as the live-fire training and Soldiers fire the same tables they will execute during live-fire.

Live-Fire Training

3-29. After gaining confidence and demonstrating proficiency under dry and simulated fire conditions, Soldiers conduct CQM live-fire training. CQM live-fire training emphasizes target identification and acquisition, responsible weapons handling, and rapid decision making. Instead of large silhouette targets, Soldiers engage smaller targets consisting of multiple shapes and colors that challenge them to engage variable targets under the verbal command of a safety. These ranges require Soldiers to rapidly assess an environment and identify targets while emphasizing accuracy at close quarters. Leaders can enhance this training by having Soldiers perform under stressful conditions.

3-30. A stress shoot challenges Soldiers to accurately engage targets with an elevated heart rate, under variable light conditions, and with excessive ambient noise to distract them. Training may also include the use of dummy rounds interspersed with live munitions to require Soldiers to perform immediate action on their weapons. Soldiers may also be issued magazines with unknown numbers of rounds to require multiple and unforeseen reloads. Trainers can introduce these requirements and conditions on a standard 25-meter range; however, effective CQM training culminates with live-fire shoot house training when available. Shoot house training requires Soldiers to rapidly identify and engage targets within buildings and rooms at close ranges. This training provides guardian angels with the most realistic representation of the conditions they may face when deployed and requires Soldiers to employ all the CQM skills learned during the training strategy. As always, safety overrides experience, and units must carefully conduct risk management to ensure proper control measures are in place to mitigate the risks associated with advanced marksmanship and CQM training events.

> ***Note.*** In addition to the overall training strategy, individual CQM, advanced rifle marksmanship, and shoot house training events are often conducted in a progression from dry, to blank, to live fire. This additional safety measure familiarizes Soldiers and safeties with the task, conditions, and standards for the training event and may identify unforeseen hazards.

TRAINING TO EXPLOIT

3-31. Soldiers and units train to exploit conditions and execute activities necessary to fully capitalize on an attacker's exposure after an incident occurs. Units use the information gathered from exploitation to better understand an OE, to expose the potential threat network, and, subsequently, to drive future operations. Training to exploit involves mastering the supporting tasks that enable units to detain and question attackers, preserve evidence, and investigate the scene of an attack. These supporting tasks consist of training to detain, search, process, and question suspect individuals, and to conduct effective SE.

DETAIN, SEARCH, AND PROCESS

3-32. Attackers and suspects (accomplices or facilitators) who surrender or are captured following an attack are detained, searched, and processed as detainees until a decision is made regarding their disposition. Soldiers train on the tasks and techniques required to detain, search, and process an attacker. Searching and processing a detainee provides security, control, and intelligence to the capturing unit while simultaneously ensuring the welfare of the detainee in U.S. custody. All detainee processing must be accomplished with care to collect critical intelligence, preserve evidence, maintain accountability, and protect detainees from danger or harm. The 5 Ss and T technique consists of search, silence, segregate, speed, safeguard, and tag. Soldiers use the 5 Ss and T technique to process an attacker or suspect individual. This technique provides a structure to guide Soldiers in conducting detainee operations until they transfer detainee custody to another authority or location.

Search

3-33. The first step in this process is to render the individual safe by disarming and searching the attacker. Preferably from a covered position, Soldiers verbally instruct the attacker to disarm through either basic commands in the attacker's native language or through an interpreter. After the attacker removes visible weapons and moves away from those weapons, the Soldier instructs the attacker to manipulate their uniform in a manner that confirms the presence or absence of concealed explosive devices (either pull uniform tight or lift uniform to reveal undergarments). This is an extremely important step. Because FSF attackers often show little regard for their own welfare and have no intention of surviving an attack, Soldiers must ensure the attacker is not wearing or concealing an explosive device. If a device is discovered, the Soldier instructs the attacker to remove the device and move to a safe location to continue apprehension and processing. Soldiers then cordon the area around the device ensuring other U.S. Service members, partnered forces, and civilians remain a safe distance away. Soldiers notify explosive ordinance disposal and maintain an effective cordon until the device is neutralized.

+ 3-34. After removing visible weapons and explosives, Soldiers restrain and control the detainee and conduct a more thorough search. This search is methodical and always performed by a least two Soldiers. One Soldier searches the detainee while the other supervises and observes, ensuring the Soldier conducting the search remains safe and conducts the search professionally. The Soldier searches the attacker for additional weapons and items of intelligence value. The observing Soldier records items identified and taken from the attacker. The Soldier annotates weapons, ammunition, and equipment on a DD Form 2745, *Enemy Prisoner of War (EPW) Capture Tag*, and annotates personal items on a DA Form 4137, *Evidence/Property Custody Document*.

Note. The point of capture (known as POC) is where most detainee abuse allegations occur; it is the point where emotions following enemy contact may run high and where there is a need to conduct individual searches and tactical questioning to prevent additional casualties. Leaders and Soldiers must monitor unit and individual stress to prevent violations of the law of war or U.S. policy.

Note. Conduct same-sex searches when possible. If mixed-sex searches are necessary for speed or security, conduct them in a respectful manner and avoid any action that could be interpreted as sexual misconduct. To prevent allegations of sexual misconduct, the on-site commander or leader must provide appropriate supervision, with more mature and experienced personnel conducting mixed-sex searches.

Note. Once the attacker has been searched and deemed safe, U.S. forces provide first aid for injuries, and inspect and return the attacker's PPE until they move the attacker to a safe location.

Silence

3-35. If multiple attackers or suspects are detained, the unit ensures they cannot communicate with each other. The unit silences uncooperative detainees by muffling them with a soft, clean cloth tied around their mouths and fastened at the back of their heads. The unit does not use duct tape or other adhesives, place a cloth or other objects inside the mouth, or apply physical force to silence detainees.

Segregate

+ 3-36. Detainees are segregated according to local policy and SOPs (segregation requirements differ from operation to operation). The ability to segregate detainees may be limited by the availability of Soldiers to secure the detainees at the point of capture. At a minimum, the unit attempts to segregate detainees by grade, sex, age, and security risk.

Note. Segregation is used for security reasons or to separate groups as required by the Geneva Conventions (grade, nationality, family). Segregation differs from the interrogation approach s*eparation* as defined in FM 2-22.3.

Speed

3-37. The unit quickly removes detainees from any continuing risks associated with other combatants or sympathizers who may still be in the area. If there are more detainees than the Soldiers can control, the unit requests additional support from higher headquarters, searches the detainees, and holds them in place until reinforcements arrive.

Safeguard

3-38. Units protect detainees and ensure the custody and accountability of all confiscated items. Soldiers safeguard detainees from combat risk, harm caused by other detainees, and improper treatment or care. Soldiers report all injuries. They correct and report violations of U.S. military policy that occur while safeguarding detainees. Acts or omissions that constitute inhumane treatment are violations of the law of war and, as such, Soldiers must correct immediately. Simply reporting violations is insufficient. If a violation is ongoing, a Soldier has an obligation to stop the violation and report it.

Tag

3-39. Soldiers ensure each detainee is tagged using a DD Form 2745. Soldiers link confiscated equipment, weapons, and evidence to the detainee using the DD Form 2745 control number. When Soldiers use a DA Form 4137 to document confiscated items, Soldiers link those items to the detainee by annotating the DD Form 2745 control number on the form.

ADDITIONAL TRAINING

3-40. While the 5 Ss and T technique captures the principles of detainee operations in an actionable framework, a comprehensive training strategy requires that leaders train Soldiers on additional aspects of detainee processing at the point of capture. Additional training tasks include the following:

- Apply Army values, rules for the use of force, and ROE.
- Understand theater-specific escalation of force.
- Preserve, document, and control evidence and items that may be of intelligence value.
- Complete necessary forms (DD Form 2745, DA Form 4137, and DA Form 2823 [*Sworn Statement*]).
- Establish search, security, and biometric identification teams.
- Perform basic first aid and tactical casualty care.
- Capture, search, and security tasks.

3-41. In addition to training on the steps required to detain, search, and process an FSF attacker, units should construct (and Soldiers should be familiar with) a detainee processing kit. Detainee processing kits enable capturing units to properly secure; quickly, efficiently, and safely process; and quickly move detainees to a collection point. At a minimum, a detainee processing kit contains the following items:

- Disposable restraints.
- Disposable latex or vinyl gloves.
- Plastic trash bags for detainee property.
- Plastic bags for evidence or confiscated property.
- Blank forms (DD Form 2745, DA Form 4137, and DA Form 2823).
- Document protectors.
- String, twine, or 550 cord.
- Duct, packing, or adhesive tape.
- Blindfold material (cloth).
- Unit SOPs for handling and processing detainees and evidence.
- Visual language cards.
- Paper, envelopes, and tape (various sizes).
- A digital camera and video camera (with batteries).
- An explosive-residue detection kit.
- Colored, permanent markers and chalk.
- A sketch pad.
- Meal, ready-to-eat boxes for documents, evidence, or files.

TACTICAL QUESTIONING

3-42. *Tactical questioning* is the field-expedient initial questioning for information of immediate tactical value of a captured or detained person at or near the point of capture and before the individual is placed in a detention facility (JP 3-63). Tactical questioning uses direct questions and is limited in duration. Tactical questioning is not interrogation and does not use the techniques approved for interrogations.

3-43. Immediately following an FSF attack, tactical questioning may yield pertinent information regarding additional accomplices, attack planning, and the wider threat network. It may also provide information to aid with SE. Once an FSF attacker or accomplice is deemed a detainee, trained Soldiers can conduct tactical questioning. Soldiers treat all persons being questioned, regardless of the purpose, humanely and without cruel, inhumane, or degrading treatment or punishment. Because Department of Defense trained and certified interrogators are the only personnel authorized to transition between tactical questioning and interrogation, commanders consider employing interrogators as tactical questioners as long as such employment does not detract from higher-priority human intelligence missions. Intelligence interrogators must follow the guidance in FM 2-22.3 and the requirements of AR 381-100, DODD 3115.09, and other relevant policies and regulations. Any questioning of a detainee that is not conducted by a Department of Defense trained and certified intelligence interrogator must carefully follow the specific guidelines for tactical questioning.

3-44. Tactical questioning consists of direct questions concerning the details surrounding an attack, the attacker, and the threat network. Soldiers conducting tactical questioning ask detailed questions to gather as much information as possible about the attack. They attempt to collect information concerning what other FSF members knew about the attack, how the attacker arrived at the scene of the attack, how the attacker gained access, and how the attacker obtained the weapons used in the attack. Initial responses to these and other questions may be followed up with additional questions attempting to gain as much precise information as possible. Later, the intelligence staff and investigators can refine this information to yield a more comprehensive understanding of the threat network, an OE, and the incident at hand. Tactical questioning focuses on the facts related to the attack that may yield additional, actionable information; trained and certified interrogators can question the attacker at a later time to determine motive.

3-45. Training to conduct tactical questioning begins at home station and can be conducted in a progression from the classroom to situational training exercises. During these training events, Soldiers are challenged to tactically question in a manner that reveals all the details surrounding an incident or attack, especially those

that may seem insignificant or trivial. Human intelligence collectors have trained on conducting tactical questioning and can be used to facilitate this training. For more information on tactical questioning see ATP 3-55.4.

SITE EXPLOITATION

3-46. Commanders conduct SE in the aftermath of an FSF attack or when an FSF attacker is discovered before an attack. SE consists of tactical site exploitation and technical site exploitation. Generally, tactical SE includes activities performed at or near a specific location. Technical exploitation is conducted off site in a laboratory. In the aftermath of an FSF attack, units can perform tactical SE to assist in the investigation and develop a more comprehensive understanding of the attack, the threat, and the local security environment.

3-47. SE may be hasty or deliberate. The main difference between hasty and deliberate SE is the time available for planning and preparation. Units conduct hasty SE after an FSF attack; however, units can use deliberate SE to further exploit the threat network when Soldiers discover an FSF attacker before an attack. In these instances, units conduct deliberate SE at an attacker's home, barracks, or unit to further expose and exploit the threat. SE leverages multiple capabilities including search techniques, biometrics, forensics, and document and multimedia exploitation.

3-48. Tactical SE consists of individual and collective tasks completed by Soldiers to establish facts. These facts provide critical information that supports the resolution of the commander's critical information requirements and can be used to better understand an OE and threat network.

3-49. The complexity of tactical SE and the potential confusion and chaos following an FSF attack require training and rehearsals to ensure proper coordination and execution. Commanders ensure subordinates train on the required supporting tasks and understand their role in the SE process. Lane training conducted in an environment similar to the anticipated AO is a sound method for training Soldiers on the individual search, documentation, and evidence-handling skills required by tactical SE. Tactical SE tasks that require training include—

- Establishing site security.
- Establishing initial control points within the search area. At a minimum, units establish entry control points.
- Coordinating with FSFs to ensure the combined response leverages all available assets and capabilities.
- Documenting search and collection results.
- Using tactical questioning.
- Questioning witnesses and victims in accordance with intelligence and local customs.
- Using biometric enrollment and screening.
- Following evidence handling procedures.
- Transferring detained persons and confiscated materiel.
- Employing proper search techniques.

3-50. SE requires proper task organization and rehearsals at the unit level. Commanders task organize their unit for SE by designating a security force and a SE team to search, detect, and collect information, evidence, and materiel. When employing a defense in depth, commanders task organize for SE by assigning the internal security team responsibility for controlling access to the search site and the external security team responsibility for overall security. Remaining members of the patrol, either the mobile security team, reserve, or guardian angels, can then be task organized as the SE team.

3-51. SE can be personnel intensive and units can request additional support from their headquarters to facilitate effective SE. If available, this may be technical support by functional experts with specialized forensic training and equipment, or it may consist of reinforcements to assist with providing security or searching the site.

3-52. Collective training for SE requires units protect the site, search the site, prioritize and seize relevant materiel, search and question witnesses or individuals , preserve the site and materiel, transfer control of the site, and transfer information, persons, and materiel to proper authorities.

Protect the Site

3-53. Leaders establish and maintain protection of the site while executing tactical SE. The security element designated to protect the site prevents interference with the search element. Units apply the appropriate tactical methods, such as inner and outer cordons or a combination of methods and tasks, to control the site for a subsequent exploitation.

3-54. The security element seeks technical advice from subject matter experts before declaring the site free of hazards and safe for the tactical SE team. Once the specialized teams confirm the site is ready for exploitation, the security element controls access to the site to prevent loss and destruction of any information or materiel and secures all individuals the search element wants to evaluate on-site.

Search the Site

3-55. Soldiers conduct visual and equipment-aided site searches. Searches are conducted in a methodical and controlled manner in accordance with unit SOP. Tactical SE teams thoroughly document the site and its contents before conducting invasive searches and collection activities. Complete documentation includes written descriptions, sketches, photographs, or video recordings. This documentation creates a record of the starting point for search actions. When units must search their partnered FSF facilities, barracks, or headquarters, leaders communicate with the partnered FSF to explain the procedures and protocol for such actions. They attempt to gain support and understanding from the partnered FSF to preserve the relationship and facilitate an effective combined response.

Prioritize and Seize Relevant Materiel

3-56. Seizure criteria focuses on the commander's critical information requirements and other information requirements that aid in understanding the attack, the threat, and the wider threat network. The intent of a tactical SE is to seize only items that answer information requirements or are associated with the threat. Seizure criteria includes all threat related or extremist propaganda such as leaflets, books, and pamphlets; a check for pre-set or last station accessed on radios, televisions, or other devices; the attacker's personal electronic devices to include cell phone, laptop computer, and tablet; information providing further insight into the identification and affiliation of the attacker or any accomplices such as passports, letters, pictures, and phonebooks; known or suspected weapons and munitions used or cached by the attacker; and equipment and materiel used by the attacker to manufacture improvised explosive devices.

3-57. When searching partnered FSF facilities, barracks, or headquarters, units cooperate with the partnered FSF to seize only relevant materiel related to the attack. Units avoid seizing materiel that would overly disrupt, degrade, or halt FSF operational capacity or capabilities. Units only seize information and materiel when they have reasonable suspicion or probable cause that the items were used by the attacker or related to the attack. Reasonable suspicion implies that any reasonable person would suspect that the information or materiel was or would have been involved in the attack. Probable cause implies that a reasonable person would believe that the information or materiel has been or would have been involved in the attack. The determination of probable cause is completely subjective. This decision is a matter of professional judgment, based on the information known at the time and the competence and character of the decision maker. If the materiel has no value to the threat or relation to the attack, it is returned once assessed.

Search and Question Witnesses

+ 3-58. Tactical questioning is conducted on captured or detained attackers and suspected accomplices or facilitators; however, witnesses and other persons present at the site, including FSFs, can be searched and voluntarily questioned. These persons are consolidated at a safe location, away from the site being searched and out of public view. Soldiers search and segregate all persons to prohibit them from communicating. Units only conduct mixed-sex searches as a last resort when they have no other means available. Soldiers search individuals for weapons and potentially exploitable materiel, to include pocket litter. Pocket litter includes a receipt or simple scrap of paper with a telephone number. After the initial search and questioning, individuals identified as a potential threat or accomplice are detained, processed, and can be tactically questioned. Units enroll these persons in the biometric database in accordance with theater policy.

3-59. The voluntary questioning of individuals on-site includes collecting information needed to complete the enrollment form on the tactical biometric collection device. The team leader moves between the search teams and Soldiers to share information and refine questioning. All persons found on-site are subject to questioning. The questioning stops immediately if the person objects or refuses to respond.

3-60. The lead Soldier tasked with questioning asks simple, direct questions and rehearses before engaging in questioning. At a minimum, Soldiers ask persons their name, association with the attacker and other individuals on-site, their residence (or unit for FSF), and reasons for being on-site. The lead Soldier briefs the interpreter on the questions asked and any performance expectations before conducting the questioning. The Soldier controls the pace and records the individual's translated comments using a digital recording device if available. If a second Soldier is available, that Soldier may act as a recorder.

3-61. Soldiers treat all individuals professionally and question individuals in a firm but calm manner. Persons found on-site are not subjected to any mistreatment, threats, intimidation, or other coercive behaviors.

Preserve the Site and Materiel

3-62. Preservation refers to protecting a site and its contents from damage, loss, or change. In general, the degree of preservation required depends on several considerations. These considerations include the purpose of the operation, sensitivity of the site, and significance of the site. When an FSF attack occurs at a FSF headquarters or facility, it is important that SE activities do not significantly disrupt or degrade the partnered unit's operational capability.

Transfer Control of the Site

3-63. Site transfer is a planned and orderly handover to another security force or FSF authority. The patrol leader or SE team leader transfers control of the site after collecting and processing relevant materiel and persons. Commanders assess the site's condition before determining how and when to transfer the site. When transferring partnered FSF facilities, barracks, or headquarters, Soldiers make an effort to return the site to its original state. Commanders explain the reasons for confiscating materiel and communicate with their FSF partners regarding when they can expect the return of these items.

3-64. Although units use the minimum amount of force to accomplish the mission, property damage can still occur. If tactical SE teams have changed, removed, or damaged FSF property, commanders have to consider the legal implications. Commanders ensure that Soldiers document damage and FSFs have the opportunity to resolve the property loss through the appropriate means.

Transfer Information, Persons, and Materiel

3-65. Soldiers transfer information, materiel, and persons having possible intelligence value to initial collection points identified in theater guidance. Soldiers then transfer these items to the appropriate technical exploitation facility. Higher headquarters establishes an initial collection point, such as a captured materiel exploitation center, to process and prioritize captured threat items. The initial collection points serve as a distribution point to support the transfer of the information and materiel to operational, strategic, or national technical exploitation facilities. Persons of interest are transferred to the detainee collection point in accordance with theater guidance.

TRAINING TO RECOVER

3-66. Training to recover consists of activities that promote resiliency, reduce stress, and enhance the unit's ability to conduct effective consequence management and public affairs.

Promote Resilience

3-67. Training to recover rests largely on a unit's resiliency and its ability to rebuild its relationship with partnered FSF following an attack. Commanders build resilient units by demonstrating the Army leadership attributes and competencies outlined in ADP 6-22. They create and sustain a positive climate through open communication, trust, cohesion, and teamwork. Actively engaging in leadership practices that positively encourage and motivate individuals builds personal resilience, thereby building a resilient unit. In a

multiple-partner environment, commanders promote these same attributes in FSFs, recognizing that through communication, trust, and cohesion, both units can recover from an FSF attack. Promoting resilience is also achieved by preventing and managing combat and operational stress.

Preventing and Managing Combat and Operational Stress

3-68. FSF attacks compound combat and operational stress. Combat and operational stress is a negative adaptation to high stress and potentially traumatic event exposure. Soldiers perceive and experience such an event as a threat to safety and stability. At the tactical level, an FSF attack undermines the trust and confidence requisite for Soldiers to operate effectively alongside their FSF partners. Deployed behavioral health personnel provide treatment interventions for combat and operational stress. Combat and operational stress efforts provided by behavioral health professionals are preventive in nature and consist of three primary prevention services:

- **Combat and operational stress universal prevention**. This service consists of surveillance and mitigation activities to reduce or avoid stressors and increase Soldiers' tolerance and resilience to severe stress. Universal prevention is applied at the unit level.
- **Combat and operational stress indicated prevention**. This service consists of surveillance and mitigation activities involving behavioral health personnel with individual Soldiers identified as having possible warning signs of combat and operational stress reactions.
- **Combat and operational stress treatment prevention**. This service consists of mitigation and stabilization activities to reduce long-term morbidity and complications in Soldiers with one or more diagnosable psychiatric or mental disorders.

3-69. Unit cohesion and morale is the best predictor of combat resiliency within a unit. Units with high cohesion tend to experience a lower rate of combat and operational stress reaction casualties than units with low cohesion or morale. High cohesion and morale enhance positive adaptations and promote resiliency in Soldiers. Unit cohesion and morale is founded on the following:

- **Confidence in leaders**. Good leaders demonstrate competency to their subordinates. They know what needs to be done, how it is done, who does it, and how long the task should take. Leaders earn authority and respect based on unit confidence in that leader's ability to guide the unit to success.
- **Confidence in training**. Training helps Soldiers develop the skills required to perform their duty. Confidence results from Soldiers knowing they have received the best possible training for combat and are fully prepared.
- **Confidence in the unit**. Each Soldier needs to be confident that their peers are competent, well trained, and prepared for the rigors of combat. Soldiers must live and train together to build trust and confidence in each other. Within larger organizations, units share the same SOPs and TTP so that Soldiers can quickly adapt and demonstrate competence when reorganization or cross-leveling occurs after an FSF attack.
- **Confidence in equipment**. Soldiers who learn to operate and maintain assigned equipment develop confidence in their ability to employ it. This, in combination with an individual's belief in personal capabilities, raises overall confidence in fighting ability.

Stress Reduction Techniques for Leaders

3-70. Leaders take proactive action to address combat stress. Unit leaders have the following stress management techniques available:

- Techniques for training include the following:
  - Be decisive and assertive; demonstrate competence and fair leadership.
  - Set realistic goals for progressive development of the individual and team.
  - Systematically test the achievement of goals and measure progress.
  - Learn the signs and symptoms of stress.
  - Be aware of background stress sources prior to combat; for example, family concerns and financial problems.

- Create a spirit to win under stress.
- Provide realistic training. Realistic training is a primary stress-reduction technique that builds confidence and assures Soldiers their leaders are doing what is best for them.
- Provide training for recognizing and mitigating combat stress. Training may be conducted by a certified behavioral health counselor or Master Resiliency Trainer.
- Practice and master stress-coping techniques.
- Encourage experienced Soldiers to mentor and teach new arrivals.

- Techniques for deployment include the following:
  - Ensure every effort is made to provide for the Soldiers' welfare.
  - Whenever possible provide sleep and rest, especially during continuous operations.
  - Recognize that duration and intensity of an operation increases stress.
  - Be aware of environmental stressors such as light, noise, temperature, and precipitation.
  - Recognize that individuals and units react differently to the same stressors.
  - Recognize that fear is a normal part of combat.
  - Rest minor stress casualties briefly, keeping them with their unit if possible.
  - Allow open communication with Soldiers and provide an upward, downward, and lateral flow of information.
  - Understand that stress in response to threatening or uncertain situations is normal.
  - Look for signs of stress and a decreased ability to tolerate stress.
  - Keep Soldiers well-supplied with food, water, and other essentials.
  - Provide mail, news, and other media.
  - Ensure access to medical, logistic, and human resource support.
  - Maintain morale, unit identity, and esprit de corps.
  - Keep unit members together and build cohesion.

3-71. Commanders promote resiliency by ensuring Soldiers are trained and aware of the resiliency resources available. These resources include medical providers, chaplains, Master Resiliency Trainers, and behavioral health counselors. For more information on combat and operational stress control see ATP 6-22.5.

Consequence Management and Public Affairs

3-72. FSF attacks are often a form of strategic messaging and, as such, they require a coordinated and unified response. Commanders manage the information-related consequences of an FSF attack by leveraging public affairs. *Public affairs* is communication activities with external and internal audiences (JP 3-61). Units conduct public affairs activities to help commanders shape the information environment through the distribution of truthful, timely, and factual information. Although the PAO is the commander's principal advisor and counselor on public affairs, all leaders conduct training on media engagement and messaging to better posture the unit for success in the information environment.

3-73. PAOs train fellow public affairs professionals, nonpublic affairs Soldiers, and Department of the Army Civilians to communicate the command's message. Training may be group media familiarization or focused one-on-one interview techniques with subject matter experts. To promote a combined response, PAOs remain ready to train and assist FSF leaders in communicating with the media. Effective training replicates operational realities and teaches the fundamentals of media and military interaction. Such training emphasizes that the media as a communication channel to internal and external audiences and not an adversary.

3-74. Public affairs training provides nonpublic affairs Soldiers and civilians with guidelines regarding interaction with the media, reactions to media encounters, and interview preparation. For commanders, staffs, and other Army leaders, public affairs training builds on individual training. It focuses on synchronizing public affairs considerations into the planning and decision-making process. It enables commanders, staffs, and other Army leaders to recognize how media coverage can affect Soldier morale, combat effectiveness, FSF perceptions, tactical execution, and mission accomplishment. Public affairs training enables

commanders, staffs, and other Army leaders to recognize, understand, and plan for the strategic, operational, and tactical repercussions of an FSF attack in the information environment.

3-75. Public affairs training is conducted by unit PAOs or, if unavailable, through the garrison public affairs office. For more information on public affairs see FM 3-61.

This page intentionally left blank.

Chapter 4

Foreign Security Force Planning and Operations

Although FSF threat prevention is an enduring process, the potential ramifications of a successful attack require commanders consider threat prevention and response throughout all steps of the planning process. Commanders deliberately plan threat prevention and response during all operations involving partnered FSFs. This chapter offers planning considerations that, when incorporated during troop leading procedures and the military decision-making process, assist units in properly addressing the FSF threat.

PLANNING CONSIDERATIONS

4-1. Commanders and staffs use the operations process to plan, prepare, execute, and assess military operations. This publication leverages both troop leading procedures and the military decision-making process to integrate FSF threat 8mitigation techniques into mission planning. Given the increased risk of FSF attacks during partnered operations, the planning guidance provided here assumes a mission involves FSFs.

4-2. Commanders and staffs have several tools available to address the FSF threat during planning. Commanders use a protection cell to integrate and synchronize protection tasks and systems during both routine activities and major operations. As such, a protection cell is an important resource for assessing the FSF threat and incorporating prevention and defeat measures into mission planning. The protection cell assists commanders with developing vulnerability assessments for locations where U.S. forces operate alongside FSFs. Protection cell members work closely with the intelligence staff to ensure their assessments accurately reflect the threat posed by the various FSFs a unit may operate alongside. The staff sections in these cells are important resources for drafting operational risk assessments to better inform decision making and protect U.S. forces.

4-3. As information drives intelligence, commanders and staffs strive to maintain situational awareness and understanding of both FSF threats and conventional threats in their AOs. Leaders use digital and analog communications to leverage information gathered from higher echelons, lower echelons, and adjacent units. Other key sources of information include AARs, situation reports, and patrol debriefs. Additionally, face-to-face interactions with the local population and FSFs often yields valuable information regarding threats across a joint operational area.

4-4. When planning operations, leaders consider risk and the importance of cultural implications associated with specific dates or events. For example, religious holidays, anniversaries, or recent significant incidents are all planning considerations that may impact operational design.

4-5. During operational planning, commanders balance FSF threat prevention and defeat measures against the risk to the mission and the risk to forces. During SFA and stability operations, commanders ensure that prevention and defeat measures do not cause unintentional harm and undermine their mission by alienating partnered forces. Conversely, commanders ensure that prevention and defeat measures do not put Soldiers at undue risk by isolating or exposing them and making them vulnerable to attack or capture. In the latter case, commanders adjust the mission parameters to better protect both Soldiers providing security and leaders deemed vulnerable to an FSF attack.

TROOP LEADING PROCEDURES

4-6. Troop leading procedures are a set of procedures used to assist units in preparing for operations. These procedures consist of seven steps:

- Receive the mission.
- Issue a warning order.
- Make a tentative plan.
- Initiate movement.
- Conduct reconnaissance.
- Complete the plan.
- Issue the order.
- Supervise and refine.

Paragraphs 4-7 through 4-19 describe these procedures.

Receive the Mission

4-7. Upon receipt of mission, leaders assess the higher echelon headquarters' order and begin analyzing mission requirements. They determine the type of operation and their role in it, the commander's intent, key tasks, and the desired end state. They confirm with the higher echelon commander and staff that they properly understand the mission.

4-8. At this step in the planning process, leaders consider the impact of FSFs, and they may seek clarification on FSF roles and limitations. Leaders should request information on the disposition of the partnered FSF unit and details regarding recent attacks in the area. Leaders need to know if soldiers from this unit attacked U.S. forces in the past. Leaders assess these factors to determine the threat level for the particular mission since such factors may drive subsequent planning considerations.

4-9. Units draft a tentative risk assessment for the operation and begin identifying control measures to mitigate the FSF threat. If the operation will occur at a site the unit frequents, then the unit consults the location's vulnerability assessment to address previously identified vulnerabilities or past incidents.

Issue a Warning Order

4-10. When issuing a warning order, leaders suggest threat awareness and mitigation measures relevant to the pending mission. They may identify the partnered FSF unit and review FSF members suspected of being potential threats. Leaders may also discuss the tentative task organization, security force roles, and partnership assignments for their subordinates to allow time for adequate preparation and rehearsals. A brief discussion of the mission objective and location allows subordinates to identify rally points, key locations, and defensible structures. An effective warning order also identifies Soldiers or teams designated as guardian angels.

4-11. Leaders remind Soldiers of the following items during preparation for combined operations:

- They should not use derogatory or offensive language (even in friendly conversation).
- They should be courteous and hospitable yet maintain awareness and present a hard target.
- They should respect cultural norms and behaviors.
- They should establish and maintain rapport and treat all persons with respect.

Make a Tentative Plan

4-12. When developing a tentative plan, leaders incorporate FSF threat considerations by comparing their initial concept of operations against potential enemy COAs. Does the concept properly account for FSF participation in the operation? How does the concept address an FSF attack? After identifying control measures to prevent or neutralize threat COAs, leaders then assess equipment and personnel available against force protection requirements to identify shortcomings or vulnerabilities. Leaders empower all individuals to provide recommendations on how to mitigate potential threats. Possible considerations during this step of the troop leading procedures include the following:

- Assessing the operation's likely duration. Leaders consider the impact this will have on security force planning and force protection considerations.
- Incorporating intelligence on enemy cells and activities into planning. Leaders consider enemy composition, disposition, strength, recent activities, ability to reinforce, and possible enemy courses of action, including using civilians as cover.
- Assessing the size, capabilities, and response time of adjacent or supporting units.
- Answering these questions:
  - If the operation includes a KLE, or other vulnerable encounter, what measures will be implemented to mitigate the FSF threat?
  - What will be the location, uniform, and weapon's status of those in attendance?
  - Who will be present for the engagement?
  - How many guardian angels are required?

Initiate Movement

4-13. Movement consists of the preparation and rehearsals relevant for the pending mission. To combat the FSF threat, leaders ensure guardian angels are identified, equipped, and have rehearsed their tasks. They also rehearse FSF attack response drills. These include immediate response drills, cordon protocols, casualty evacuation, and rally point responsibilities. During this step, the unit coordinates with adjacent and supporting units to facilitate a shared understanding of actions taken during an attack. Generally, the unit in contact remains in control until the threat is neutralized. Leaders take the time to ensure that all Soldiers understand the proper force protection posture, uniform, and weapon's status.

4-14. Initiating movement also requires ensuring that all mission-essential equipment is present and serviceable. Units inspect additional equipment including nonlethal weapons, SE kits, biometric toolkits, individual communications equipment, detainee processing kits, medical aid bags, and personal locator beacons. This equipment is inventoried, inspected for serviceability, and issued to the appropriate teams or individuals prior to an operation.

Conduct Reconnaissance

4-15. Leaders consider the FSF threat during their reconnaissance. During reconnaissance, leaders attempt to ascertain the layout of key buildings or compounds on the objective. This is especially important if their mission involves a KLE, ceremony, or large public event. Leaders determine whether the location is suitable for the event and how their unit can secure it. Leaders identify rally points, cordon parameters, casualty collection points, helicopter landing zones, and ingress and egress routes during their reconnaissance.

4-16. The plan addresses vulnerabilities and mitigation measures identified during the reconnaissance. Commanders and staffs consider these questions when making the plan:

- Where and when is the unit most vulnerable, and how could an FSF member attack the unit?
- Who would an attacker likely target and how could an attacker breach security?
- How would an attacker likely flee the scene?

Complete the Plan

4-17. Commanders provide general consequence management guidance in the coordinating instructions. However, they provide specific mitigation measures and responsibilities in the tasks to subordinate units. While mitigation measures are mission specific and focused, contingency plans and battle drills are broad enough to address rapidly changing circumstances. They should—

- Include guidance on engaging with the local population and instructions for de-escalating volatile situations.
- Describe the threat, the environment, and partnered unit disposition.
- Discuss vulnerabilities inherent to the location and the measures used to mitigate these vulnerabilities.

- Address the task organization, scheme of maneuver, and scheme of protection to ensure teams and individuals are not unduly isolated or exposed to a potential attack.
- Describe access control procedures and identification methods for FSFs on the objective.
- Clearly define the tasks and roles of the FSFs during the operation.
- Identify key partnerships between U.S. and FSF leaders and where these personnel will be located.
- Describe how units will use guardian angels during KLEs or other events and who they are protecting.
- Clearly identify all layers of the unit's defense in depth and which subordinate team is responsible for securing each layer.
- Identify rally points, cordon protocols, and attack response measures unique to the mission location and objective.

Issue the Order

4-18. When issuing the order, leaders emphasize FSF threat prevention and response measures relevant to the mission. They also include a current intelligence summary that addresses recent FSF attacks in their AO. Leaders clearly articulate their security plan for the operation and identify security responsibilities in the tasks to subordinate units. Additional considerations that leaders might address during the operation order brief include—

- Mission, risk management, safety considerations, ROE, and escalation of force policies.
- Weapon's status and restrictions for both U.S. Soldiers and FSFs.
- A backbrief to ensure that all Soldiers understand the force protection and risk mitigation measures in place to prevent an attack. An effective backbrief requires Soldiers to describe their responsibilities to the unit's overall security plan.
- Separate briefings for U.S. forces if risk mitigation measures cannot be shared with partnered FSFs.

Supervise and Refine

4-19. The final step of troop leading procedures facilitates dialogue and coordination between leaders and subordinates to ensure the plan is properly resourced, feasible, and understood by all. When supervising and refining, leaders ensure that subordinates and partnered FSFs understand the coordination measures required to synchronize actions between units and echelons. Final pre-combat checks and inspections ensure PPE and mission-essential equipment is present and serviceable. Finally, this step ensures subordinates or partnered FSFs who have questions or concerns about the mission seek clarification from leaders. FSF threat considerations include—

- Adjusting the plan based on updated information collection.
- Making final coordination with adjacent units, quick reaction forces, and higher headquarters.
- Conducting a rehearsal of concept drill with key leaders and partnered forces.
- Observing subordinates as they rehearse with FSFs. Leaders look for signs of animosity or strange behavior that may indicate a potential threat.
- Reviewing weapons handling and arming status with FSFs.
- Rehearsing FSF attack response drills with relevant personnel.
- Challenging Soldiers to backbrief the ROE and escalation of force procedures.
- Briefing the commander or designated representative on the concept of operations and any unmitigated risks or potential shortcomings.

THE MILITARY DECISION-MAKING PROCESS

4-20. Commanders and staffs using the military decision-making process consider FSF threat prevention through each of the steps. They focus on producing an order that meets the commander's intent while providing subordinates with the information, resources, and flexibility to implement control measures that reduce the likelihood and impact of a potential attack.

Receipt of Mission

4-21. Upon receipt of mission, commanders address their intent for partnering with FSFs during the operation. They explain how they envision synergy between U.S. forces and FSFs accomplishing the mission, and they describe the role of each. Commanders and staffs assess the time available and determine when and how partnered forces will be alerted to the mission and what initial guidance they will receive. The warning order includes planning and preparation guidance, such as rehearsals and coordination that subordinate units conduct to mitigate an FSF threat.

Mission Analysis

4-22. During mission analysis, commanders and staffs develop a mission statement, commander's intent, and initial planning guidance. They conduct intelligence preparation of the battlefield, and they propose the initial commander's critical information requirements and essential elements of friendly information (EEFIs).

4-23. When conducting mission analysis, the staff considers threat, vulnerability, and risk to aid in developing a concept of operations that both achieves the unit's objective and mitigates the potential for an FSF attack. Intelligence preparation of the battlefield is an essential component of mission analysis. It considers the potential for an FSF attack. Given the mission, the staff determines if FSFs pose a threat to friendly operations and how FSFs may use their capabilities to impact these operations. Like the conventional enemy COAs developed during intelligence preparation of the battlefield, the staff also assists in developing potential FSF threat COAs for combined operations. The staff can then plan against and analyze these COAs during COA analysis. The staff then distributes an updated threat assessment to subordinate units and other staff sections to be addressed in their running estimates.

4-24. If a mission will occur at a previously assessed location, the unit staff references the vulnerability assessment when developing the risk assessment. If a mission will occur at a new or unfamiliar location, the unit staff takes the time and resources available to conduct a hasty vulnerability assessment of the compound and buildings they will use during the mission. Often, a hasty vulnerability assessment relies on maps and satellite imagery to provide a basic understanding of an objective's terrain.

4-25. Subordinate units and other staff sections use the threat assessment, including the FSF threat COAs, and the vulnerability assessment to develop a mission-specific risk assessment. The risk assessment identifies any control measures to mitigate an FSF attack. Once the staff completes these processes and the unit commander approves them, the staff updates the commander's critical information requirements and EEFIs to reflect relevant control measures identified in the risk assessment.

4-26. The intelligence and protection cells work together to ensure threat mitigation measures are included in friendly COA development. To prevent undue bias during COA development, the unit staff may produce COA evaluation criteria at the conclusion of mission analysis. FSF attack mitigation and response measures may be included as evaluation criteria for COA analysis and comparison. Additional information on the FSF threat is included in the second warning order.

COA Development

4-27. The key outputs from COA development are COA statements and sketches. Each COA statement and sketch includes a clear task organization that depicts both U.S. and partnered FSF units. The task organization accounts for a potential FSF attack by ensuring units can reinforce and support each other. Considerations should also be made for the tasks assigned to U.S. and multinational partners, ensuring that culturally sensitive tasks (for example, searching local civilians or clearing a religious site) are assigned to the appropriate unit. See ADP 5-0 for more on COA development.

COA Analysis

4-28. An effective COA analysis for combined operations includes an FSF attack; this is particularly important if the operation includes a KLE, ceremony, or other high-profile event that may prove attractive to a potential attacker. The decision support matrix, an important output of COA analysis, reflects the commander's guidance regarding an FSF attack and the steps to take should an attack occur. During COA analysis commanders and staffs address these questions:

- How will an attack impact the mission?
- Could an attack trigger the reserve?

The execution matrix, another important output of COA analysis, accounts for the time and coordination required to implement threat mitigation measures. This includes the time needed to clear and secure critical sites before events like KLEs.

COA Comparison

4-29. If FSF threat considerations are included as evaluation criteria during COA analysis, these may be weighted per the commander's guidance during COA comparison. However, if the FSF threat is not formally addressed as evaluation criteria, then it should be discussed with the commander during COA comparison. Commanders and staffs consider how well each COA mitigates and reacts to an attack without compromising the mission.

COA Approval

4-30. Once a commander has approved a COA, that commander's staff ensures that the commander's critical information requirements, risk reduction control measures, and EEFIs account for updated threat prevention and response measures. The staff updates the decision support matrix and execution matrix to reflect the commander's guidance regarding changes made by a potential threat or an attack. The warning order includes more detailed guidance on threat mitigation and force protection measures.

Orders Production, Dissemination, and Transition

4-31. During orders production and dissemination, the unit staff verifies that subordinate units understand the plan, the role of partnered FSFs, and the control measures directed from higher echelons to mitigate a potential FSF attack. The unit staff coordinates with partnered forces and may provide a version of the order that protects critical information, such as EEFIs and FSF attack response measures, while still allowing the partnered force to contribute effectively. The unit staff ensures that subordinate units have the resources, intelligence, and equipment to protect the force and mitigate the threat.

PREPARATION

4-32. Plans, orders, and rehearsals for operations involving FSFs deliberately address the FSF threat by outlining mission-specific force protection measures and TTP tailored to the threat. All members of the team—especially those Soldiers charged with performing duties as guardian angels or other key elements of the unit's security posture—understand and rehearse these mission-specific measures. Planning and rehearsing force protection and security operations is a critical step in preventing and defeating attacks.

4-33. All units rehearse FSF threat prevention and defeat procedures before all combined operations. Rehearsing actions before execution allows participants to become familiar with the operation and translate a written plan into coordinated action. Rehearsals also help orient Soldiers to the conditions and terrain they will find on the objective. Moreover, the repetition of required tasks during the rehearsal leaves a lasting mental picture of the sequence of key actions within an operation. Threat mitigation techniques and battle drills should be addressed in unit SOPs and rehearsed prior to execution.

4-34. In addition to conducting a rehearsal of concept drill, leaders ensure that rehearsals are conducted at the team, squad, and platoon levels to ensure all elements of the unit's security infrastructure understand their roles should an attack occur. External security, mobile security, internal security, the reserve or quick reaction force, and guardian angels all rehearse their actions in the event of an attack. These team or squad rehearsals may culminate with the entire unit rehearsing for an FSF attack.

4-35. Effective leaders carefully assess whether they rehearse attack response drills with their partnered FSFs since this may compromise a unit's security by revealing information that a potential attacker can exploit. Units conduct FSF attack rehearsals without partnered forces in a location where they cannot be observed by multinational partners.

4-36. When preparing for combined operations, SFA missions, or stability operations, a patrol leader briefs attached personnel, such as key leaders or advisors, on the unit's FSF threat prevention and defeat measures. This brief includes explaining the key leader or advisors' actions in the event of an attack and clearly articulating the prevention or defeat measures the unit will implement during the mission. If possible, these attached personnel participate in the unit's rehearsals. If they are unavailable for rehearsals, the unit uses role players to simulate the attached personnel.

4-37. During preparation, leaders ensure that Soldiers do not share threat prevention and response measures with partnered forces as this may compromise the unit's security. Soldiers protect information such as predetermined rally points, emergency ingress and egress routes, and security force rotation schedules as EEFIs.

ASSESS

4-38. Lessons learned, retained, and implemented help units adapt to an ever growing array of threats. In the aftermath of an FSF attack, units assess the effectiveness of their threat prevention and response measures to identify lessons learned for future operations. AARs are an effective means for identifying these lessons; teams, squads, small units, and staffs conduct AARs. To ensure the widest dissemination, each echelon shares lessons learned both laterally and vertically. Agile and adaptive units can then review and amend risk assessments, force protection measures, TTP, and SOPs. They can then incorporate lessons learned into future operations.

This page intentionally left blank.

Source Notes

This division lists sources by page number. Where material appears in a paragraph, it lists both the page number followed by the paragraph number.

Chapter 1

1-1 "This year's spring…": Islamic Emirate of Afghanistan quoted in Bill Roggio, "Taliban Promise Suicide Assaults, 'Insider Attacks' in this Year's Spring Offensive," *Foundation for the Defense of Democracies Long War Journal*, 29 April 2013. Available at https://www.fdd.org/analysis/2013/04/29/taliban-promise-suicide-assaults-insider-attacks-in-this-years-spring-offensive.

1-2 **The Soviet Union in Afghanistan.** Vignette adapted from Center for Army Lessons Learned (CALL), Call Handbook No. 12-07. *Inside the Wire Threats-Afghanistan: Green on Blue* (Fort Leavenworth, KS), February 2012, 2.

1-3 **Jordanian Soldier Kills Three U.S. Soldiers.** Vignette adapted from Memorandum 4 Nov. 2016 King Faisal Air Base Shooting AR 15-6 Investigation Summary. 07 March 2017. https://www.socom.mil/FOIA/Documents/USSOCOM%20Jordan%2015-6%20%20For%20Public%20Release%20(Redacted)%20Final%20-%207%20MAR%2017.pdf.

1-3 1-12 "A study conducted…": Summarized from Jeffrey Bordin, *A Crisis of Trust and Cultural Incompatibility: A Red Team Study of Mutual Perceptions of Afghan National Security Force Personnel and U.S. Soldiers in Understanding and Mitigating the Phenomena of ANSF-Committed Fratricide-Murders* (Washington, D.C.: The National Security Archive and Chadwyck-Healey, 12 May 2011), 3.

1-4 **Attacker Motivated by Family Member's Detention.** Vignette adapted from Jeffrey Bordin, *A Crisis of Trust and Cultural Incompatibility: A Red Team Study of Mutual Perceptions of Afghan National Security Force Personnel and U.S. Soldiers in Understanding and Mitigating the Phenomena of ANSF-Committed Fratricide-Murders* (Washington, D.C.: The National Security Archive and Chadwyck-Healey, 12 May 2011), 12–14.

1-5 **Desecration of Religious Materials Inspires Attack.** Vignette adapted from Asymmetric Warfare Group, "The Insider Threat in Afghanistan," Brief, 03 February 2014.

1-6 **Corrupt Officer Attacks U.S. Air Force Advisors.** Vignette adapted from Oriana Pawlyk, "Questions Remain As Families Mourn Victims Of 2011 Green-On-Blue Kabul Attack," *Air Force Times*, 27 April 2016.

1-7 **Taliban Co-opts Afghan Border Policeman.** Vignette adapted from Bilal Sarwary, "Anatomy of an Afghan 'Turncoat' Killer," from *BBC News* at bbc.co.uk/news, 21 October 2011. Available at https://www.bbc.com/news/magazine-14713523.

1-8 **Attacker Motivated by Abuse.** Vignette adapted from Jeffrey Bordin, *A Crisis of Trust and Cultural Incompatibility: A Red Team Study of Mutual Perceptions of Afghan National Security Force Personnel and U.S. Soldiers in Understanding and Mitigating the Phenomena of ANSF-Committed Fratricide-Murders* (Washington, D.C.: The National Security Archive and Chadwyck-Healey, 12 May 2011), 57.

Chapter 2

2-1 2-5 Summarized from Jeffrey Bordin, *A Crisis of Trust and Cultural Incompatibility: A Red Team Study of Mutual Perceptions of Afghan National Security Force Personnel and U.S. Soldiers in Understanding and Mitigating the Phenomena of ANSF-Committed Fratricide-Murders* (Washington, D.C.: The National Security Archive and Chadwyck-Healey, 12 May 2011), 57.

2-7 2-34 The Predictive Classification Concept discussion is adapted from the Department of Energy, *Predictive Modeling for Insider Threat Mitigation* (Springfield, VA: National Technical Information Service, 2009), 5–9.

2-8 Figure 2-1. Department of Energy, *Predictive Modeling for Insider Threat Mitigation* (Springfield, VA: National Technical Information Service, 2009), 7.

2-13 2-69–2-70 Concept adapted from Pete Escamilla and Eric Lopez, "Securing the Security Force Assistance Advisors in Afghanistan," from *Small Wars Journal*, 10 September 2013. Available at https://smallwarsjournal.com/jrnl/art/securing-the-security-force-assistance-advisors-in-afghanistan.

2-14 Figure 2-2. Figure adapted from Pete Escamilla and Eric Lopez, "Securing the Security Force Assistance Advisors in Afghanistan," from *Small Wars Journal*, 10 September 2013. Available at https://smallwarsjournal.com/jrnl/art/securing-the-security-force-assistance-advisors-in-afghanistan.

Glossary

The glossary lists acronyms and terms with Army and joint definitions. Term for which ATP 3-37.15 is the proponent publication (the authority) is marked with an asterisk (*). The proponent publication for other terms is listed in parentheses after the definition.

SECTION I – ACRONYMS AND ABBREVIATIONS

AAR	after action review
ADP	Army doctrine publication
AO	area of operations
AR	Army regulation
ATP	Army techniques publication
COA	course of action
CQM	close-quarters marksmanship
DA	Department of the Army
DODD	Department of Defense directive
EEFI	essential element of friendly information
FM	field manual
FSF	foreign security force
HNSF	host-nation security forces
JP	joint publication
KLE	key leader engagement
NATO	North Atlantic Treaty Organization
OE	operational environment
PAO	public affairs officer
PPE	personal protective equipment
ROE	rules of engagement
SE	site exploitation
SFA	security force assistance
SOP	standard operating procedure
TTP	tactics, techniques, and procedures
U.S.	United States

SECTION II – TERMS

biometrics

The process of recognizing an individual based on measurable anatomical, physiological, and behavioral characteristics. (JP 2-0)

***co-option**

A process an enemy, insurgent, or terrorist organization uses for recruiting an existing foreign security force member.

detection

In tactical operations, the perception of an object of possible military interest but unconfirmed by recognition. (JP 3-11)

deterrence

The prevention of action by the existence of a credible threat of unacceptable counteraction and/or the belief that the cost of an action outweighs the perceived benefits. (JP 3-0)

exploitation

(joint) Taking full advantage of any information that has come to hand for tactical, operational, or strategic purposes. (JP 2-01.3)

force protection

Preventive measures taken to mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities, and critical information. (JP 3-0)

foreign security forces

Forces, including, but not limited to military, paramilitary, police, and intelligence forces; border police, coast guard, and customs officials; and prison guards and correctional personnel, that provide security for a host nation and its relevant population or support a regional security organization's mission. (FM 3-22)

high-value target

A target the enemy commander requires for the successful completion of the mission. (JP 3-60)

public affairs

Communication activities with external and internal audiences. (JP 3-61)

risk management

The process to identify, assess, and control risks and make decisions that balance risk cost with mission benefits. (JP 3-0)

site exploitation

(joint) A series of activities to recognize, collect, process, preserve, and analyze information, personnel, and/or material found during the conduct of operations. (JP 3-31)

tactical questioning

The field-expedient initial questioning for information of immediate tactical value of a captured or detained person at or near the point of capture and before the individual is placed in a detention facility. (JP 3-63)

References

All websites accessed on 18 November 2019.

REQUIRED PUBLICATIONS

These documents must be available to intended users of this publication.

DOD Dictionary of Military and Associated Terms. November 2019.

ADP 1-02. *Terms and Military Symbols*. 14 August 2018.

FM 1-02.1. *Operational Terms*. 21 November 2019.

RELATED PUBLICATIONS

These documents contain relevant supplemental information.

JOINT AND DEPARTMENT OF DEFENSE PUBLICATIONS

Most joint doctrinal publications are available online at https://www.jcs.mil/Doctrine/. Most Department of Defense issuances are available at https://www.esd.whs.mil/dd/.

DODD 3115.09. *DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning*, incorporating Change 2. 11 October 2012.

JP 2-0. *Joint Intelligence*. 22 October 2013.

JP 2-01.3. *Joint Intelligence Preparation of the Operational Environment*. 21 May 2014.

JP 3-0. *Joint Operations,* incorporating Change 1. 17 January 2017.

JP 3-07.2. *Antiterrorism*. 14 March 2014.

JP 3-11. *Operations in Chemical, Biological, Radiological, and Nuclear Environments*. 29 October 2018.

JP 3-31. *Joint Land Operations*. 03 October 2019.

JP 3-60. *Joint Targeting*. 28 September 2018.

JP 3-61. *Public Affairs*, incorporating Change 1. 17 November 2015.

JP 3-63. *Detainee Operations*. 13 November 2014.

ARMY PUBLICATIONS

Most Army doctrinal publications are available online at https://armypubs.army.mil/default.aspx.

ADP 3-37. *Protection*. 31 July 2019.

ADP 5-0. *The Operations Process*. 31 July 2019.

ADP 6-22. *Army Leadership and the Profession*. 31 July 2019.

AR 15-6. *Procedures for Administrative Investigations and Boards of Officers*. 01 April 2016.

AR 381-12. *Threat Awareness and Reporting Program*. 01 June 2016.

AR 381-100. *Army Human Intelligence Collection Programs* (S//NF). 22 February 2016. (This classified publication is available on the SIPRNET. Contact the preparing agency of this publication for access instructions.)

ATP 2-22.82. *Biometrics-Enabled Intelligence*. 02 November 2015.

ATP 2-22.85/MCRP 3-33.1J/NTTP 3-07.16/AFTTP 3-2.85/CGTTP 3-93.6. *Multi-Service Tactics, Techniques, and Procedures for Tactical Employment of Biometrics in Support of Operations*. 06 May 2016.

ATP 3-37.2. *Antiterrorism*. 03 June 2014.

ATP 3-39.35. *Protective Services*. 31 May 2013.

ATP 3-55.4. *Techniques for Information Collection During Operations Among Populations*. 05 April 2016.

ATP 3-90.15. *Site Exploitation*. 28 July 2015.

ATP 6-22.5. *A Leaders Guide to Soldier Health and Fitness*. 10 February 2016.

FM 2-22.3. *Human Intelligence Collector Operations*. 06 September 2006.

FM 3-22. *Army Support to Security Cooperation*, incorporating Change 1. 22 January 2013.

FM 3-39. *Military Police Operations*. 09 April 2019.

FM 3-61. *Public Affairs Operations*. 01 April 2014.

FM 6-27/MCTP 11-10C. *The Commander's Handbook on the Law of Land Warfare*, incorporating Change 1. 07 August 2019.

NATO PUBLICATIONS

Most NATO publications are available online at https://assistca.dla.mil/.

NATO ATP-3.16.1. *Countering Insider Threats (CIT)*. 13 April 2016.

NATO STANAG 6513. *Countering Insider Threats (CIT)*. 13 April 2016.

OTHER PUBLICATIONS

Bordin, Jeffrey. *A Crisis of Trust and Cultural Incompatibility: A Red Team Study of Mutual Perceptions of Afghan National Security Force Personnel and U.S. Soldiers in Understanding and Mitigating the Phenomena of ANSF-Committed Fratricide-Murders*. Washington, D.C.: The National Security Archive and Chadwyck-Healey, 2011.

Center for Army Lessons Learned (CALL), Call Handbook No. 12-07. *Inside the Wire Threats-Afghanistan: Green on Blue* (Fort Leavenworth, Kansas), February 2012.

Escamilla, Pete and Eric Lopez. "Securing the Security Force Assistance Advisors in Afghanistan." *Small Wars Journal*. 10 September 2013. Available at https://smallwarsjournal.com/jrnl/art/securing-the-security-force-assistance-advisors-in-afghanistan.

National Defense Authorization Act of 2017. https://www.congress.gov/bill/114th-congress/senate-bill/2943.

Pawlyk, Oriana. "Questions Remain As Families Mourn Victims of 2011 Green-On-Blue Kabul Attack." *Air Force Times*. 27 April 2016.

Roggio, Bill. "Taliban Promise Suicide Assaults, 'Insider Attacks' in this Year's Spring Offensive." *Foundation for the Defense of Democracies Long War Journal*. 29 April 2013. Available at https://www.fdd.org/analysis/2013/04/29/taliban-promise-suicide-assaults-insider-attacks-in-this-years-spring-offensive.

Sarwary, Bilal. "Anatomy of an Afghan 'Turncoat' Killer." From *BBC News* at bbc.co.uk/news. October 21, 2011. Available at https://www.bbc.com/news/magazine-14713523.

TRISA, *Insider Threat Handbook* (Fort Leavenworth, Kansas), 14 October 2011.

U.S. Department of Energy. *Predictive Modeling for Insider Threat Mitigation*. Springfield, VA: National Technical Information Service, 2009.

United States Special Operations Command. "4 November 2016 King Faisal Air Base Shooting AR 15-6 Investigation Summary," memorandum. 07 March 2017. MacDill Air Force Base, Florida. Available at https://www.socom.mil/FOIA/Documents/USSOCOM%20Jordan%2015-6%20%20For%20Public%20Release%20(Redacted)%20Final%20-%207%20MAR%2017.pdf.

WEBSITES

Army Training Requirements and Resources System, https://www.atrrs.army.mil/Default.aspx.

Center for Army Lessons Learned, https://call2.army.mil.

Joint Lessons Learned Information System, www.jllis.mil.

Defense Language Institute Foreign Language Center, http://www.dliflc.edu/.

PRESCRIBED FORMS

This section contains no entries.

REFERENCED FORMS

Most Department of the Army (DA) forms are available online at https://armypubs.army.mil/. Most Department of Defense forms are available online at https://www.esd.whs.mil/dd/.

DA Form 2028. *Recommended Changes to Publications and Blank Forms*.

DA Form 2823. *Sworn Statement*.

DA Form 4137. *Evidence/Property Custody Document*.

DD Form 2745. *Enemy Prisoner of War (EPW) Capture Tag*.

This page intentionally left blank.

Index

Entries are by paragraph number.

A

access control, badges and, 2-55
methods for, 2-54
modifications to, 2-59
reporting unauthorized persons, 2-57
restricted locations and, 2-56
security patrols and, 2-58

accountability, methods of, 2-19
of foreign security forces, 2-20
personnel, 2-18
uniforms and equipment, 2-17

assessments, types of, 2-38

B

behavioral indicators, category 1, 2-30
category 2, 2-31
category 3, 2-32

biometric screening, 2-46

biometrics, benefits of, 2-47
defined, 2-46
forensics and, 2-49
recruitment and, 2-48

C

combat and operational stress, morale and, 3-69
prevention of, 3-68
reduction techniques, 3-70

co-option, defined, 1-21
methods for, 1-21
recruitment, 1-22

course of action analysis, outputs of, 4-28

course of action approval, outputs of, 4-30

course of action comparison, 4-29

course of action development, outputs of, 4-27

criminal attack, 1-19

criticality assessment, 2-40

cultural awareness, components of, 2-7
guidelines during operations, 2-5
professionalism and, 2-6

cultural awareness training, 3-5
methods for, 3-6
while deployed, 3-7

D

defense in depth, 2-69
external security, 2-71
framework of, 2-70
internal security, 2-73
mobile security, 2-72
reserve, 2-74

detainee processing, forms, 3-39
principles of, 3-35–3-38
training for, 3-40

detainee processing kit, 3-41

detaining processing, principles of, 3-32

detection, defined, 2-25

deterrence, defined, 2-60

E

enemy attack, 1-20

environment, biographical information and, 2-22
components of, 2-21

environmental baseline, 2-21
methods for establishing, 2-23
relief in place and, 2-24

escalation of force, 3-14
language training, 3-15

exploit, purpose of, 2-90
pursuit operations and, 2-91
site preservation, 2-92

exploitation, defined, 2-89

F

force protection, adjustments to, 2-63
defined, 2-61
threat courses of action and, 2-62
weapon status and, 2-64

foreign security force threat, 1-1
information sources, 4-3
planning considerations, 4-4
risk and, 4-5

foreign security force threat attack, 1-1
accountability during, 2-85
categories of, 1-10
characteristics of, 1-2
combined response, 2-88
environment, 1-7
historical context of, 1-9
locations of, 1-5
methods, 1-3
purpose of, 1-6
recover, 2-98
reporting procedures, 2-87
response framework, 2-81
roles and responsibilities during, 2-82–2-84
security during, 2-86
targets, 1-4, 1-8

foreign security forces, defined, 1-1

G

general attack, causes of, 1-25
corruption, 1-26
drug abuse, 1-25
mental illness, 1-25
resource disputes, 1-27

guardian angel training, components of, 3-22
resources for, 3-24

guardian angels, 2-75
at training events, 2-80
equipment, 3-23
locations for use, 2-77
patrolling and, 2-79
personnel selection, 3-21
point of dominance and, 2-78
responsibilities of, 2-76

H

high-value target, defined, 1-7

I–J–K

ideological attack, 1-16
indicators, 1-17

impersonation, 1-24

infiltration, 1-23

information, joint and Army repositories for, 2-53
sources of, 2-51

information sharing, 2-50
detainees and, 2-52
interviews, 2-96

L

lessons learned, 2-97, 4-38

M–N

military decision-making process, 4-20
mission analysis, course of action evaluation criteria, 4-26
outputs of, 4-22
risk assessment, 4-25
threat courses of action, 4-23
vulnerability assessment, 4-24
mission preparation, attached personnel, 4-36
drills and rehearsals, 4-13
operations security, 4-37
pre-combat checks, 4-14
rehearsals, 4-32–4-35
roles and responsibilities, 4-19

O

operation order, 4-17
briefing considerations, 4-18
operations order production, roles and responsibilities, 4-31
operations process, 4-1

P–Q

personal attack, 1-11
causes of, 1-12
combat stress, 1-14
cultural animosity, 1-12
prevention of, 1-15
xenophobia, 1-13
personnel searches, procedures for, 3-33–3-34
personnel selection, characteristics, 3-2
rank and, 3-4
posture, 2-65
characteristics of, 2-66
personal protective equipment and, 2-68
weapon status and, 2-67
predictive classification concept, 2-34
data and, 2-36
method for use, 2-35
prevention, characteristics of, 2-4
prevention and response framework, 2-1
defeat, 2-3
deterrence, 2-2
exploit, 2-3
prevention, 2-2
recover, 2-3
protection cell, 4-2
public affairs, defined, 3-72
information operations and, 3-74
purpose of, 3-72
training methods, 3-73
training resources, 3-75

R

rapport, benefits of, 2-9
building and maintaining, 2-14–2-15
challenges to, 2-8
compromise and, 2-13
leadership and, 2-12
military competence and, 2-11
planning engagements, 2-16
preparation for, 2-10
reactionary attack, 1-18
receipt of mission, 4-21
receive the mission, information requirements, 4-8
risk assessment, 4-9
reconnaissance, considerations for, 4-15
vulnerability and, 4-16
recover, 2-102
engagement, 2-100
morale, 2-101
public affairs, 2-99
resiliency, importance of, 3-67
resources for, 3-71
risk assessment, 2-45
risk management, defined, 2-37

S

security force assistance advisor, aptitude for, 3-3
site exploitation, 3-46
area searches, 3-55
collective training, 3-52
compensation, 3-64
defined, 2-93
forensics and, 3-51
hasty and deliberate, 3-47
information requirements, 3-56
kit contents, 2-94
locations for, 2-95
material seized, 3-57
methods for questioning, 3-60
personnel processing, 3-58
purpose of, 3-48
security, 3-54
site preservation, 3-62
site transfer, 3-63
task organization, 3-50
training for, 3-49
transfer of persons and materiel, 3-65
treatment of personnel, 3-61
use of cordons, 3-53
voluntary questioning, 3-59
small unit planning, course of action assessment, 4-12

T–U

tactical questioning, defined, 3-42
principles of, 3-43
procedures for, 3-44
training for, 3-45
tactics, techniques, and procedures, purpose of, 3-19
threat assessment, 2-39
threat detection, 2-25
behavioral indicators, 2-29
environmental indicators, 2-27
physiological indicators, 2-28
reporting and, 2-33
types of indicators, 2-26
training, 3-1, 3-8, 3-18, 3-31, 3-66
biometric toolkit, 3-16
communications, 3-17
methods for, 3-12
threat detection, 3-9
threat indicators, 3-10
use of credentials, 3-11
while deployed, 3-13, 3-20
troop leading procedures, 4-6
receive the mission, 4-7

V

vulnerability assessment, 2-41
purpose of, 2-42
triggers and, 2-44
weapon-target pairing and, 2-43

W–X–Y–Z

warning order, 4-10–4-11
weapons training, components of, 3-25
dry fire, 3-26
simulation-based, 3-27
stress shoot, 3-30
targets, 3-29
use of simunitions, 3-28

ATP 3-37.15, C1

23 May 2025

By Order of the Secretary of the Army:

RANDY A. GEORGE
General, United States Army
Chief of Staff

Official:

MARK F. AVERILL
Administrative Assistant
to the Secretary of the Army
2513406

DISTRIBUTION:
Active Army, Army National Guard, and United States Army Reserve. Distributed in electronic media only(EMO).

This page intentionally left blank.

This page intentionally left blank.

PIN: 206136-001