2020 USAF Year of Integrated Base Defense

DEFENDING AIR BASES IN AN AGE OF INSURGENCY

Integrated Base Defense Principles for Commanders

VOLUME III

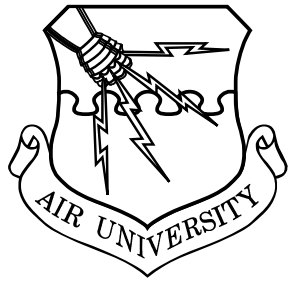
Edited by

Col Shannon W. Caudill, USAF, Retired

with Maj Gen Andrea D. Tullos, USAF, and Col Erik K. Rundquist, USAF, retired

Foreword by Gen James M. Holmes, USAF

Afterword by Maj Gen John T. Wilcox II, USAF



Defending Air Bases in an Age of Insurgency

Volume III: Integrated Base Defense Principles for Commanders

Shannon W. Caudill, Editor
Colonel, USAF, Retired

Andrea D. Tullos
Major General, USAF

Erik K. Rundquist
Colonel, USAF, Retired

Air University Press
Maxwell Air Force Base, Alabama

Air University Press

Director
Maj Richard Harrison

Managing Editor
Dr. Christopher Rein

Design and Production Managing Editor
Luetwinder T. Eaves

Project Editor
Donna Budjenska

Editorial Assistant
Kimberly Leifer

Cover Art, Book Design, and Illustrations
Daniel Armstrong
Timothy Thomas

Composition and Prepress Production
Nedra Looney

Air University Press
600 Chennault Circle, Building 1405
Maxwell AFB, AL 36112-6010

https://www.airuniversity.af.edu/AUPress/

Facebook: https://www.facebook.com/AirUnivPress
and
Twitter: https://twitter.com/aupress

Library of Congress Cataloging-in-Publication Data

Caudill, Shannon W.
Defending air bases in an age of insurgency /
Shannon W. Caudill, Colonel, USAF.
pages cm
Includes bibliographical references and index.
ISBN 978–1–58566–241–8
1. Air bases—Security measures—United States.
2. United States. Air Force—Security measures.
3. Irregular warfare—United States. I. Title
UG634.99.C48 2014
358.4'14—dc23

2014012026

Published by Air University Press in March 2021

This book is dedicated to those who defend air bases—our Airmen, members of the joint force, and our joint and coalition partners.

*****

We also present this book in memory of a gifted base defender, commander, and warrior:
Lt Col Brian L. Copper Jr., USAF

Contents

Illustrations *vii*

Foreword *ix*
James M. Holmes

About the Authors *xiii*

Acknowledgments *xv*

Introduction *xvii*

Ten Base Defense Principles for Commanders *xxiii*

1 You Own It! 1

2 Get Left of the Boom: Deter, Disrupt, Deceive 5

3 Influence the Base Security Zone . . . or Someone Else Will 11

4 Unity of Effort: Synchronize the Fight 17

5 Everyone Must Have a Role in Base Defense . . . and Play It! 23

6 Intelligence Drives Maneuver: A Joint-Interagency Approach Is Critical 27

7 Air-mindedness Includes Using Air Assets for Base Defense 31

8 Law Enforcement Skills Are Critical to Base Defense and Irregular Warfare 35

9 Manage the Risk: Commit Intellectual Capital to the Fight 41

10 Nowhere to Hide: Anticipate Future Threats and Develop Countermeasures 47

Conclusion 55

Afterword 59
John T. Wilcox II

Appendix A: Base Defense Terminology 61

Appendix B: Recommended Reading List for Air Base Defense and Counterinsurgency 67

Appendix C: Notable Airfield Attacks 69

Appendix D: Relevant Quotations about Air Base Defense 73

Abbreviations 77

Bibliography 79

Index 87

Illustrations

Figures

1	Integrated defense effects	*xviii*
2	Overhead shot of Camp Bastion	1
3	Notional defense-in-depth schematic	2
4	The "Dover Effect"	6
5	Fort Dix Six	8
6	Base boundary considerations	12
7	Intelligence process	30
8	Risk-Management Process	44

Tables

1	Notable soft target attacks	38
2	Statistical comparison of fixed-wing aircraft destroyed and damaged by air base attack	48

Foreword

Likely readers of this book do not need to be told the United States has been in a continual state of conflict since 1990. It is sobering to think an entire generation of Airmen and their families entered the Air Force, served over two decades, and retired in this time frame after completing a steady stream of deployments in the skies over, or on the ground in, Iraq, Somalia, the Balkans, Afghanistan, and Syria. In addition to these deployments, the same Airmen also protected the homeland in the wake of the 9/11 attacks and responded to humanitarian crises in Africa, Asia, South America, and within our own borders. The promise of the post–Cold War peace dividend never materialized for the US military—and in particular our nation's Air Force.

During this generation, our air warfare capabilities dramatically changed. The employment of stealth technology, precision-guided munitions, remotely piloted aircraft, and globally networked information systems ensured our smaller Air Force remained a highly flexible and lethal instrument of national power. Airmen not only delivered air superiority—they also delivered air supremacy to a level never seen in the history of warfare. However, air superiority is not a birthright, nor is it a forgone conclusion for the next generation of Airmen. To think otherwise is folly.

Our adversaries continue to operate across a wide spectrum of capabilities and have chosen to avoid our strengths and take advantage of our vulnerabilities at home or abroad. They are lone-wolf attackers inspired by online hate messages. They are insider threats or computer "hacktivists" who target critical information systems. Highly capable insurgents and organized criminal networks have proven they possess both the means and will to affect sortie generation. While we fought violent extremist organizations, state-sponsored terrorist groups and resurgent near-peer militaries have also deployed new surface, air, cyber, and space capabilities that have forced the US and its allies to reexamine basing options and create new approaches to deployment.

The next generation of Airmen will contend with adversaries who fight outside the confines of traditional armed conflict. These adversaries are adept at hybrid warfare and have already demonstrated plausible deniability by employing "little green men" in Crimea and

ambiguous maritime threats in the South China Sea.[1] Moreover, advancements in stand-off technology such as smart mortar rounds and simple-to-operate man-portable air defense systems offer unique challenges to our expeditionary airfields. The use of unsophisticated tactics such as vehicle ramming and basic incendiary devices are proliferating. Likewise, commercially available small unmanned aerial systems, geocaching smartphone computer applications, and social media flash mobs offer organizational, kinetic, and intelligence, surveillance, and reconnaissance opportunities to the next generation of tech-savvy threat actors.

How will the next generation of Airmen meet this challenge? The first two volumes of the Air University–sponsored work *Defending Air Bases in an Age of Insurgency* generated significant conversation about threats to air and space installations and operations. Military and civilian authors from around the world presented case studies, delivered international perspectives, recommended doctrinal and procedural changes, and provided insight about how to organize and protect our Air Force for future conflicts. This third volume goes beyond the technical aspects of defending bases and focuses on the responsibilities of the person responsible for ensuring mission success: the commander.

This work presents basic principles for air base commanders to consider when it comes to ensuring mission success in the air at ground level. The principles focus on risk management, mission planning, integrating air and ground force capabilities, capitalizing on law enforcement skills, and effectively using intelligence/information to your advantage. Many of these areas mirror what a ground-based task force commander would be responsible for in a contingency environment. As in that case, success will require us to prioritize many of these tasks, albeit from an air-minded perspective. We ask our wing and installation commanders to focus on the "deep fight" when it comes to employing air- and space power. There is, however, a very real "near fight" at each air base that is equally demanding, complex, and dangerous. New Agile Combat Employment concepts being developed for future conflict decentralize air asset basing and will require understanding of these tools and threats at the squadron level and below. Comprehensive training of the skills and tasks described in this volume will be required to ensure all Airmen understand their role in defending the base from evolving threats.

I commend the authors and Air University for developing this guide. I urge commanders at all levels to research, study, and employ these truths when it comes to your installations and deployed bases. People First, Mission Always!

JAMES M. HOLMES
General, USAF

Notes

(All notes appear in shortened form. For full details, see the appropriate entry in the bibliography.)

1. Pifer, "Crimea: Six Years After Illegal Annexation"; and Chorn and Sato, "Maritime Gray Zone Tactics."

About the Authors

Col Shannon W. Caudill, USAF, retired (BS, Norwich University; MSA, Central Michigan University; MMS, Marine Corps Command and Staff College; MSS, Air War College; George Walker Executive Leadership Fellow, University of Charleston, West Virginia), is a doctoral student at the University of Charleston, an adjunct professor of leadership at Air Command and Staff College and the University of Charleston, founder of Home Plate Consulting and Writing Services, LLC, and owner of online book-sale business Baseball in Georgia. As a career Air Force security forces officer, he has worked at the unit, major command, and Joint Staff levels; commanded three security forces squadrons; and accumulated 18 months of combat experience in Iraq. He has written numerous white papers and articles on terrorism, leadership, base defense, and law enforcement that have been published in *Air and Space Power Journal, Joint Force Quarterly, American Diplomacy,* and the *Guardian*—the Joint Staff's antiterrorism publication. He is the editor and coauthor of the Air University Press three-volume monograph series, *Defending Air Bases in an Age of Insurgency*. In addition, he is coauthor of the history book *Baseball in Kennesaw*. As an educator, he has served on the resident and adjunct faculties of Air War College, Air Command and Staff College, Lake Region State College, North Dakota, and the University of Charleston, West Virginia.

Col Erik K. Rundquist, USAF, retired (BS, USAFA; MMAS, Army Command and General Staff College; MSSC, Syracuse University, New York; National Defense Fellow, Boston University), is a PhD candidate with King's College London, an external fellow to Boston University's International History Institute, and the Senior Aerospace Science Instructor for the Air Force Junior Reserve Officer Training Corps at North Henderson High School in Hendersonville, North Carolina. He is the former commander, Detachment 8 Air Force Installation and Mission Support Center. He was responsible for supporting Air Combat Command's security/antiterrorism risk management, engineering support operations, emergency services, and mission beddown activities for 1,200 aircraft, 24 wings, 14 bases, and over 200 operating locations worldwide. He has served in various duty positions including group commander, Air Combat Command chief of security forces, squadron commander, and joint staff officer

where he managed the DOD antiterrorism program for Secretary of Defense Robert Gates. As the former commander, 455th Expeditionary Mission Support Group, and commander, Task Force 1/455 at Bagram Airfield, Afghanistan, he led over 1,500 personnel—operating and defending the DOD's strategic air hub into Afghanistan—and was the battlespace owner for Parwan Province. His other contingency experiences include the United Nations Protection Force in the Balkans; Operations Allied Force and Shining Hope in Albania and Kosovo; Determined Response (USS *Cole*) in Yemen; Enduring Freedom in Kyrgyzstan and Afghanistan; and Iraqi Freedom, where he led his squadron in an operational combat jump into Bashur, Iraq, while attached to the 173rd Airborne Brigade. He deployed again to Tallil, Iraq, as the defense force commander for the 407th Air Expeditionary Group and 22nd Corps Support Group and as the J-7 director to the Combined Joint Special Operations Air Component Command at Balad, Iraq, and Bagram, Afghanistan.

Maj Gen Andrea D. Tullos, USAF (BA, University of Virginia; MAS, University of New Mexico; National Defense Fellow; MANSS, National Defense University), is the commander of Second Air Force, Keesler Air Force Base, Biloxi, Mississippi. She is responsible for the development, oversight, and direction of all operational aspects of basic military training as well as initial skills, advanced, and supplemental nonaviation training for 93 percent of the Air Force's enlisted force and officer corps. Second Air Force delivers more than 3,400 courses spanning 265 Air Force specialties and graduates 150,000 Airmen, Soldiers, Sailors, Marines, and international students annually. The command includes five training wings at Keesler AFB; Sheppard and Goodfellow AFB, Texas; Joint Base San Antonio-Lackland, Texas; and a network of 80 training detachments and operating locations around the world. Before this assignment, Major General Tullos was the Director of Security Forces, Deputy Chief of Staff for Logistics, Engineering, and Force Protection, Headquarters US Air Force, the Pentagon, Arlington, Virginia.

Acknowledgments

The authors wish to thank Air University (AU) Press for their continued support in publishing this third and final volume of *Defending Air Bases in an Age of Insurgency*. Special thanks to our AU Press Project Editor, Donna Budjenska, for the great care she gave this manuscript. Thanks also to AU Press's Kim Leifer, Nedra Looney, and Timothy Thomas for their contributions to the book's final product. The authors of all three volumes in this series want to express our deep appreciation to Daniel Armstrong for designing such a beautiful and unique cover for these books.

We are also grateful to Gen David Goldfein, the former Air Force Chief of Staff, for his support for base defense issues. First, he declared 2019 the "Year of the Defender" and provided resources to upgrade security forces and base defense assets.[1] Second, General Goldfein announced that 2020 was the "Year of Integrated Base Defense" with a focus on continued defensive modernization and innovation. General Goldfein's initiatives illustrate and underpin the critical importance of integrated base defense to the effectiveness and sustainability of airpower. This volume provides future wing, group, and squadron commanders as well as maturing Air Force and Space Force leaders some guiding principles through which they can better lead, protect, and secure their people and air- and space power assets. We are grateful to the contributions of the following people for their insights and suggestions as we finalized volume three: Col Bryan Gillespie, USAF (retired); Col Brian Greenroad, USAF (retired); Lt Col Ben Jacobson, USAF; Lt Col Chris Lacek, USAF; Lt Col Clay Nichols, USAF; Lt Col Joe Sorenson, USAF; and Col Troy Roberts, USAF. We also thank Nicholas Caudill for his suggestions on the choice of background for the cover of this book. Finally, we thank all the authors and contributors in volumes one and two who inspired and informed so many of the lessons we distilled from their study of integrated base defense found in this final book.

Notes

1. Tirpak, "Goldfein: USAF Needs 'to Return to Our Expeditionary Roots.'"
2. Delgado, "CSAF Charts Air Force Defender Way Forward."

Introduction

Commanders are responsible for force protection . . . it should be a commander's skill and judgment that remains of primary importance when making decisions about force protection. The staff can provide recommendations, but it has no responsibility for resulting actions; the commander alone is responsible; therefore, the commander alone is accountable.

—Lt Gen William B. Garrett III, USA
Maj Gen Thomas M. Murray, USMC
US Central Command Bastion Attack
Investigation Executive Summary

Wearing US Army uniforms, the attackers penetrated the air base's defenses under the cover of night. Armed with rifles, rocket-propelled grenade launchers, and suicide vests, the 14-man team began its deadly and well-planned mission against an air base in Helmand Province, Afghanistan, jointly manned by the North Atlantic Treaty Organization's (NATO) International Security Assistance Force (ISAF). Hours of combat ensued, and the morning light revealed the destruction of six McDonnell Douglas AV-8B Harrier II ground-attack aircraft and six refueling stations and damage to two other aircraft and six aircraft hangers.[1] In the aftermath, 14 insurgents and two US Marines, including the flying squadron commander, lay dead while eight coalition military members and one contractor were wounded. In September 2012, this insurgent operation constituted the most successful ground attack against ISAF's air assets to date in the Afghanistan conflict and the costliest ground-based attack against a US military airfield since the Vietnam War. While Camp Bastion was not defended by the US Air Force, it serves as a cautionary tale for commanders about their inherent responsibility to ensure an integrated defense (ID) is in place to meet the threat. In the end, two American general officers were forcibly retired after the Camp Bastion attack, because, as the Commandant of the Marine Corps put it, they "did not exercise the level of judgment expected of commanders of their grade and experience in their decisions related to oversight of a layered, integrated, defense-in-depth force protection plan."[2]

Aircraft are extremely fragile. If you look at the cost of a B-2 bomber or a ramp of F-22 aircraft, several well-placed mortar rounds

Key
AFOSI: Air Force Office of Special Investigations
EOC: emergency operations center
IDP: integrated defense plan
IDRMP: integrated defense risk management process
MWD: military working dog
RAM: random antiterrorism measures

Figure 1. Integrated defense effects (Source: Incident Continuum, Air Force Incident Management Course, Maxwell Air Force Base, 2016.)

can wipe out or cripple billions of dollars in modern aircraft. The destruction of a barracks occupied by the technical experts needed for air operations, such as the pilots or aircraft mechanics, will render air platforms unusable. Indeed, in Vietnam, the Vietcong specifically targeted lodging occupied by pilots, seeking to cripple air operations on the ground.[3] In Vietnam, Vietcong and North Vietnamese forces attacked American air bases 475 times between 1964 and 1973, primarily with indirect fire (IDF), destroying 99 US and South Vietnamese aircraft and damaging 1,170 aircraft.[4] In today's environment, similar

losses would be unsustainable because of the cost and lengthy manufacturing timeline needed for sophisticated stealth aircraft.

Commanders must make hard choices on base defense, considering mission requirements, resource constraints, and the dangers of a determined enemy enabled by technology like remotely piloted vehicles (RPV) and GPS-guided munitions. The threat is growing, and defenses are less certain. A major leadership challenge for Air Force commanders is the arena of air base defense. The Air Force simply does not stress these skills as essential to building future leaders in the officer corps, yet the defense of air bases is a central component of airpower. Therefore, commanders are left to spin up quickly, sometimes at a base under fire. It is up to you, the commander, to build the proficiency needed to command the base defense, put your own imprint on it, and exercise your leadership responsibility and judgment in the protection of your people and war-fighting assets.

Air Force strategy for defending air bases is now known as integrated defense (formerly known as air base defense, air base ground defense, or integrated base defense).[5] ID provides the requisite secure foundation from which the USAF launches combat operations and protects its personnel and resources—it represents an operational task. Without strong ID capabilities, USAF and joint force personnel and resources are more vulnerable to attacks that potentially decrease combat effectiveness, reduce sortie rates, and degrade the ability to project power. More importantly, if the USAF ID mantra "every Airman is a sensor" is to have long-term meaning, then a true integration of all units and personnel must be included in the base defense plan and vigorously practiced and exercised.

Airpower theorist Giulio Douhet wrote in 1921 that "it is easier and more effective to destroy the enemy's aerial power by destroying his nests and eggs on the ground than to hunt his flying birds in the air."[6] This idea is captured in Air Force Doctrine Document 1, *Air Force Basic Doctrine*: "Air and space power is most vulnerable on the ground. Thus, force protection is an integral part of air- and space power employment."[7] In 2015, RAND Corporation released a study on air base attacks, which concluded that air base threats, including new missile technology and ground attacks, will greatly affect air operations in the future. RAND prophesized the "end of the era of air base sanctuary"—launching air operations from relatively safe air bases will become a thing of the past. Additionally, RAND provided a critique of how the Air Force approaches base defense and recovery

issues: "Too often, base defense and recovery are treated as support functions to be delegated to security forces and civil engineers. Although base and wing commanders take base defense seriously, it has not been a priority for the institutional air force, primarily because it has not been conceptualized as a core warfighting problem."[8]

Commanders can create truly synchronized base defense efforts by fostering organizational constructs and leaders that rapidly adapt to the operational environment and threat. Establishing a successful and effective base defense posture relies on a proactive base security system focused on the full spectrum of threats to operations. Commanders can only do so if they utilize all available assets, especially joint, coalition, and host-nation partners. Joint and combined integration of base defense forces is therefore critical to this effort. It can only be accomplished if responsibilities for the defense are well understood and supported by all commanders and backed by a robust and regularly tested command-and-control system. It is also a function of the organizational culture and expectations for each Airman, as well as joint and coalition force partners on the installation. The goal is to create a sort of muscle memory for the installation in implementing the defense through exercise repetition, tabletop exercises, and continuous improvement. The same concepts that are foundational to airmanship and air-mindedness are foundational to ID. The Australian Air Power Development Centre said it best when it observed, "By virtue of the multi-dimensionality of air forces, airmen think differently and, therefore, are more likely to find alternative solutions to problems."[9] Air-mindedness lends itself to innovation and that same spirit and focus should enable the defense of an air base. Commanders and leaders do not need to learn all the skill sets found in security forces (SF) or military police; instead, they need to understand the basics of ID, shape their unit's role in it, and tap into the military decision-making and risk-management skills the Air Force or Space Force has already given them.

As leaders reflect on the successes and failures of USAF operations in Iraq and Afghanistan and a renewed focus takes hold on the threat of emerging peer competitors, there must be a holistic debate and discussion on air base defense. Additionally, we must be cognizant of growing threats in the homeland, which include insider threats as well as self-radicalized terrorists. Therefore, this volume in the *Defending Air Bases in an Age of Insurgency* series puts forth 10 guiding principles for commanders and leaders to consider in leading base

defense. Additionally, while the title of this book series addresses insurgency, it also includes many direct lessons and historical accounts regarding peer competitors that will inform your base defense regardless of the adversary. The authors and contributors who shaped these propositions hope this material will provide a starting point for improving the intellectual understanding of the complexity of defending air bases in the modern era and challenges brought forth by threats empowered by the proliferation of technology.

Notes

1. Starr, Lawrence, and Sterling, "ISAF: Insurgents in Deadly Attack."
2. Amos, Memorandum for record, Accountability Determination of US Commanders for the 14–15 September 2012 Attack.
3. Elliott and Elliott, *Documents of an Elite Viet Cong Delta Unit*, 38.
4. Vick, *Snakes in the Eagle's Nest*, 68.
5. In October 2019, Gen David Goldfein, the US Air Force Chief of Staff, designated 2020 the year of "Integrated Base Defense," which may well indicate a return to this term vice integrated defense (ID) as the preferred nomenclature. Delgado, "CSAF Charts Air Force Defender Way Forward."
6. Douhet, *The Command of the Air*, 53–54.
7. US Air Force, *Air Force Doctrine Document 1*, 34.
8. Vick, *Air Base Attacks and Defensive Counters*, 64.
9. Royal Australian Air Force Air Power Development Centre, "What Is Airmindedness?"

Ten Base Defense Principles for Commanders

1. You Own It!
2. Get Left of the Boom: Deter, Disrupt, Deceive
3. Influence the Base Security Zone . . . or Someone Else Will
4. Unity of Effort: Synchronize the Fight
5. Everyone Must Have a Role in the Base Defense . . . and Play It!
6. Intelligence Drives Maneuver: A Joint-Interagency Approach Is Critical
7. Air-mindedness Includes Using Air Assets for Base Defense
8. Law Enforcement Skills Are Critical to Base Defense and Irregular Warfare
9. Manage the Risk: Commit Intellectual Capital to the Fight
10. Nowhere to Hide: Anticipate Future Threats and Develop Countermeasures

Chapter 1

You Own It!

The Camp Bastion attacks illustrate how difficult base defense can be in a complex, coalition environment. The attack on US Marine Corps aircraft and personnel fell in the British base defense sector. Despite an integrated and robust command, control, and communications capability with American and British representation, the base lacked integrated defense in depth, adequate force protection engineering (physical barriers), manned security towers, static security posts and machinegun positions, and ground defense sensors to provide warning of a sector penetration.[1]

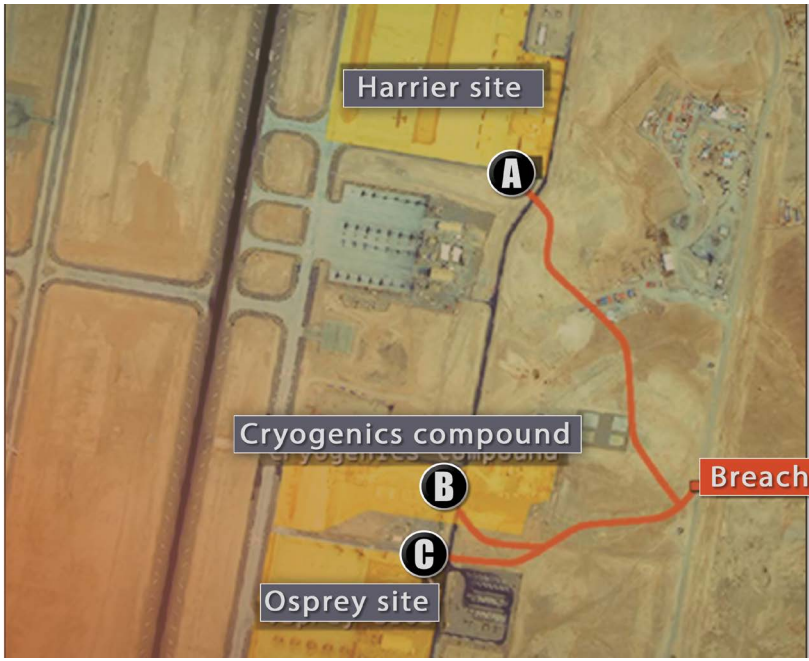
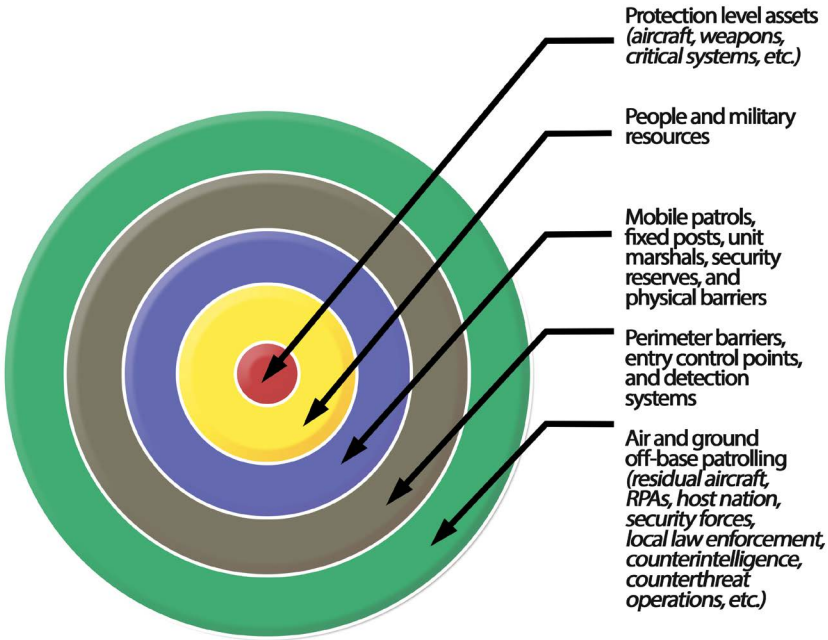


Figure 2. Overhead shot of Camp Bastion where attackers split into three teams (A, B, C). Other than two metal fences, there was nothing to impede the attack (i.e., no defense in depth). (Source: Air Combat Command base attack video series, 2015.)

Regardless of British responsibilities, two US Marine Corps general officers were relieved because they did not ensure the safety of their aircraft. The US Marine flying squadron commander died with his aircraft. In the British Parliament's House of Commons report on the attack, members observed that "no one was actually doing any guarding" from the perimeter to the aircraft—a wide open door the enemy exploited.[2] After an inquiry, one British politician put it bluntly: "That is the sticking point. . . . We (UK) manned the perimeter, but the Americans lost their jobs."[3] In short, regardless of the division of labor for security, if your aircraft, assets, or people suffer from an attack, you still own the results. Complacency and blind collegiality kill.



Key
RPA: remotely piloted aircraft

Figure 3. Notional defense-in-depth schematic (Source: Air War College, Defending Air Bases in an Age of Insurgency, Spring Elective, 2016)

From wing commanders to noncommissioned officers on combat patrol, all Airmen need to be connected and understand their part in the base defense mission and the plan for a defense in depth that protects the most critical mission assets (see fig. 3). Ultimately, the commander must be personally involved and engaged in developing and implementing an effective base defense effort. Commanders need to create an organizational climate that builds and values learning organizations that thrive by challenging assumptions, taking the initiative in building partnerships, and proactively engaging the local population and friendly forces in the operational environment surrounding its air bases. Investing in our intellectual capital is the way forward to creating a "thinking" force that will be quicker to adapt to new enemy tactics. It is not enough to know the science (i.e., interlocking fields of fire, blast mitigation, risk management, physical barriers, etc.) and the art (commander's estimate, information operations, tactical deception, etc.) of base defense. One must also learn the nonkinetic actions that can often deter, dissuade, disrupt, or disable enemy operations in the base security zone.

Invest time: Have key leaders provide an overview of the ID and gauge whether your subordinate commands and tenant units comprehend, accept, and buy in to their role in it. Conduct tabletop exercises, execute an unscheduled recall exercise, and gauge your emergency operations center (EOC) response to a mass casualty exercise. These scenarios will build quick foundational understanding of the capabilities and plans of your Defense Force and EOC. Learn basic law enforcement processes by having SF pull you over, conduct a field interview, apprehend you, and then transport you for processing in a detention cell. In the wake of the George Floyd and Freddy Gray cases (where African-Americans were wrongfully killed while in police custody)[4] and other recent law enforcement controversies, it is imperative commanders understand the apprehension process used by SF and Air Force Office of Special Investigations (AFOSI) agents on their behalf. As the "mayor" of your base or unit, you will quickly learn the protocols used for officer safety and the physical environment of a detainee. Ultimately, you need to know these details, because each security and law enforcement process is designed to preserve good order and discipline, base security, and, ultimately, your mission.

Finally, with the exception of the Camp Bastion attack, the US military has been largely successful in protecting its aircraft and people during the recent conflicts in Afghanistan and Iraq, but the 2020

attacks on a Kenyan airfield underscore the importance of consistency in applying sound base defense practices. Poor US and Kenyan air base defense led to a successful attack by al-Shabab forces on 5 January 2020, which resulted in the deaths of three Americans and the destruction of six aircraft. Gen Stephen J. Townsend, USA, commander, United States Africa Command, said, "We weren't as prepared, and we're digging in to find out why that is the case."[5]

Notes

1. Garrett and Murray, Enclosure 3, Executive Summary of the Army Regulation (AR) 15-6 Investigation of the 14–15 September 2012 Attack on Camp Bastion, Leatherneck, and Shorabak (BLS) Complex, Helmand Province, Afghanistan (hereafter Executive Summary), 7–8.
2. British Parliament, *Afghanistan—Camp Bastion Attack*, vol 2, EV-13.
3. British Parliament, EV-24.
4. Deliso, "Timeline: The Impact of George Floyd's Death"; and Woods and Pankhania, "Baltimore Timeline."
5. Everstine, "AFRICOM: U.S. Forces Were Not Prepared."

Chapter 2

Get Left of the Boom: Deter, Disrupt, Deceive

In May 2006, six homegrown, but foreign-born, self-radicalized extremists were arrested for plotting an attack on Soldiers at Fort Dix, New Jersey, an Army training site. The would-be attackers filmed themselves conducting firearms training and took the footage to a video store to switch the format to DVD. The recording showed the men calling for jihad, or holy war, against the United States and shouting "God is great" in Arabic. Luckily, the video store attendant informed the Federal Bureau of Investigations (FBI) about the contents of the videotape; the FBI then infiltrated the group and arrested them before they could conduct the attack.

However, largely underreported is the fact that the perpetrators discussed a total of nine potential US military targets in the US homeland. According to the indictment, the group surveilled five installations: in addition to Fort Dix, they profiled Dover Air Force Base, Delaware; Fort Monmouth and Lakehurst Naval Air Station, both in New Jersey; and the US Coast Guard building in Philadelphia.[1] The conspirators also noted potential attacks against Naval Station Philadelphia and the "nearby air force base," which likely referred to McGuire Air Force Base, located adjacent to Fort Dix (now known as the consolidated Joint Base McGuire-Dix-Lakehurst).[2] As they narrowed their focus on Fort Dix, they discussed attacking critical infrastructure including the base electrical grid to "cause a power outage and allow for an easier attack of the military personnel there."[3]

The group also developed future plans for high-profile targets, including attacking the Army-Navy game participants in naval billeting or potentially at the game itself held at Lincoln Field in Philadelphia. They discussed the possibility of sinking US naval vessels while docked at the Port of Philadelphia. As they narrowed their search to the five potential targets for surveillance, they repeatedly videotaped the perimeters of the bases. For example, the conspirators surveilled Dover Air Force Base security operations and physical security and determined it "was too difficult of a target because of its high security."[4] Your defensive posture can create the "Dover Effect" by establishing observable and continuously changing security routines. The goal is

to affect the decision cycle of a determined enemy by forcing him to choose a more appealing and certain target.

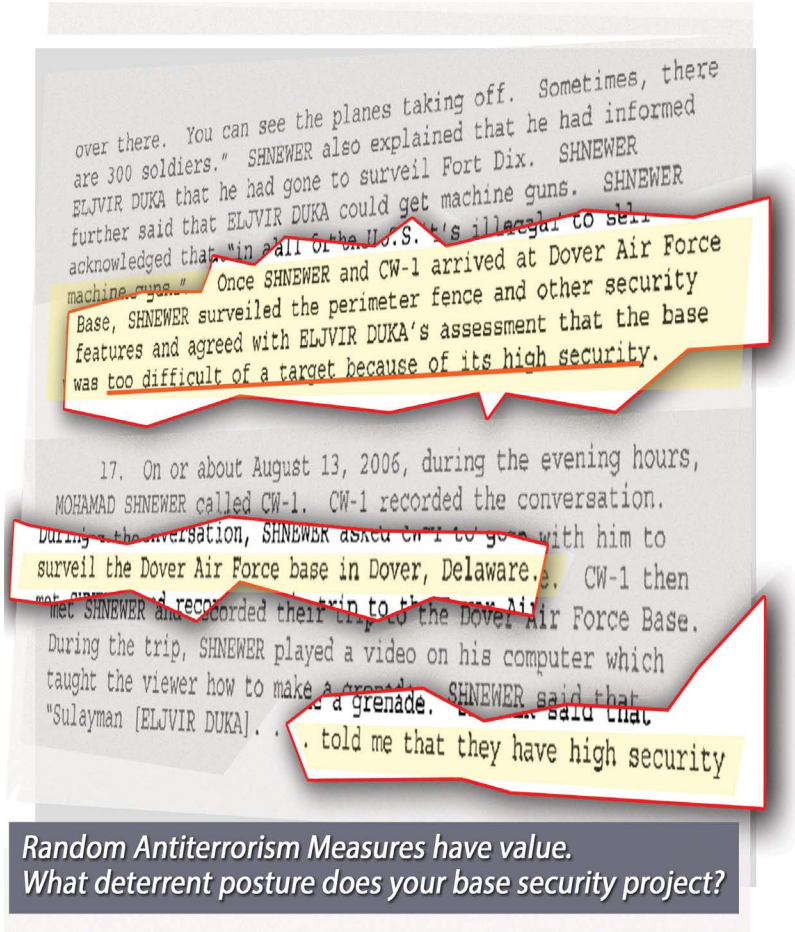


Figure 4. The "Dover Effect": learning the deterrent effect of security from the Fort Dix Case Study.

The group eventually selected Fort Dix as its primary target because one member had access to the base through his father's pizza delivery business, which gave them more certainty on targeting and base security routines. Serdar Tatar's father owned Super Mario's restaurant, which made deliveries to both Fort Dix and McGuire Air Force Base. Significantly, Tatar was able to acquire a map of Fort Dix,

labeled "Cantonment Area Fort Dix, NJ," which helped the conspirators target personnel and facilities. The group also believed that the massing of Soldiers during training events would provide easy targets because they gained intelligence that the Soldiers often trained without ammunition.

The attackers estimated that a group of six or seven people could kill 100 unarmed Soldiers. One conspirator commented, "My intent is to hit a heavy concentration of soldiers"—a prospect that seemed possible at Fort Dix given their surveillance and knowledge of the installation.[5] Their goals were "to kill as many American soldiers as possible" by procuring mortars, rocket-propelled grenades, and machine guns.[6]

Attacking unarmed personnel in a training environment is not a new idea. On 9 October 2002, one US Marine was killed and another was wounded after two gunmen infiltrated a military training exercise on Failaka Island in the Persian Gulf near Kuwait City.[7] Two Kuwaiti radicals, deemed terrorists by the Kuwaiti government, used AK-47 automatic rifles to attack Marines who were training with blank rounds. On a smaller scale, the Failaka Island attack parallels the plan of the Fort Dix conspirators. For commanders with training missions, these two scenarios provide compelling reasons to examine the force protection arrangements for training sites with massed forces.

Information is power. The goal is to "get left of the attack" or proverbial boom (influencing or defeating an attack before it can begin by gaining the advantage through intelligence; see fig. 1). Law enforcement and intelligence partnerships are critical and can only be realized by fostering relationships that build trust and therefore lend themselves to information sharing. Stateside, commanders need to ensure liaison with state and local law enforcement, major urban area fusion centers (threat and warning intelligence), and the FBI's Joint Terrorism Task Forces (JTTF). The JTTF provides valuable conduits for sharing vital homeland security information and countering domestic terrorism. Overseas, leaders must foster strong relationships with the host nation's military leadership, intelligence, and SF, as well as local officials and coalition forces, to ensure threat intelligence is shared in a timely manner, trends are analyzed, and action is taken in the battlespace to deter enemy action or aggressive protestor activity.

In parallel with random antiterrorism measures (RAM), installations must develop military deception plans to moderate the risk to personnel and potential for materiel losses during an air base's transition

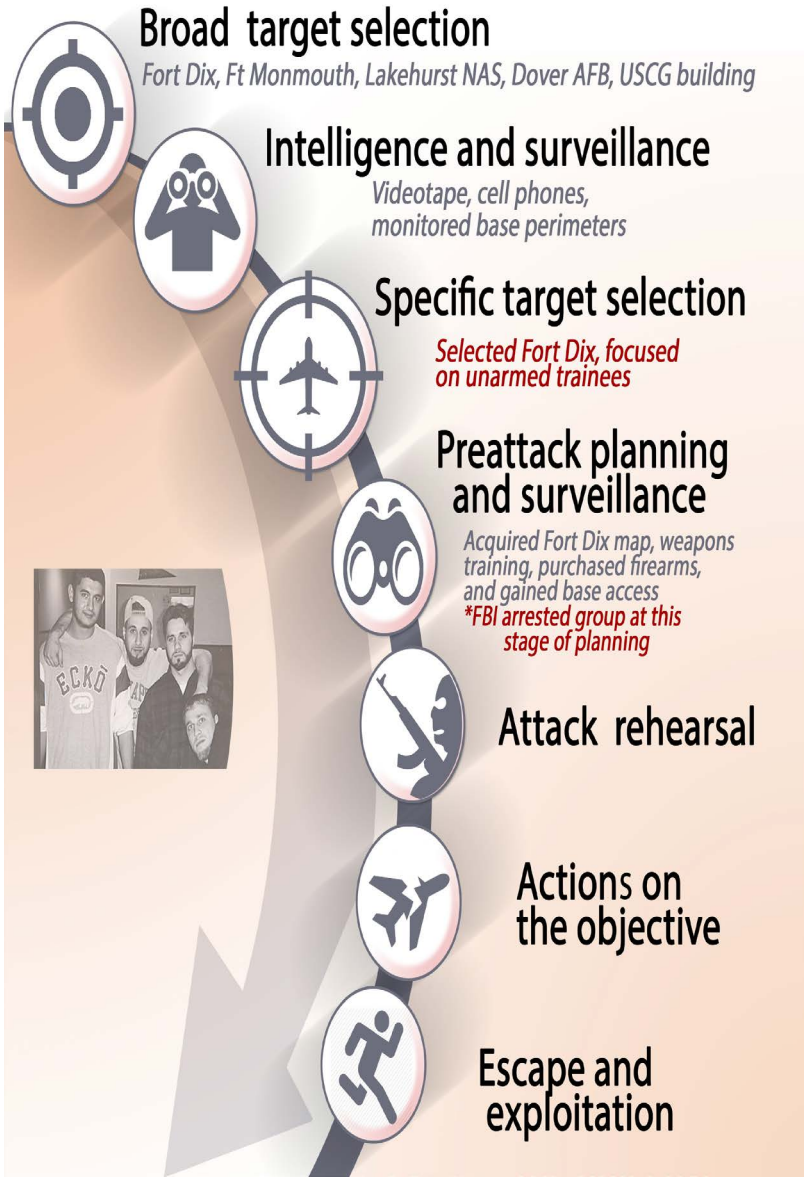


Figure 5. Fort Dix Six: Targeting Military Trainees, Air Force Incident Management Course, Maxwell Air Force Base, 2015. (Reference: US Army Training and Doctrine Command, Handbook No. 1: A Military Guide to Terrorism in the Twenty-first Century [Fort Leavenworth, KS: TRADOC, 15 August 2007], https://apps.dtic.mil.)

to or execution of contingency operations. The goal of deception operations is "to deter hostile actions, increase the success of friendly defensive actions, or to improve the success of any potential friendly offensive action."[8] Examine the security posture your base projects along your perimeter and provide a constantly changing and observable security presence. Stagnation in creativity and an unchanging security routine provide the enemy confidence that your installation is a soft and predictable target. Influence the enemy's decision cycle so they shop for another target—control what you can control. Ensure your commanders at all levels are overseeing a robust operational security program in support of your RAMs and military deception plans. In short, lead your version of the "Dover Effect" through active, intellectual engagement and by challenging the status quo.

Notes

1. United States of America vs. Dritan Duka.
2. United States of America vs. Dritan Duka.
3. United States of America vs. Dritan Duka.
4. United States of America vs. Dritan Duka.
5. United States of America vs. Dritan Duka.
6. United States of America vs. Dritan Duka.
7. Schmitt, "Threats and Responses: Skirmish."
8. Joint Chiefs of Staff, *Joint Publication 3-13.4, Military Deception*.

Chapter 3

Influence the Base Security Zone . . . or Someone Else Will

Airmen should properly frame the operational environment of the area adjoining the base boundary to gain an understanding of the power brokers, key influencers, and potential threats in the battlespace. Some operating locations will have a clearly delineated ground battlespace owner (BSO), as was the case in Iraq and Afghanistan. At other locations, it may be less clear, or an authoritative or capable battlespace owner may not exist. It is up to you, the commander, to fully engage in your force protection and base defense responsibilities so that you understand the players and threats in the base security zone (BSZ) (see fig. 6 below). You have considerable expertise available to help you create by using the expert advice you receive and relying on your intuition and judgment.

Understanding the BSZ is critical in both expeditionary and garrison operational environments. Airfields rarely operate as self-sustaining islands of security removed from threats and disruptions common to any other industrial area. Power, fuel, water, food, communications infrastructure, and an ample supply of workers are essential to running and maintaining an airfield. An airfield is a small part of a larger biosphere. The base (and its Airmen) represents an obvious and lucrative target for criminal elements, spies, terrorists, and insurgents. From an active base defense perspective, history has shown the overwhelming majority of attacks against airfields have been launched from "outside the wire" (i.e., improvised rockets, mortars, snipers, lasing incidents, etc.). This tendency is compounded by the vulnerability of aircraft to small arms and surface-to-air fire while operating in the approach and departure profiles of an active airfield. The widespread use and commercial availability of small unmanned aerial vehicles expand the threat envelope even further and allow any group to incorporate an air component into their operational plans. Understanding and, more importantly, *shaping* this environment are critical to installation commanders and for sortie generation.

Operating and coordinating throughout the BSZ (and beyond) provide the commander depth and knowledge and two critical luxuries: time and space. In an expeditionary environment, this may

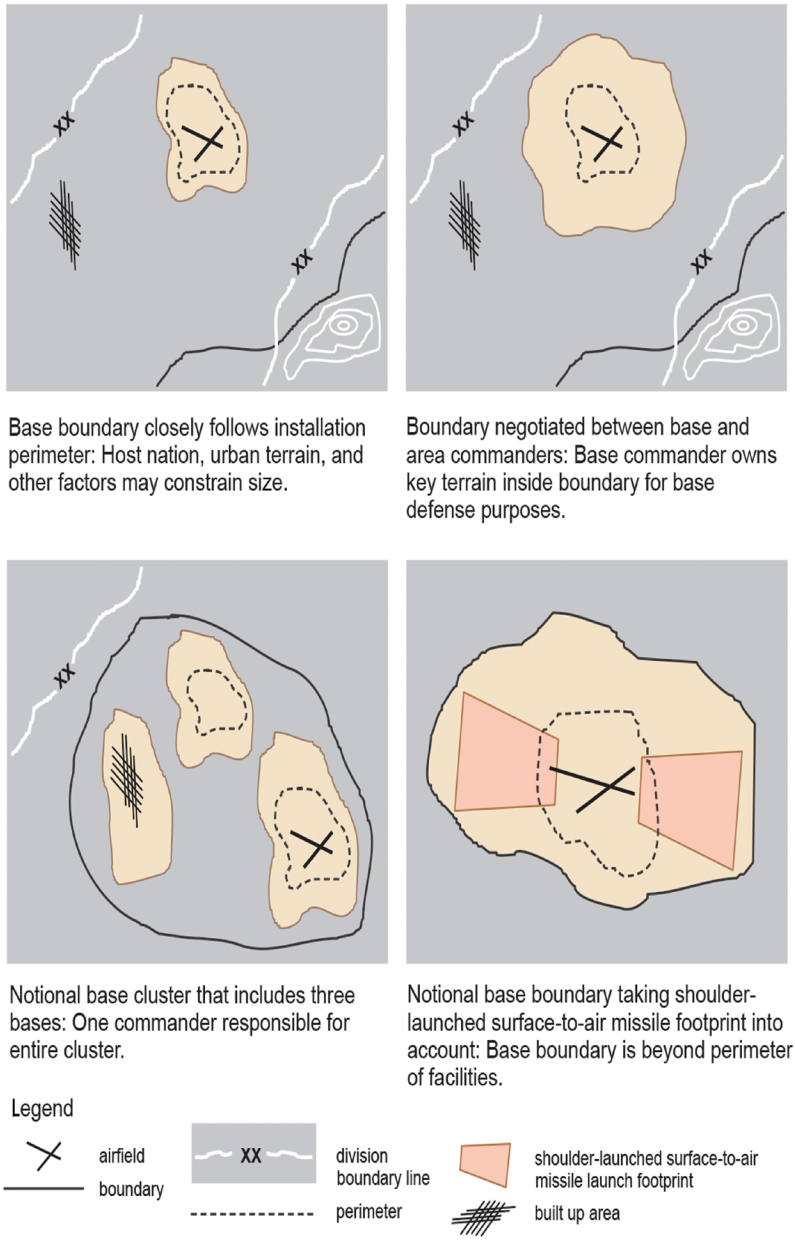


Figure 6. Base boundary considerations. (Reproduced from JP 3-10, *Joint Security Operations in Theater*, 13 November 2014, IV-3, http://dtic.mil/doctrine/new_pubs/jp3_10.pdf.)

mean dedicating SF patrols to operate several miles outside of the installation to deny key terrain from an insurgent who is focused on rocketing an air base or attempting to shoot down a troop-laden C-17 aircraft. In a main operating base in Europe or the homeland, it could mean ensuring your SF and AFOSI detachments are fully engaged with local law enforcement to protect off-base mass gatherings or sharing information on criminals and terrorists operating within the area (including helping you establish "no-go" areas for your Airmen). Regardless, your defense force requires continuous engagement with the local population surrounding the base; as a commander, you set this tone for engagement. In a more complex combat environment, a ground commander/BSO is clearly identified (a more detailed explanation and exploration of the BSO concept will be offered later). This commander usually has primary responsibility for interaction with the local populace and officials. If this is the case, Airmen should not write off their own involvement and should maintain some influence in the battlespace through a proactive and engaged approach. In many cases, aircraft operations (noise, lighting, etc.) could adversely affect the lives of those living within the BSZ, which, if not managed or addressed, could lead to grievances that undercut local support for air operations. Leaders must be made aware of how air operations affect the local community and take thoughtful steps to engage in constructive conversations that lead to the mitigation of concerns and grievances.

One case study highlights the need for continuous and adaptive engagement with forces in the battlespace. At the beginning of Operation Iraqi Freedom, many observers in the press and politics lauded the initial British counterinsurgency (COIN) strategy in southern Iraq as the template for victory the rest of the country. After the invasion of Iraq in 2003, British troops quickly adapted a peacekeeping model and began foot patrols of Basra, wearing regimental berets instead of helmets and driving unarmored vehicles. However, what was praised widely as the way forward disintegrated into a disastrous rout over time. As Shiite criminal and Mahdi Militia groups organized, British casualties began to mount. During a period in 2006–2007, as much as 80 percent of recorded attacks in Iraq targeted British forces, which directly affected the political support for British action.[1] This in turn caused the British government to press its military forces to quickly transfer security control to the Iraqi forces.

Over the course of a year, the British forces in Basra went from patrolling the streets from six main bases to withdrawing all forces to their contingency operating base at Basra Air Station. The net effect was to vacate the battlespace to the enemy, isolate and barricade the remaining British forces at one air base, and become a magnet for rockets and mortars. The lesson for US forces defending air bases is to stay engaged in the battlespace to maintain accurate intelligence, gain support of the populace, and leverage local authorities for the security of the installation. Basra is a cautionary example of how we should maintain the initiative in the battlespace and constantly adapt to the changing tactics of the enemy. In short, if the population is not safe, neither are you. The base must not be walled off from the local populace with no interest in or responsibility for their security situation or well being.

David Kilcullen's seminal paper, "Twenty-eight Articles: Fundamentals of Company-level Counterinsurgency," offers the following wisdom for success in COIN operations, all of which is applicable in the defense of air bases.

> Whatever else you do, keep the initiative. In counterinsurgency, the initiative is everything. If the enemy is reacting to you, you control the environment. Provided you mobilize the population, you will win. If you are reacting to the enemy—even if you are killing or capturing him in large numbers—then he is controlling the environment and you will eventually lose. In counterinsurgency, the enemy initiates most attacks, targets you unexpectedly, and withdraws too fast for you to react. Do not be drawn into purely reactive operations: focus on the population, build your own solution, further your game plan, and fight the enemy only when he gets in the way. This gains and keeps the initiative.[2]

During the insurgency in Iraq, an Air Command and Staff College professor relayed a story about an Air Force major who was involved in a student seminar on COIN. When the professor asked the major why he lacked an enthusiasm for the topic of COIN, the major responded, "Why should I? My responsibility stops at the fence line."[3] This thinking is outdated and cedes operational control to the enemy and operational influence to a friendly force that may not have protection of the air base as a primary concern. In fact, a commander should generally look at a fence as nothing more than a legal demarcation of a boundary with generally no tactical or operational value beyond that of signage. Unless a fence is monitored (with sensors or cameras), observed, and integrated into an obstacle plan as part of

defense in depth, it offers little more than an element of deterrence—but perhaps also a false sense of security. Moreover, there are COIN opportunities that can exist inside the confines of an airfield, for example hiring local workers, training host-nation forces, key leader engagements, countersurveillance operations, law enforcement raids in third-country national and contractor housing areas, and so on. Maj Gen Thomas H. Deale, USAF, retired, a three-time wing commander—twice in Afghanistan—emphasized the importance of thinking outside the fence line by stating, "You must understand the strategic and operational value of everything that is going on within your battlespace, even if you do not own it."[4]

Notes

1. Ucko, "Lessons from Basra."
2. Kilcullen, "Twenty-eight Articles."
3. Air Command and Staff College Faculty discussion with Col Shannon W. Caudill, 2013.
4. Maj Gen Thomas H. Deale, interview, n.d.

Chapter 4

Unity of Effort: Synchronize the Fight

Synchronization of base defense resources is central to mounting any successful defense strategy. It is especially important when defense forces comprise joint and coalition forces sharing a complex battlespace. Regardless of who owns the battlespace outside the air base perimeter, Airmen should establish themselves as reliable partners who bring forth their expertise and assets to play a positive role in supporting the ground BSO's COIN or stability operations, because ultimately it helps flying operations by having a more secure and stable operating environment in the BSZ. The lessons learned in Iraq and Afghanistan provide templates for engagement and synchronization in the battlespace. It is important to accept that host-nation and coalition forces have different rules of engagement (some known and others hidden from partners) and American forces have different statutes and authorities that potentially limit their roles in combat operations. For instance, there will be a wide range of interpretations and guidance among coalition partners about warning shots, use (or nonuse) of less lethal technology, employment of military working dogs, an aerial "show of force," and so forth. A successful synchronization effort takes into account all of these differences to distill the key areas in which unity of effort can be achieved. Seek understanding of partner capabilities and limitations, then act to incorporate them into the base defense to the level they are capable, willing, and authorized to participate.

At Joint Base Balad (JBB), for example, Airmen learned to leverage nonkinetic assets and operations to achieve lasting effects in support of the ground BSO's COIN and stability campaign plans. The wing hosted biweekly COIN and civil-engagement synchronization meetings to ensure full support to the BSO from the Army, Air Force, and Department of State partners at JBB. Equally, the BSO embraced Air Force and other partner units as a means of realizing his overall campaign objectives along three decisive lines of operation: security, economic development, and governance. Five times per week, at a minimum, wing staff representatives, SF, operations group representatives, and joint intelligence support element (JISE) analysts met

with the BSO and partner units to optimize coordination and information sharing. These meetings included synchronization of operations, targeting, reviewing intelligence fusion, evaluation of the BSO's weekly effects summary, and the sharing of operational notes from numerous synchronization meetings at the field grade and company grade officer levels. For operators, this meant providing support such as intelligence, surveillance, and reconnaissance (ISR) data on the locations of high-value individuals, sweeps over IDF hot spots, aerial monitoring of security for Iraqi election polls, and aerial show-of-force flights by F-16s over terrain from which IDF attacks frequently originated.

The BSO was responsible for synchronizing all friendly forces in the area of operations, which included conducting kinetic and nonkinetic actions, maintaining situational awareness of all forces, and controlling fire-support coordination measures. The BSO leveraged the capabilities of all coalition, host-nation, and other partner units, including nonmilitary entities such as the Department of State's provincial reconstruction teams and nongovernmental organizations. Their accomplishments proved that, if properly synchronized, such mutually supporting operations create a symbiotic relationship and unity of effort, ultimately yielding a more efficient and effective use of resources. US Joint Forces Command noted that the BSOs are learning to take advantage of all available operational enablers: "Many joint players . . . operate in the battlespace owners' areas of operation . . . . Battlespace owners are becoming increasingly more comfortable with these 'non-assigned' players in their battlespace."[1] For Airmen, the goal is to create a common operating picture and achieve a unity of effort that better protects the installation, establishes security and influence in the BSZ, and, ultimately, better protects flying operations to support the larger strategic mission. For instance, Task Force 1/455 at Bagram, Afghanistan (commanded by an Airman), coordinated ground patrols and synchronized BSZ operations at key times to deter attacks when larger transport aircraft were being launched and recovered at the expeditionary airfield.

It is important to recognize that all operating bases in the BSO's area of operations can have profound positive or negative second- and third-order effects across the operational environment. These include decisions that may appear confined to the base itself, whether they are air provost services (law and order operations), contracting, construction, or simply hosting a local children's event. If such opera-

tions and activities are poorly coordinated and if local national ties and perceptions are not clearly understood, they can undermine the BSO's relationship with key local officials and adversely affect efforts along multiple lines of operation and effort. Major General Deale summarized by stating, "To be effective at base defense, you have to have an accurate/detailed perspective of the threat and mission environment as well as the organizational dynamics of friendly forces and the resources that will interact to effectively provide for the defense. You must integrate and synchronize your efforts with the greater battlespace commander. . . . You're not just on your own."[2]

Airmen should remember that the relationship with ground BSOs should be given a great deal of attention and care. Additionally, the BSO may change periodically, whether it is a new unit and commander rotating in from the same service or, as in the case of Tallil Air Base, Iraq, a completely new BSO appointed from a different coalition partner (both Romania and Italy were battlespace owners at this air base).[3] Ultimately, the synchronization efforts demonstrated at JBB and elsewhere provide examples of how air bases can truly optimize battlespace effects among coalition and joint partners to improve the aerodrome operating environment.

Centralized control and decentralized execution are tenets of airpower.[4] Similarly, throughout history, the centralized control of air base defense forces has proven essential to effectively countering attacks on air bases. During the Tet Offensive on 30 January 1968, simultaneous multi-battalion-level attacks occurred at Bien Hoa and Tan Son Nhut Air Bases, Republic of South Vietnam.[5] During these attacks, defenders relied heavily upon the installation's centralized control of base defense to properly position responding forces to repel enemy attackers and mount counterattacks on enemy forces already inside the perimeter.

Proper command and control provided by a joint base defense operations center (JDOC) is essential to enable senior decision makers with overall situational awareness to properly direct and position friendly forces to counterattacks. Centralized control also prevents individual units (with good intentions) from responding to an event autonomously, leading to confusion and possibly fratricide and inadvertently subverting the efforts of another responding force. This lack of a coordinated response could also lead to gaps in the overall scheme of the defense. Centralized control of responding forces under

the defense plan ensures a controlled response that preserves the integrity of the defensive scheme of maneuver.

JBB provides another example of centralizing base defense under one leader. From 2008 to 2011, the 332nd Air Expeditionary Wing organized its base defense assets under the JBB defense force commander (DFC), an Air Force SF colonel, who was responsible for ensuring BSZ security and integrated, joint base defense.[6] This group commander and his team worked tirelessly to leverage the joint assets operating in the vicinity of JBB to implement a collaborative approach with partner joint units and host-nation forces that would produce operational gains and "mitigate potential risks and defeat adversary threats to Air Force operations."[7]

Furthermore, the DFC synchronized his ID operations through the JDOC, collocated with a BSO's tactical operations center. The JDOC directed and integrated all subordinate security systems and communications elements, serving as a tactical integrator of both ground intelligence affecting the air base and guidance for BSO effects that drove the base defense effort. Maj Gen Brian Bishop, then the wing commander, emphasized this point by observing, "My defense force commander, Col John Decknick, understood the mission, laid foundational relationships with the Battlespace Owner and partners, and integrated our efforts to eliminate seams in the defense. As a result, the BSO was confident in our Airmen as they performed the outside-the-wire mission."[8]

A truly joint team, JBB's defense structure included tactical control of the counter-rocket, artillery, mortar (C-RAM) joint intercept battery. C-RAM Soldiers and Sailors were responsible for employing the system's intercept, sense, respond, and warn capabilities, as a unique defense against enemy IDF attacks and as a localized warning to populated areas of the base.[9] Countless lives were saved simply by the alarm warning them to take cover several seconds before impact. Placing C-RAM under tactical command of the USAF DFC ensured the best possible integration of C-RAM capabilities into the overall physical security and force protection architecture of JBB and the counter-IDF plan. As the threat of terrorist and insurgent forces using precision munitions and RPVs grows, the US military will likely need a C-RAM-like system as a key enabler under one DFC.

Major General Bishop summarized the JBB base defense experience by stating, "My biggest take-away for base defense is the JDOC. You integrate everything through the JDOC: outside-the-wire opera-

tions, air support through the JTACs [joint terminal attack controller], C-RAM, sensors, intelligence, etc. From the command perspective, I had a very high level of confidence in what the JDOC team was doing to protect the base."[10]

Notes

1. Luck and Findlay, "Insights and Best Practices," 5.
2. Deale, interview.
3. Maj Jeffery Becker, email correspondence with Col Shannon W. Caudill, 4 May 2013.
4. USAF, *Air Force Doctrine Document (AFDD) 1, Air Force Basic Doctrine, Organization, and Command*, 37.
5. USAF, *AFDD 1-1*, *Leadership and Force Development*, 66–77.
6. USAF, *Air Force Policy Directive (AFPD) 31-1*, *Integrated Defense*, 8.
7. USAF, *AFPD 31-1*, 2.
8. Brian Bishop, interview, n.d.
9. US Army, "Army Programs: Counter-Rocket, Artillery, Mortar (C-RAM)."
10. Bishop, interview.

Chapter 5

Everyone Must Have a Role in Base Defense . . . and Play It!

Defending air bases, their requisite airpower assets, and joint personnel should be a mission in which all Airmen (and joint personnel) are invested and play an active role. Today, USAF doctrine emphasizes that everyone shares in the responsibility of the new ID concept. Air Force Doctrine Document 3-10, *Force Protection,* states, "Every Airman is a sensor, and protecting the force is everyone's duty. All Airmen are responsible for force protection, whether reporting suspicious activity while engaged in their primary duties, augmenting base defense, or assisting in response to a natural disaster."[1]

Despite the rhetoric, the USAF has not lived up to this bumper sticker slogan. For instance, unlike sister services at some operating bases in Iraq, Airmen stood out because they were not required to carry a personal weapon for their own protection, and the majority played no role in base defense. Moreover, on deployments, an Airman's first stop upon arriving at an expeditionary airfield was often spent turning in their assigned weapon to an armory instead of maintaining it for personal protection or having it available for an ID role. Also fueling this disconnect was a propensity to contract security taskings to private firms. The prevailing thought was, if you have a security concern, simply write a check for more contractors—a concept that ultimately led to increased congressional scrutiny and legal challenges from use-of-force incidents that damaged relations with host-nation populations.[2] But more importantly, the inclination to rely on contractors has denigrated or hindered the concept of Airmen becoming sensors and playing a role in base defense.

If Airmen are separated from any obligation to their own defense or that of defending the base they operate, there will be a price to pay down the line, either from an insider threat or direct attack by an enemy force. Indeed, it may take a calamity on the scale of what the British suffered in World War II to sort out the future of Air Force base defense. Dismayed at how few of his Royal Air Force personnel participated in the defense of British air bases on Crete from German air assault and their subsequent loss, British Prime Minister Winston Churchill lamented:

> Every man in Air Force uniform ought to be armed with something—a rifle, a tommy-gun, a pistol. . . . Every airman should have his place in the defence scheme. . . . It must be understood by all ranks that they are expected to fight and die in the defence of their airfields. . . . The enormous mass of non-combatant personnel who look after the very few heroic pilots, who alone in ordinary circumstances do all the fighting, is an inherent difficulty in the organization of the Air Force. . . . Every airfield should be a stronghold of fighting air-groundmen, and not the abode of uniformed civilians in the prime of life protected by detachments of soldiers.[3]

Base defense should be comprehensive and involve the entire military population in one form or another. This requires leaders who will confront complacency and challenge those in their command who disavow any responsibility for their own security. A positive example of how Airmen can play a constructive role in the defense comes from Bagram Air Base, Afghanistan. In 2011, all Airmen were required to be armed and play a role in base defense and personal protection.[4] In addition, the base was broken into defensive sectors, and each sector had smaller defensive strongholds. All joint personnel, not just SF, defended these internal sectors. Not only did this ensure a comprehensive defense, but it also enabled the limited number of SF and military police to focus their efforts on the perimeter, exterior avenues of approach to the base and their response to actual penetration attempts.

Future military operations will undoubtedly limit the use of contractors in base defense. This will necessitate the further integration of Airmen and all base personnel into the defensive scheme. As has been noted about the USAF's ID doctrine, there is the intent of policy and doctrine and then there is the reality of how it is applied or rejected by the dominant organizational culture. The Marines have the motto that states, "Every Marine is a rifleman," regardless of military specialty. If ID is to be truly transformative, it must evolve to the concept that "Every Airman is a Defender," denoting an inherent obligation by Airmen to defend their joint and coalition partners, their aircraft and assigned sector, and themselves from an attack or insider threat. Major General Deale noted that "base defense is not just the defender's activities; it has to be a defense in depth with all Airmen engaged."[5] Know your mission, know your operational environment, and ensure everyone under your command knows their responsibility in the defensive scheme.

Notes

1. USAF, *AFDD 3-10, Force Protection*, 3.
2. Schwartz, *The Department of Defense's Use of Private Security Contractors.*
3. Churchill, *The Second World War,* vol. 3, *The Grand Alliance*, 692–93.
4. Capt Lucas Hall, email correspondence with Col Shannon W. Caudill, 18 April 2013.
5. Deale, interview.

Chapter 6

Intelligence Drives Maneuver: A Joint-Interagency Approach Is Critical

The failure to commit adequate intelligence assets to air base defense can lead to spectacular and devastating attacks. The terrorist organization the Liberation Tigers of Tamil Eelam (LTTE), also known as the Tamil Tigers, made an audacious attack on the Bandaranaike International Airport and its adjoining Sri Lankan air force base. Using suicide squad tactics, they infiltrated the military runway through storm drains on 24 July 2001.[1] Their attack destroyed or damaged 26 civilian and military aircraft and "revealed the weakness of strategic and tactical intelligence collection, analysis, dissemination, and review and, second, force protection. . . . There was no prioritization of intelligence gathering, projection, and sharing to erode the LTTE network."[2]

USAF intelligence assets have historically emphasized air operations to the detriment of intelligence about ground-based defense threats—a situation that proved highly problematic in Vietnam. As the Office of Air Force History observed, "Hobbling external security [in Vietnam] was the lack of reliable intelligence on enemy activities within striking distance of bases. This arose chiefly from the Air Force's failure to generate tactical ground intelligence."[3]

Illustrating this point, Lt Col Kenton Miller, the 3rd Security Police Squadron Commander at Bien Hoa, noted in his after-action report after the Tet Offensive in January 1968:

> The enemy regiment dressed in North Vietnamese Army (NVA) uniforms walked nine hours to reach the base. They walked past a 50,000 man US Army Camp (Long Bien Post), Army of the Republic of Vietnam (ARVN) Ranger permanent installation, III Corp ARVN HQ, 101st US Division base camp, staged in a village 200 yards off base, proceeded by two ARVN ambush sites, past two ARVN outposts on the base perimeter, over three base perimeter fences, through the minefield, and remained undetected until observed by a USAF Security Police K-9 team.[4]

In contrast to bases in Vietnam, JBB enjoyed a true commitment of intelligence assets for base defense. To remedy historical shortfalls in ground intelligence analysis, the 332nd Air Expeditionary Wing at JBB stood up a dedicated, ground-focused, force-protection intelligence

organization in November 2008 modeled after the joint intelligence cell template operated by the previous Army DFC.[5] Led and manned by USAF ISR professionals, the JISE received augmentation from contracted intelligence analysts focused on ground threats and the BSZ. Robust ground intelligence operations fully enabled Army and Air Force ground forces to defend JBB through proactive deterrent patrols, surveillance, and data analysis for terrain which IDF tended to originate.

The BSO fully leveraged USAF intelligence analysis and capacity to create synergy with his own intelligence staff, thereby optimizing the JISE's capabilities. This completely synchronized effort supported intelligence fusion designed to drive defense operations in the BSZ. The JISE's goal of attaining predictive battlespace awareness required foreknowledge and the ability to shape operations based not only on reviewing the enemy's past actions but also on predicting actions the enemy would likely take in the future. Classic approaches to intelligence based on analyses of historical trends tend to drive a defense posture that responds after attacks occur. In those paradigms, ground forces are no more than "shot responders" in a counter-IDF fight, essentially sweeping for the enemy in the location from which the IDF round came, as indicated by radar and spotter reports. This reactive approach became a frustrating exercise comparable to a game of "whack-a-mole," chasing the enemy around the battlespace without generating any lasting effects with the commitment of a great deal of energy and resources with little to show for it.

The JISE's analysis led to an intelligence-driven targeting process that enabled Air Force SF to move from a mostly reactive defensive posture to a proactive scheme of maneuver. Lasting effects of this strategy require dominance of the human terrain within and outside an installation as well as understanding the relationships among key groups, tribes, and individuals. This reality drove Airmen to study and gain insights into the violent extremist networks operating in the area and to participate actively in mapping and pressuring these networks through a constant presence. Both AFOSI and SF Airmen fed the intelligence cycle by gathering information from relationships they had established in the battlespace, thereby closing the intelligence gap between themselves and the enemy network.

Joint ID operations adopted an intelligence-driven model that followed four lines of operation based on JISE analysis: (1) denying the enemy unobserved freedom of movement, particularly in traditional

attack locations; (2) mapping out insurgent networks and identifying key leaders, weapons facilitators, and support nodes; (3) establishing patterns of life (e.g., determine who met with whom, when and where they met, and how they moved, shot, and communicated); and (4) mapping out the human terrain to discover fault lines among locals who hate the coalition, those who grudgingly tolerate but do little to help coalition forces, and, finally, those who might be willing to support efforts to secure the installation and the area surrounding it.

This effort prompted the development of an intelligence-collection plan and operational framework that cycled over a two-week period, maximizing the existing ground combat power. Additionally, intelligence analysis of historical data produced a strategy that denied the enemy access to his favored locations for launching attacks during the most likely times for hostile activities. Each intelligence objective had a list of subobjectives for signals intelligence resources, a similar list for airborne ISR resources, and so forth, including one for SF Airmen during their combat patrols.

Importantly, the Air Force's most recent irregular warfare doctrine recognized some of the positive lessons of JBB, Iraq. These included the intelligence synergy achieved by noting Airmen "coordinated closely with the battlespace owner (US Army) to ensure information sharing and the seams in the defense were covered." The wing leveraged "existing human networks to gauge US COIN efforts at various mass gatherings in and around the base boundary . . . [and] combined COIN and HUMINT [human intelligence] efforts of the entire 332nd Air Expeditionary Wing [which] resulted in an overall decrease of indirect fire attacks against the base by more than 50 percent."[6] Finally, the lessons learned from Iraq have application to home station as well. A commander must develop information-sharing processes and strengthen ties with local officials on a wide range of activities such as enhancing an installation's Eagle Eyes program, encouraging emergency response partnerships, and participating in regularly scheduled forums between installation, local, state, and federal law enforcement agencies. These meetings are likely already taking place; as a commander you need to be involved, or at least informed. Ultimately, commanders must understand the intelligence tools available to them, drive analysts toward useful products and analysis, and stay engaged in the intelligence process (see fig. 7 below) so that timely changes can be made to the defensive posture of the installation to meet the changing nature of the threat.

Figure 7. Intelligence process. (Source: Joint Chiefs of Staff, Joint Publication 2-0, Joint Intelligence, Washington, DC: Office of the Joint Chiefs of Staff, 22 October 2013, I-6, https://www.jcs.mil.)

Notes

1. Gunaratna, "Intelligence Failures Exposed."
2. Gunaratna.
3. Fox, *Air Base Defense in the Republic of Vietnam*, 171.
4. Miller, *3rd SPS Ground Defense Lessons Learned*, 6.
5. Col Timothy Farrell, email correspondence with Col Shannon W. Caudill, 4 May 2013.
6. USAF, *AFDD 3-2, Irregular Warfare*, 34.

Chapter 7

Air-mindedness Includes Using Air Assets for Base Defense

Leveraging air assets directly enables base defense. Vietnam showed the utility of gunship, ground attack, and helicopter employment in deterring and repelling enemy ground attacks from the air. In Iraq from 2008 to 2012, JBB's base defense effort integrated and incorporated air assets into its defensive scheme. JBB utilized JTACs as needed to support the base defense by requesting air support. Additionally, the wing fostered a collaborative atmosphere among many joint players who provided aerial support to the defense mission on largely an ad hoc and volunteer basis.

Through the standard air tasking order and collection-management processes, the JISE obtained regular Global Hawk and Joint Surveillance Target Attack Radar System (JSTARS) geospatial products as well as nationally derived intelligence products delivered through the combined air operations center's (CAOC) forward-deployed Air Force National Tactical Integration Cell. Despite the usefulness of these planned ISR assets, they were dwarfed by contributions of the expeditionary operations group and Army aviation units, both fixed and rotary wing, which delivered countless hours of "residual" ISR. To realize the most value from planned and residual airborne assets, the JISE had to produce, execute, and assess a comprehensive collection plan.

The JISE was effective at pulling together disparate units to reach a commonly desired end state: protecting their own people from IDF attacks. Because of the absence of an insurgent air threat and very few opportunities to strike targets kinetically, pilots and air planners welcomed the opportunity to fly residual ISR to protect the base, using their remaining fuel and loiter time after completing their primary missions. Members of the operations group collected intelligence, logging hundreds of hours as they followed insurgent leaders to meetings at all times of the day and night, and Army aviation units loitered at a distance, capturing imagery of insurgents' patterns of life. The JISE orchestrated a collection plan adaptable to residual flight schedules to piece together persistent ISR 15- to 60-minute time

intervals—the length of time that a residual asset would make itself available for the local ISR effort.

The JISE collection coordinator produced a daily collection plan known as the "residual deck." For each collection target, the plan included specific elements of information needed by JISE analysts to fill gaps in their knowledge of the target, the target's activities, and insurgent networks associated with the target. JISE partner analysts supplied crucial information about the activity patterns of each target by maintaining this information on a simple spreadsheet compiled each week. Planning also factored in predictable attack patterns of the enemy that took advantage of sandstorms, rain, and the moon's cycle. Given the nature of the Iraqi insurgency, successful ISR operations had to include ground-based collection by patrols in close contact with high-value individuals and the populace surrounding them.

Another example comes from Afghanistan. In 2010, at Bagram Air Base, synchronization and collaboration of available air assets included Predator unmanned aerial vehicles (UAV), F-16 and F-15 fighter aircraft, AH-64 attack helicopters, OH-58 observation helicopters, and Scan Eagle UAVs, which enhanced battlespace awareness and helped senior decision makers deconflict priorities to maximize available resources and properly position responding forces from the JDOC. Drawing on his experience as a wing commander in Afghanistan, Major General Deale said, "There is an 'air-minded' approach to air base defense; it is not just a large forward operating base to defend. Airmen need to ensure that defense of an air base goes well beyond perimeter security, including defending the mission by addressing the SAM [surface-to-air missile] threat and approach corridors—integrating military deception and other innovative methods to assure the continuity of air operations."[1]

In the case of Bagram, despite the complexity of air operations (with sorties launching around the clock), the wing leadership understood the value of flying ISR assets in support of base defense. The 455th Expeditionary Security Forces Squadron (ESFS) coordinated an "operations box" where they could fly organic Raven-B assets or launch Scan Eagle ISR platforms to support ground-based Air Force SF patrols or conduct independent area sweeps. In addition, despite the incredibly busy traffic pattern, the Mission Support and Operations Group commanders analyzed the air traffic pattern and historical base attack windows and locations and permanently employed an

aerostat "persistent threat detection system" aloft to provide ground maneuver forces a tactical edge.[2]

As displayed by vignettes from Iraq and Afghanistan base defense techniques, air assets can play an important role in the defensive scheme. Ultimately, prior coordination and synchronization of combat aircraft into the base defense scheme enabled US aircraft providing close air support capability to kill insurgents outside the wire, including those who were too close to the perimeter wall to be observed and engaged by SF personnel at tower positions on the base perimeter. Airmen must bring all their skill sets to the table to defend the air base, not trap themselves in one-dimensional thinking about ground threats. In short, air-mindedness is a framework for base defense operations.

Notes

1. Deale, interview.
2. Observations, Col Erik Rundquist, 455 EMSG/CC and TF 1/455 Commander Bagram, Afghanistan, 2011–2012.

Chapter 8

Law Enforcement Skills Are Critical to Base Defense and Irregular Warfare

Conflicts in both Iraq and Afghanistan resulted in an increased demand for law-and-order capability and revalidated the importance of basic law enforcement skills within the ID construct. After the merger of the law enforcement and security missions within the SF career field in the mid-1990s, SF underestimated the future requirements for law enforcement capability in base defense operations and irregular warfare. Subsequently, law enforcement skills deteriorated after the first Gulf War. High demand for this capability in Operations Iraqi Freedom and Enduring Freedom validated law enforcement as an important contributor to COIN operations and base defense. Law enforcement supports the nine stated desired effects of ID by aiding deterrence, detection, assessing, warning, defeating, delaying, defending, and recovery operations (refer to fig. 1).[1]

Law enforcement operations ensure public safety and good order and discipline and, importantly, enable intelligence activities through the investigation, tracking, and analysis of criminal activities on and off the installation. Law enforcement personnel play an important role in deterring crime, instituting theft prevention, ensuring traffic safety, conducting detainee operations, supporting security, and establishing local police force liaison. Air bases in combat zones are not US-only installations. Force structure caps and host-nation limitations mean heavy reliance on coalition, contractor, host-nation, and foreign national support. Theft of coalition supplies and materials by local nationals, contractors, friendly forces, or foreign nationals working inside the perimeter can affect the outcome of insurgent attacks outside the wire. In addition, black markets materialize, which can undercut good order and discipline, encourage the pilfering of supplies, and even lead to the sale of weapons by contractors and others that may enable the enemy. In short, police investigations give base leadership a deeper understanding of the nexus between criminal elements and potential terrorists and insider threats, which feeds intelligence activities supporting base defense.

Two modern examples show how the interconnection between criminal activity and terrorist groups can enable anticoalition forces.

In one, illegal arms sales in the International Zone in Baghdad threatened internal security and provided enablers to insurgent groups and criminal elements in 2006.[2] Another example is from JBB, Iraq, in 2009, where investigators discovered a black market fuel theft operation that was fed by a supporting network of illegal fueling points off the installation, potentially funding groups who were attacking the base.[3] The fuel was stolen on base by contractors, transferred off the installation, and sold for a profit. Both case studies illustrate that bases are ultimately porous because some trusted elements with access will use that access for nefarious purposes. Active and skilled law enforcement professionals provide the means necessary to identify the gaps and seams in the defense that would otherwise go undetected.

The need for law enforcement expertise is often overlooked, but history captures its necessity. In World War II, Gen William Tunner found himself struggling to resupply Chinese and American forces over the famed Hump: the Himalayan Mountains. The operational demands of this mission were extreme, but the pilferage of food and other supplies by indigenous workers became a true mission impediment. Tunner's leaders quickly adapted to this internal mission threat and created a police force to combat the theft. General Tunner described the effort:

> Our base at Barrackpore north of Calcutta was patrolled by one of the most unique police forces in the Army Air Force—a group of 259 Indians recruited from pension policemen, veteran soldiers, and retired Indian army officers. They were divided into four companies, one composed of Ghurkas, one of Sikhs, one of Pathans, and one of Hindus, each under the command of an American enlisted man. The American noncoms conscientiously studied the religion, customs, and language of the men in their companies, and could give them a verbal pat on the back—or chew them out—in their own language. Petty thievery decreased noticeably after the Indians began patrolling the beat.[4]

Effective law enforcement operations deny enemies and their support networks the ability to pilfer supplies and materials. Moreover, such operations allow coalition forces to concentrate on the mission. Law enforcement closes important avenues of ingress and egress used by smugglers and thieves and denies the enemy the ability to exploit these porous avenues of base access.

The stresses of combat can create an environment rich in problems like physical and sexual assault, vehicle accidents, and dereliction of duty, all of which can poison unit cohesion, dampen mission focus, and sap military strength. Ultimately, a well-organized law enforce-

ment effort will preserve and protect your mission, enable your understanding of the physical and human terrain in your area of operation, and illuminate how criminal networks operate in your backyard.

Additionally, strong law enforcement patrolling and community relationships are central to effective deterrence and response, especially with the growing threat of lone-wolf and self-radicalized terrorist attacks in the United States. In May 2016, Islamic State–linked hackers released photographs and addresses of 70 US Air Force pilots and military members in the hope that sympathizers and self-radicalized terrorists would materialize to attack them.[5] In June 2016, intelligence agencies reported that the Islamic State of Iraq and Syria (ISIS) had collected information on 77 US and NATO air force bases and had called on supporters to attack these locations.[6] A strong force protection plan goes beyond the physical boundaries of the installation and focuses on prudent security steps for individuals and families off the installation as well—where many can be targeted more easily.

Airmen often forget that the Air Force was the victim of a lone gunman attack in 1994 when a former Airman, discharged for mental health issues, returned to the base hospital to exact his revenge.[7] Dean A. Mellberg killed five people and wounded 23 at Fairchild Air Force Base's hospital. His initial attack focused on fatally shooting his psychiatrist and a psychologist, but he then turned his wrath on other hospital personnel and patients, killing an 8-year-old girl, wounding two toddlers, and killing the elderly spouse of a retiree.[8] No one was safe. Thankfully, an SF bike patrolman stopped Mellberg by confronting him outside the hospital and fatally shooting him before he could move to another facility to continue the attack. Regardless of the motivation, there are real and growing threats to air bases that require vigilance, preparation, exercises, and joint planning with local law enforcement.

Finally, greater coordination between the military and law enforcement is needed with the increasing political radicalization of veterans, law enforcement members, and, yes, active duty. There have been many instances of this phenomenon in recent years, but two are worth highlighting: (1) an Air Force sergeant killed a law enforcement officer as part of the radical antigovernment Boogaloo movement in 2020,[9] and (2) the 2021 Capitol Hill insurrection (1 in 5 of the defendants charged had military experience).[10] Table 1 shows the increasing lethality of individuals or small groups in attacking soft targets.

Table 1. Notable soft target attacks

Incident	*Year*	*No. Attackers*	*Weapon types*	*No. Killed*	*No. Injured*
Las Vegas Music Festival, NV	2017	1	Rifles	58	413
Orlando Night Club, FL	2016	1	Rifle, pistols	49	54
Inland Regional Center, San Bernardino, CA	2015	2	Rifles, pistols	14	22
Sandy Hook Elementary School, Newtown, CT	2015	1	Rifle, pistols	26	2
Movie Theater, Aurora, CO	2012	1	Rifle, shotgun, handgun, teargas	12	70
22/7 Oslo & Utoeya Island, Norway	2011	1	Rifle, improvised explosive device (IED)	77	33
Mumbai Attacks, India	2008	10	automatic weapons, grenades	173	308
Virginia Tech University, Blacksburg, VA	2007	1	handguns	33	23
Beslan School, Beslan, Russia	2004	32	automatic weapons, IEDs, rocket-propelled grenades	385	100+
Columbine High School, Littleton, CO	1999	2	handguns, shotguns, 99 small IEDs	15	24
Fairchild AFB, Spokane, WA	1994	1	rifle	4	23

(Source: Air Force Incident Management Course, Maxwell Air Force Base, 2016. Note: This is not a comprehensive list of every incident but rather a sampling that shows a variety of soft targets and their outcomes.)

Notes

1. USAF, *AFPD 31-1*, *Integrated Defense*, 3.
2. Special Inspector General for Iraq Reconstruction, *Quarterly Report to Congress*, 183; and Dahl, "Summary Report of Det 3, 732 ESFS, Mission Accomplishments."
3. Lt Col Keith McCormack, interview and email correspondence, 8 April 2013.
4. Tunner, *Over the Hump*, 96.
5. Pawlyk, "ISIS-linked Hackers Claim to Release Personal Information."

6. Handcocks, "ISIS Threat to US Air Bases."
7. "An Airman's Revenge: 5 Minutes of Terror."
8. "An Airman's Revenge: 5 Minutes of Terror."
9. MacFarquhar and Gibbons-Neff, "Air Force Sergeant with Ties to Extremist Group Charged."
10. Dreisbach and Anderson, "Nearly 1 In 5 Defendants in Capitol Riot Cases Served in the Military."

Chapter 9

Manage the Risk: Commit Intellectual Capital to the Fight

Ground combat and base defense operations, dynamic activities with infinite variables (threats) and finite resources, provide opportunities for you to lead. For commanders, the Air Force has moved away from being overly proscriptive on how to defend its bases and given its installation commanders a high degree of authority. This lack of specificity may be liberating at times and frustrating at others. Regardless, the base is executing the installation commanders' intent as they are generally the risk acceptance authority, although there are exceptions that will be discussed later. While there is no foolproof checklist on how to conduct base defense operations, you should be familiar with five fundamentals on how to conduct the fight.[1]

Aggressiveness. Regarding the geometry of an airfield, your defense forces should be aggressive in their action where they actively seek the initiative by meeting threats as far away from resources as much as possible. While an assault force typically enjoys advantages such as surprise, time, location, and attack methodology (swarming, stand-off, penetrating, surveillance, etc.). Defenders: enjoy the advantage of terrain and base familiarization; prepare the ground (alarms, rehearsals, sensors); seek intelligence and information sharing; and ultimately try to affect the attacker's sense of certainty and security.

Defense in depth. The security force should provide defense in depth to deny an assailant the opportunity to reach a resource by penetrating a single line. Depth increases the chance of detection and provides an opportunity to maintain continuous contact with an attacking force while responding forces maneuver into position to generate mass and fix the opposing force. As noted earlier regarding the BSZ, depth provides the commander time to make an informed decision, alert base personnel to take appropriate actions, and commit a quick reaction force to block or counterattack. Depth is accomplished by close coordination with external forces (local law enforcement, Army maneuver units, and coalition forces), off-base SF patrols, sensor fields, ISR, and so forth.

360° awareness. The security plan must take into account an all-around and three-dimensional perspective. Unlike larger army or naval formations, air bases are fixed locations and cannot give up ground, unless the base is to be evacuated. Insurgencies are characterized by the lack of a contiguous linear battlefield where air bases are not afforded the safety of a rear area behind friendly lines (as seen in WWII, the Cold War, and Desert Storm). Moreover, airfields offer unlimited approaches for special operations forces and insurgents (tunnels, sewer systems, cyber, stand-off, maritime approaches, etc.), not to mention the fact that local populations on expeditionary air bases present significant insider threat challenges.

Integration. Any base defense plan needs to be integrated where multiple parties mutually support each other for a common purpose. Tactically, this can mean interlocking fields of fire and observation between different organizations and covering gaps that come to light as the plan is developed. Often, installation command centers, such as JBB's JDOC, enable full integration and mission deconfliction. Commanders must also examine and test the relationship between multiple C2 elements such as crisis action team, wing operations center, emergency operations center, maintenance operations center, unit control centers, higher headquarters on the base, and so forth, and aggressively seek to fill gaps and information voids.

Key terrain. Finally, air base defense activities should be organized around key terrain. Key terrain is any ground/facility that offers concealed approaches to the base or provides the holder a marked advantage. For instance, anywhere that enables an attacker to observe base activities, monitor/jam communications, or safely assemble forces is probably key terrain. From a kinetic perspective, key terrain also is ground where an insurgent can fire directly or indirectly against an installation or critical off-base infrastructure (navigation aids, supply lines, fuel systems, etc.). Key terrain needs to be physically occupied, randomly patrolled, or denied (through obstacles, sensors, weapons fire, or removing the terrain).

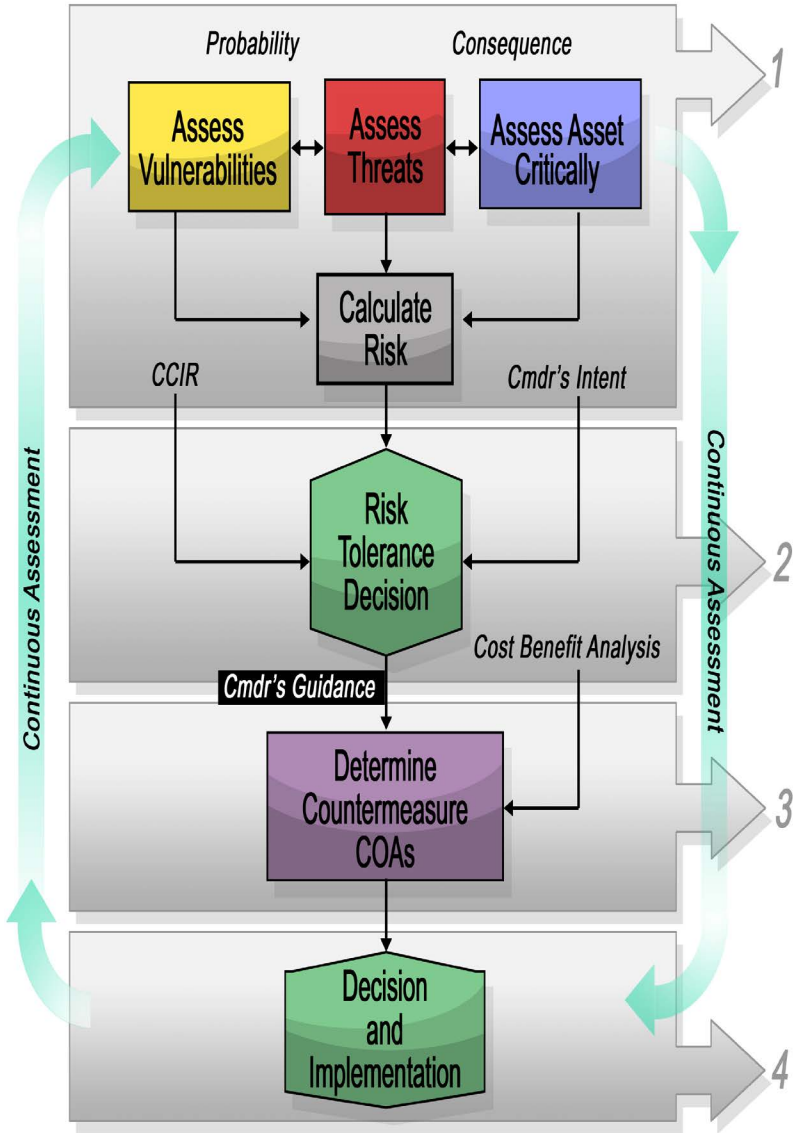
By quickly examining the key fundamentals of base defense, the critical takeaway is that there is no foolproof checklist for how to hold and secure ground. However, these fundamentals orient you to the characteristics of successfully employing a base defense force. The Air Force transitioned from compliance to "effects-based" security in 2009, which both permitted and encouraged installation commanders to exercise tactical flexibility. However, when sequestration re-

duced the number of available military personnel and reallocated physical security funds for other projects while defense forces remained at a high deployment tempo, terrorist organizations demonstrated the strategic reach to inspire and motivate attacks within the United States (i.e., Little Rock, Fort Hood, Boston, Chattanooga, and San Bernardino). Commanders have been asked to increase their risk tolerance in a very dynamic and unforgiving environment.

Regarding risk management, installation commanders must be made aware of significant challenges.[2] Air Force policy mandates that all installations, regardless of geographic location, require a comprehensive integrated defense plan (IDP) signed by the wing commander. The IDP indicates how the base is to be defended using all available resources and with proscriptive methods derived from risk analysis and management tools that examine factors such as threat, vulnerability, and criticality.

Once the IDP is developed, it must be tested repeatedly and under a range of conditions to determine its level of effectiveness. How do commanders know if their intent and approaches are working? The answers are regular base defense and force protection exercises, continuous leader engagement, war-gaming, constant analysis of the plan, and continual evaluation of real-world events and intelligence. Be mindful that the various functional communities on the installation have different perspectives on threats—international terrorism, homegrown violent extremists, foreign intelligence, information protection, domestic criminal and gang activity, medical force health protection, operational security, cybersecurity, and so forth. All these inputs are important to the protection of your installation—and very rarely in today's environment will all these inputs default to the "no threat to low threat" setting. The effort to develop an IDP via the risk-management process requires the active participation of all mission owners and cannot be relegated to a handful of functional communities.

Buying down risk—going, going, gone. As the leadership develops an IDP and assesses facilities and missions, the team must make actionable recommendations to reduce the risk to missions and forces. Often, discussions involve getting more "gates, guards, and guns" to reduce risk. In some cases, this may be a solution, but as a commander you may have limited maneuver forces to dedicate to this task. Be open to suggestions such as reducing the signature (i.e., remove signs identifying a particular building), advocate for creating a redundant/backup capability, use technology to enhance entry



Key
CCIR: commander's critical information requirement
COA: course of action

Figure 8. Risk-Management Process: creating a smart defense that better uses resources to meet the threat. (Source: AFI 31-101, Integrated Defense.)

control and circulation flow throughout a building, ensure alarms are in place, increase SF patrol coverage, examine force protection engineering solutions, determine if owners of the facilities should be armed (i.e., unit marshal program or selective arming), and so forth. More often than not, the working groups can generate solutions to reduce risk that are acceptable to all parties involved.

Notes

1. Erik K. Rundquist, "Air Base Defense Doctrine," taught to HQ Air Mobility Warfare Center's Phoenix Readiness and Contingency Support Operations Course, Fort Dix, NJ, 1996–1999.

2. The authors would like to thank the ACC/A4S, Integrated Defense Operations Branch (A4SO), Mr. Wayne Chapman, and Mr. Curtis Easley for providing an historical analysis and perspectives on defending air bases under the auspice of the Air Force integrated defense risk management program, interviewed 20 May 2016.

Chapter 10

Nowhere to Hide: Anticipate Future Threats and Develop Countermeasures

Protecting air bases and aerospace assets in the future will grow exponentially more complex and expensive due to the proliferation of technology, abundance of open-source intelligence, and growth in adversary capabilities. Of course, as learned in 2020, pandemics and disease epidemics can further complicate security efforts by threatening the health of security staff and making the base entry screening process lengthier and more cumbersome because of masks and health protocols. Looking forward, traditional threats such as airborne assault, IDF through rockets and mortars, and direct attack by suicide squads will continue to be staple courses of potential enemy action. It is important to examine emerging threats enabling new modes of air base attack, including the development of precision munitions, the spread of RPVs (large, small, and micro), the proliferation of shoulder-fired missiles, insider threats, and other variants of new technology for terrorists and insurgents. Looking to the future, exploitation of cyber vulnerabilities and technological proliferation will further enable air base attack. Defending air assets will become even more problematic with increasing vulnerabilities across the spectrum of threats. The problem set goes beyond the traditional kinetic threat of indirect fire or ground attack. With relatively little modern technology, enemy forces were able to cause damage to flying assets (see table 2).

The threat of terrorism has driven most base defense operations to focus operations on the defeat of vehicle-borne improvised explosive devices (VBIED). Top-tier terrorist groups have long wanted headline-grabbing attacks that are big on visual imagery, shock, and body count. Images of the Marine barracks in Beirut, Lebanon, or the Air Force's Khobar Towers in Khobar, Saudi Arabia, became the adversary's desired outcome of an attack. We see the same intent at play in the Taliban's detonation of a truck bomb on the tenth anniversary of the terrorist attacks of 11 September 2001—a strike that wounded 89 people, including 77 Soldiers. This section examines some of the more alarming threats—such as VBIEDs, which we expect the enemy

to use in future attacks—and the emerging technology that could enable them to assail our air bases. The list below highlights some, but not all, of the emerging technological threats to air bases.

Table 2. Statistical comparison of fixed-wing aircraft destroyed and damaged by air base attack

Theater	Number of fixed-wing aircraft destroyed	Number of fixed-wing aircraft damaged	Estimated size of insurgency
Vietnam (1964–73)	99	1,170	300,000[a]
Iraq (2003–12)	0	15	20,000–100,000[b]
Afghanistan (2002–14)	6	4	20,000[c]

Source: Data was produced during the 2013–14 Air Command and Staff College yearlong research elective Defending Air Bases in an Age of Insurgency, instructed by Col Shannon W. Caudill. Student researchers were Maj Russell S. Badowski, Maj Jason F. Baggett, Maj Scott Black, Maj Loren M. Coulter, Maj Colby B. Edwards, Maj Raymond J. Fortner, Maj Steward J. Parker, and Maj Michael M. Wellock. Researchers reviewed all available Air Force history reports covering Sather AB (Baghdad International Airport), Joint Base Balad, Tallil AB, Kirkuk AB, and al-Asad AB. See notes 1–3 and below for specific sources.

[a] "Origins of the Insurgency in South Vietnam, 1954–1960," The Pentagon Papers, Gravel ed., vol. 1 (Boston: Beacon Press, 1971), chap. 5, sec. 3, 314–46, www.mtholyoke.edu/acad/intrel/pentagon/pent14.htm.
[b] Daniel L. Byman, "Iraq and the Global War on Terrorism," Brookings Institution, 1 July 2007, https://www.brookings.edu/articles/iraq-and-the-global-war-on-terrorism/.
[c] Peter Bergen and Katherine Tiedemann, "Commentary: More Troops Needed for Afghan War," CNN, 4 August 2009, http://www.cnn.com/2009/POLITICS/08/04/bergen.afghanistan/index.html.

Precision indirect fire. IDF has been the traditional choice among insurgents for attacking an air base. Fired at a distance and often rigged to fire after the attacker has departed, it offers a degree of survivability. In Afghanistan, the enemy employed IDF not only to harass coalition forces but also to mask and cover ground attacks. On 22 August 2012, enemy forces even managed to damage the visiting aircraft of the chairman of the Joint Chiefs of Staff.[1] Mortars and rockets aimed at a base by someone with limited targeting information rely on the technical expertise of the operator, factors that hinder their overall effectiveness. However, a new age in precision IDF weapon systems is now upon us. On 31 March 2011, Soldiers from the 4th Brigade Combat Team fired a 120 mm precision-guided mortar round from Forward Operating Base Kushamond, Afghanistan, hitting within four meters of the target.[2] Normally a mortar fires a "dumb" round—one that has no onboard guidance system. Over time this technology will likely spread to insurgent and terrorist groups, improving their ability to pick and choose targets with extraordinary accuracy and making aircraft as well as key facilities much more vulnerable. No doubt peer competitors will employ this technology

and provide it to their proxies when advantageous to their strategic interests.

Remotely piloted vehicles. Personnel contemplating defense of an air base must consider the threat posed by RPVs by formulating a plan to tackle a range of remote threats, both ground and airborne. Who is cleared to engage such vehicles, and with what weapons? For ground-based attacks, the answer is more clearly defined and in line with established contingencies; however, a defensive gap exists in defending against airborne threats. The fact that we have yet to fully explore protocols for these defenses leaves a seam that a technologically savvy enemy could exploit.

In fact, the Department of Homeland Security warned in 2015 that it had documented over 500 cases of unknown and "unauthorized" RPVs that had flown and, in some cases, loitered over "sensitive sites and critical installations," including military bases.[3] Beyond the surveillance value, off-the-shelf RPVs are capable of being converted into flying bombs or guns. The "weaponizing" of small drones is not terribly difficult. In 2016, ISIS militants began weaponizing drones, which started as simply booby-trapping the craft and evolved into ordnance delivery against a target.[4] By 2020, US forces in Iraq reported being attacked by drones carrying bombs using ordnance made with 3-D printers.[5]

Of more pressing concern, Hezbollah has shown technological prowess through its use of explosive-laden RPVs and missile technology, even managing to cripple an Israeli warship.[6] Although American policy makers have concerned themselves with al-Qaeda in recent years, Hezbollah has proven to have global reach and staying power. It is credited as the first terrorist group to pioneer the use of suicide bombers as a weapon of mass destruction, delivering large vehicle bombs to specific targets.[7] The success of the organization comes from its financial and logistical backing by Syria and Iran, the latter supplying advanced weapons and reconnaissance equipment. Starting in November 2004, Hezbollah shocked Israelis by launching a remotely piloted surveillance plane, the Mirsad 1, that flew over Israeli towns and returned to Lebanon unharmed. At a Hezbollah rally, the organization's leader, Hassan Nasrallah, declared, "You can load the Mirsad plane with a quantity of explosive ranging from 40 to 50 kilos and send it to its target. . . . Do you want a power plant, water plant, military base? Anything!"[8]

To punctuate this point, examine the case of Rezwan Ferdaus, a 26-year-old US citizen. He was arrested on 28 September 2011, charged with plotting to attack the Pentagon and US Capitol with "large remote controlled aircraft filled with C-4 plastic explosives" and providing "material support and resources to a foreign terrorist organization, specifically to al-Qaeda."[9] According to the FBI, Ferdaus planned to augment his "aerial assault" by three explosive-laden drones with a ground attack that included "six people, armed with automatic firearms and divided into two teams." Ferdaus explained that "with this aerial assault, we can effectively eliminate key locations of the P-building [Pentagon] then we can add to it in order to take out everything else."[10]

Social media: Flash mobs, terrorism, and networking base attacks. Instantaneous communication dramatically improves enemies' information operations and base attacks, allowing them to draw upon elements of a sympathetic local populace to create situations that embarrass an air base's leadership or overwhelm defenses. Thus, intelligence and law enforcement must stay one step ahead of an increasingly agile foe by becoming more adept in their collection efforts. Basic technology (such as cell phones) affects society in unusual ways by creating unprecedented means for communicating and coordinating actions. Take for example the phenomenon of the flash mob, a group of people summoned via cell phone, social media, and viral emails for the purpose of performing some sort of act at a specific location. The web and even commercials of telecommunications companies are replete with footage of benign flash mobs who appear in a public place to carry out some sort of unusual or artistic act, like freezing in one place or performing a coordinated dance routine. Although they do this in the name of entertainment, what happens when someone uses this same technology for nefarious purposes?

Terrorists and criminal groups are increasingly using social media for the "purpose of operational communication, intelligence gathering, technical information sharing, recruiting, training, etc."[11] As an example, a study from Brookings Institution's Center for Middle East Policy found that between September and December in 2014 there were an estimated 46,000 to 70,000 Twitter accounts owned and operated by Islamic State supporters and activists with each having an average of 1,000 followers per account.[12] In 2019, a bored 21-year old party organizer started a Facebook page called "Storm Area 51: They Can't Stop All of Us" that quickly went viral, gaining over one million

RSVPs, and causing Air Force and government officials to make public statements to counter this potential security risk.[13] Finally, an example of mass criminal activity organized through social media occurred in England in 2011, in which riots occurred in London, Birmingham, Manchester, and elsewhere. British authorities identified and arrested nearly 3,000 people suspected of physically rioting or inciting violence across the country by using BlackBerry Messenger, Twitter, and Facebook.[14] David Cameron, former British prime minister, observed that "everyone watching these horrific actions will be struck by how they were organized via social media. . . . So we are working with the police, the intelligence services and industry to look at whether it would be right to stop people communicating via these websites and services when we know they are plotting violence, disorder and criminality."[15] The above examples provide a glimpse of the power of social media and its potential as a means of organizing an attack on a military installation in the future.

The rapid pace of technological advancement has spread to every corner of the globe. Cell phones are now powerful computers, networking with other devices globally. Nowhere is this more apparent than in developing countries that had poor communications because of the cost of hard-wiring infrastructure for landlines. Cell phones now make that expense moot since cell towers and satellites allow such countries to plug into the global communications grid. The same technology that enables global information sharing and advancement also supports the networking of terrorist and criminal groups.

How will this technology and social networking affect base security in the future? Protestors, mobs, and terrorist groups can now be easily summoned with no prior notice to military intelligence or law enforcement, quickly assembling near a base's entry control point or perimeter to protest, riot, or attack. In many instances, such areas would have only a handful of guards available to counter the assembled groups—a scenario that could easily overwhelm the few SF on scene and escalate beyond their capacity to quell such action.

It is easy: Obtaining maps and imagery of air bases. Enemy forces planning a ground assault of an air base used to rely on collaborators who had access to the target base to facilitate the mapping of terrain and key facilities, as well as attain pace counts that enable IDF attacks. Today the information superhighway offers access to satellite imagery and other open-source information that make the job of a would-be attacker much easier. One such website, that of the

Federation of American Scientists (FAS), describes itself as "an independent, nonpartisan think tank and registered 501(c)(3) nonprofit membership organization . . . dedicated to providing rigorous, objective, evidence-based analysis and practical policy recommendations on national and international security issues connected to applied science and technology."[16] Global Security, an offshoot of FAS founded by John Pike, one of its former members, claims to be "the leading source of background information and developing news stories in the fields of defense, space, intelligence, WMD [weapons of mass destruction], and homeland security."[17] Its website features satellite images of military bases around the world, many of which the US government considers classified. Other sites, such as Google Maps, make imagery and street maps available. In sum, people now have many ways to acquire detailed maps of air bases that could facilitate attacks on those locations.

The expanding insider threat and lone wolves. For the foreseeable future, US and coalition forces will operate amid insider threats. Pentagon statistics reveal that in Afghanistan from 2008 to 2018, insider attacks by members of the Afghan National Security Forces on US and NATO personnel claimed the lives of 155 US military members, coalition troops, and contractors, and wounded over 200.[18] One of the most egregious and horrific instances of an insider threat occurred on the morning of 27 April 2011, when an Afghan air force captain killed eight Airmen and one contractor at Kabul International Airport.[19] Another incident demonstrated how a determined and crafty suicide bomber could infiltrate a Central Intelligence Agency (CIA) base in eastern Afghanistan and kill eight Americans.[20] In 2014, Afghan insurgents managed to kill a US Army major general,[21] and in 2018, a US Army brigadier general was shot while the US commanding general in Afghanistan barely escaped injury.[22]

More troubling still is the growing threat from within the ranks of American military personnel and veterans. On 11 May 2009, five American military members were killed by a US Soldier at a military counseling center in Camp Liberty, Baghdad.[23] Shootings by a US Army psychiatrist on 5 November 2009 in Fort Hood, Texas, resulted in the deaths of 13 people and wounding of 32 others.[24] Since a 2009 Department of Homeland Security report, law enforcement officials have become increasingly concerned about military veterans joining right-wing extremist groups.[25] Indeed, a Security Forces Airman apparently was involved in an extremist group and was arrested as the

primary suspect in the June 2020 killing of a California sheriff's deputy and wounding of his partner with a rifle.[26]

As displayed in table 1, it is important to remember that one person can do a great deal of harm—witness the number of lone-wolf incidents that have occurred. As an example, on 22 July 2011, Anders Breivik, a Norwegian, set off a vehicle bomb near government buildings in Oslo, killing eight, and then massacred 69 people at a youth camp on the nearby island of Utoeya.[27] On 20 July 2012, American James Holmes walked into a sold-out movie theater near Denver and began shooting, killing 12 and wounding 58.[28] Whether stateside or overseas, commanders must ensure that they provide and exercise a comprehensive interior security plan—one that includes using all the psychological tools and law enforcement capabilities available to identify insider threats.

Well-defended air bases drive the enemy to explore alternative means to affect air operations. If your defenses persuade an attacker to pursue another target, you and your team have done their job. You can do your part to affect the enemy's observe-orient-decide-act (OODA) loop, whether that is a terrorist or a lone-wolf attacker.[29] Naturally, any rational actor desires the quickest, cheapest route to success in negatively affecting air operations or creating an international sensation through a high death count, as an ongoing cost-benefit analysis drives target selection.

When examining the threat, one should constantly ask what the enemy will target, because it is not necessarily aircraft on the ground. Targets and objectives depend upon the attackers, ranging from terrorist groups to conventional forces to special operations, and upon the political objectives and actual capabilities that they can bring to bear against an air base. In Vietnam, enemy forces found ground attacks against airfields a drain on their resources. As a result, they adapted their tactics to focus on disrupting versus destroying air operations, because "whether the raids resulted in aircraft, facility, or runway damage, sortie rates were impaired."[30] Both Iraq and Afghanistan provide modern examples of IDF attacks that temporarily closed airfields, thus delaying sorties with a negative mission impact.

Understanding and countering these growing threats will play a major role in the ability of the United States and its allies to effectively project airpower effectively in the future. One solution is to base aircraft as far from hostilities as possible, which strains aircraft and aircrews with longer flight times, reduces potential loiter times, and potentially

reduces the persistence of airpower. However, it does not address the likely requirement for mobility aircraft to land near or in the combat zone to provide support to ground operations. Nor does remote basing address the technological means of attack through cyberspace, reach and lethality of technologically enabled terrorists, or special forces engagement by a determined enemy. These concerns require Airmen to conduct a truly full-spectrum threat analysis and ensure these potential vulnerabilities are addressed in force protection planning.

Notes

1. Starr, "Shrapnel Hits Joint Chiefs Chairman's Plane."
2. Christopherson, "Soldiers Fire First Precision-Guided Mortar in Afghanistan."
3. Esler, "What a Business Aviation Flight Department Needs to Know."
4. Reuters, "ISIS Booby-trapped Drone Kills Troops."
5. Woody, "Drones Are Dropping Bombs on US Troops."
6. Associated Press, "Israel: Iranian Troops Helping Hezbollah Attack."
7. Helmer, "Hezbollah's Employment of Suicide Bombing during the 1980s."
8. Myers, "Hezbollah Drone Threatens Israel."
9. Federal Bureau of Investigation (FBI), "Massachusetts Man Charged with Plotting."
10. FBI.
11. Hossain, "Social Media and Terrorism."
12. Berger and Morgan, *The ISIS Twitter Census*.
13. Montero, "Storm Area 51 Creator."
14. Lancefield, "3,000 Arrests in London Riots Investigation."
15. Halliday, "David Cameron Considers Banning Suspected Rioters."
16. Federation of American Scientists, "About FAS."
17. Global Security, "Company History."
18. Constable, "U.S. Military Scales Back Contacts."
19. Pawlyk, "Questions Remain as Families Mourn Victims."
20. Warrick, "Suicide Bomber Attacks CIA Base in Afghanistan."
21. Sciutto, Shoichet, and Fantz, "U.S. General Killed in Afghanistan."
22. Martinez, "US General Was Wounded in Kandahar Attack."
23. Williams, "US Soldier Kills 5 of His Comrades in Iraq."
24. Lieberman and Collins, *A Ticking Time Bomb*.
25. Associated Press, "Homeland Security Leaders Defend Memo on Veterans."
26. Dazio, "Airman Charged with Murder of Federal Officer."
27. BBC, "Anders Breivik Describes Norway Island Massacre."
28. Johnson and Williams, "Cops: Weeks of Planning Went into Shootings at Colo. Batman Screening."
29. Boyd, "Destruction and Creation."
30. Buonaugurio, "Air Base Defense in the 21st Century," 8.

Conclusion

Finding the precise balance between force projection and force protection lies with the subjective judgment ultimately reserved for those bestowed with the command. The fog of war, the uncertain risks of combat, and the actions of a determined foe do not relieve a commander of the responsibility for decisions that a reasonable, prudent commander of the same grade and experience would have made under similar circumstances.

—Gen James F. Amos, Commandant, US Marine Corps
Accountability Determination of US Commanders for the 14–15 September 2012 Attack on the Camp Bastion, Leatherneck, and Shorabak (BLS) Complex, Helmand Province, Afghanistan

Commanders have many demands and priorities. In a command portfolio, one area commanders are often least comfortable in is their responsibilities for a ground defense. Central to a true integrated defense is a command climate that stresses that all leaders and installation members, including coalition and joint forces, understand their role in the defense and the effects, positive and otherwise, of their own actions in the battlespace. Senior commanders set the tone, but all commanders must play a role and be the squeaky wheel when they believe there are security gaps. Looking the other way or simply writing it off as an SF and AFOSI issue is an abrogation of responsibility. From his own base defense experience, Major General Deale summarizes his view as: "The Senior Airman at any location has got to be equipped to lead the base defense. We also need Defense Force Commanders who know their business and can effectively shape the perspectives of the Senior Airman on scene to ensure an effective defense."[1]

We often focus on terrorist groups and lone-wolf attacks, forgetting that there are also nation-state forces preparing for conflict and focusing on air bases as the critical hubs to target their efforts. Not too long ago, planners at NATO bases concentrated on the USSR's plans to attack air bases. During the Cold War, the Soviets explored ways to assault and disable bases, primarily by employing the Spetsnaz (special forces). A review of Spetsnaz airfield-attack profiles in declassified Cold War–era CIA reports would prove useful because they provide insights into methods for direct strikes on these targets. These included the airdrop near an air base of 30 special operators,

who then broke into "four teams, each team with specific responsibilities including capturing vehicles and personnel for the purpose of infiltrating the target [air base]," using SAMs and explosive devices to destroy aircraft.[2] Additional methods were also practiced: a Spetsnaz company (approximately 10 teams of five to 12 men) operated against a heavily defended airfield. The company could not get closer than 2 to 3 km to the target. During the first night Block Strelas [three-tubed SAM launchers mounted on a tripod] were positioned as close as possible to either end of the field, and then attacks were initiated against pipelines, powerlines, communication lines, security personnel, and crews heading toward the airfield.[3]

This type of attack would disrupt airfield operations, create the impression that a larger Soviet force was in the area, and draw more NATO forces in for defense and away from the front lines. Imagine well-trained enemy special forces enabled by many of the aforementioned technological advances. Base defense would become incredibly difficult, and the complexity of countering the threat would escalate significantly. This is one threat to contend with in future nation-state warfare, one which does not usually spring to the forefront given the recent focus on lone-wolf, terrorist, and insurgent attacks.

Defending air bases is a challenge that can only be met by agile, dynamic thinkers, backed by an Air Force and joint force that value air base defense as a central component to airpower itself. The complexity of the threat posed to air bases and other military installations will only grow. Airmen must debate and engage with one another about the future of air base security and the required defenses for a multitude of operational environments. In command, whether deployed or at home station, you are charged with a lofty responsibility of protecting mission assets, military members, and families.

In summary, commanders must lead the defense, understand their operational environment, manage the risks and defensive partnership opportunities, and take the steps needed to safeguard the people and assets needed to sustain our national defense mission. Your Airmen and joint force members are counting on you. You own it. You've got this. Lead from the front.

Notes

1. Deale, interview.
2. Director of Central Intelligence, *Warsaw Pact Nonnuclear Threat*, 35.
3. Director of Central Intelligence, 36, 39.

Afterword

It is no coincidence that the Chief of Staff followed the 2019 "Year of the Defender" with 2020's commitment to the "Year of Integrated Base Defense." We have the best security forces in the world, but defending, or "fighting the base," requires an active role by everyone on the base. Churchill correctly observed that "every airman should have his place in the defence scheme." Our Air Force has emphasized this point with phrases like "every Airman a sensor" and "defending the base is commander business," yet there is still resistance in some corners, because it is outside functional lines or because some do not believe the concept is realistic. We are the most powerful Air Force in the world, and this is exactly why commanders at all levels need to understand their role in fighting the base. Future threats will be multispectrum and simultaneous: they will come from the air, ground, electronic spectrum, space, sea, cyberspace . . . wherever our adversaries sense an advantage. It is vital to our success that all Airmen understand and embrace their role in fighting the base.

The national defense strategy focuses on those near-peer potential adversaries that we know will threaten our operations from a 360-degree multidimensional spectrum. Whether deployed or in the homeland, our operating locations are no longer a sanctuary, and we must be able to fight through different types of attack while continuing to generate air- and space power. Our installations are our power-projection platforms. It does not matter if we are fighting in air or space—we operate from these power-projection platforms, and these bases will be targeted. Long-standing installations where high-demand, low-density aircraft are operated are but one of several likely targets, both from the kinetic and nonkinetic sense. We must be able to fight through different scenarios.

If adversaries can slow down or disrupt our sortie generation, they are successful. We must all think through our processes and procedures to ensure we can continue the fight. Think about what happens today if someone fires a shot on base: we lock down the entire base until security forces clear the affected area. We cannot afford to shut down the base for this, an Amber Alert, or any other single threat; we must apply risk management principles and fight through the scenario by releasing nonaffected sectors and defending our mission sets. Are you practicing this? Are you practicing and planning for

asset dispersal across the installation so we do not have all our spare engines, fuel trucks, or unique pieces of equipment locked in the same place? This is "fighting the base" and is each commander's responsibility. You must make sure your mission can continue with the personnel and material on hand. Can you shift personnel across mission sets to reopen a bombed-out runway, or is this a Civil Engineering only squadron responsibility? Our logistics readiness squadron personnel are also trained on heavy equipment—have you familiarized them with runway repair ops and turned them into multicapable Airmen?

Commanders lead more than their squadron mission: they are responsible for the protection of their people and warfighting assets. It is a solemn duty that cannot be subcontracted. Unfortunately, too many leaders rely solely on security forces or the ground component to protect. We are all in this together—as warriors—as Airmen—as Defenders!

It is fitting that the final volume of the *Defending Air Bases in an Age of Insurgency* series is focused on providing lessons and principles for commanders, especially principles for the next era, beyond an insurgency and instead one of a near-peer state-sponsored competitor. Our collective defense can only be truly integrated if all installation organizations are led by those who understand and embrace their responsibility to protect their people and mission.

My charge to each commander is to read this book, study your base defense plans, analyze your unit's role, and ask questions to ensure your plans have transitioned from that of insurgency to a near-peer, more skilled adversary. Please take the initiative to address those shortfalls in the design and implementation of these plans and instill a warrior culture in your organization to enable our very best defensive effort. Remember, you set the tone and ensure we can "Fight the Base!"

JOHN T. WILCOX II
Major General, USAF

Appendix A

Base Defense Terminology

(All terms drawn from the *DOD Dictionary of Military and Associated Terms*, except as noted.)

area damage control (ADC)	Measures taken before, during, and/or after a hostile action or natural or man-made disasters to reduce the probability of damage and minimize its effects.
base boundary	A line that delineates the surface area of a base for the purpose of facilitating coordination and deconfliction of operations between adjacent units, formations, or areas.
base cluster	A collection of bases, geographically grouped for mutual protection and ease of command and control.
base cluster operations center (BCOC)	A command-and-control facility that serves as the base cluster commander's focal point for defense and security of the base cluster.
base defense	The local military measures, both normal and emergency, required to nullify or reduce the effectiveness of enemy attacks on, or sabotage of, a base to ensure the maximum capacity of its facilities is available to US forces.
base defense operations center (BDOC)	A command-and-control facility established by the base commander to serve as the focal point for base security and defense.

base security zone (BSZ)	To secure airpower assets and protect personnel and resources in this area, the Air Force uses a unique planning construct, referred to as the BSZ. The BSZ is that area from which the enemy can launch an attack against the personnel and resources located on or aircraft approaching/departing the base. The term, an Air Force–specific term used intraservice only, is similar to but not synonymous with the term base boundary as defined in JP 3-10, *Joint Security Operations in Theater*. The base commander is responsible for identifying the BSZ and coordinating with the host nation or area commander for the BSZ to be identified as the base boundary. If the base boundary does not include all of the terrain of the BSZ, the base commander is still responsible for either mitigating (though coordination with the area commander or host nation) or accepting the risks of enemy attack from the area outside the base boundary. (Source: *Air Force Policy Directive [AFPD] 31-1, Integrated Defense*, and *Air Force Instruction (AFI) 31-101, Integrated Defense [ID]*)
defense force commander (DFC)	The individual provided authority to conduct integrated base defense for the senior Air Force commander responsible for an air base. The defense force commander exercises command and control through an established chain of command and directs the planning and execution of base defense operations. (Source: *AFPD 31-1* and *AFI 31-101*)

force protection (FP)	Preventive measures taken to mitigate hostile actions against Department of Defense personnel (including family members), resources, facilities, and critical information.
force protection condition (FPCON)	A Chairman of the Joint Chiefs of Staff–approved standard for identification of and recommended responses to terrorist threats against US personnel and facilities.
force protection detachment (FPD)	A counterintelligence element that provides counterintelligence support to transiting and assigned ships, personnel, and aircraft in regions of elevated threat.
force protection intelligence	Analyzed or vetted all-source information that drives effective FP decisions and operations. (Source: *AFPD 31-1* and *AFI 31-101*)
force protection working group (FPWG)	Cross-functional working group whose purpose is to conduct risk assessment and risk management and to recommend mitigating measures to the commander.
integrated defense (ID), integrated base defense	An Air Force term that indicates the integration of multidisciplinary active and passive, offensive and defensive capabilities, employed to mitigate potential risks and defeat adversary threats to Air Force operations. Installation commanders will determine the effect and intensity of ID operations required at garrison and deployed locations through a risk estimate of the installation's operating environment. (Source: *AFPD 31-1*)

joint base	In base defense operations, a locality from which operations of two or more of the Military Departments are projected or supported and which is manned by significant elements of two or more Military Departments or in which significant elements of two or more Military Departments are located.
joint security area (JSA)	A specific area to facilitate protection of joint bases and their connecting lines of communications that support joint operations.
joint security coordination center (JSCC)	A joint operations center tailored to assist the joint security coordinator in meeting the security requirements in the joint operational area.
joint security coordinator (JSC)	The officer responsible for coordinating the overall security of the operational area in accordance with joint force commander directives and priorities.
law enforcement agency (LEA)	Any of a number of agencies (outside the Department of Defense) chartered and empowered to enforce US laws in a state or territory (or political subdivision) of the United States, a federally recognized Native American tribe or Alaskan Native Village, or within the borders of a host nation.
mobile security force (MSF)	A highly mobile and dedicated security force with the capability to defeat Level I and II threats in a joint security area.
port security	The safeguarding of vessels, harbors, ports, waterfront facilities, and cargo from internal threats such as destruction, loss, or injury from sabotage or other subversive acts, accidents, thefts, or other causes of similar nature.

provost operations	The integrated application of active and passive offensive and defensive actions taken across the ground dimension of the battlespace to promote and maintain public order (law enforcement) and efficient military operations. Detects and investigates threats and criminal activity in coordination with other agencies. Safeguards detained persons. (Source: *AFPD 31-1* and *AFI 31-101*)
regional security officer (RSO)	A security officer responsible to the chief of mission (ambassador) for security functions of all US embassies and consulates in a given country or group of adjacent countries.
security	1. Measures taken by a military unit, activity, or installation to protect itself against all acts designed to, or which may, impair its effectiveness. 2. A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences. 3. With respect to classified matter, the condition that prevents unauthorized persons from having access to official information that is safeguarded in the interests of national security.
security operations	The integrated application of active and passive offensive and defensive actions taken across the ground dimension of the battlespace, to dominate the base security zone and defeat security threats and performed as part of the integrated base defense. (Source: *AFPD 31-1* and *AFI 31-101*)

tactical combat force (TCF)	A rapidly deployable, air-ground, mobile combat unit with appropriate combat support and combat service support assets assigned to, and capable of, defeating Level III threats, including combined arms.
vehicle-borne improvised explosive device (VBIED)	A device placed or fabricated in an improvised manner on a vehicle incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract.

Appendix B

Recommended Reading List for Air Base Defense and Counterinsurgency

Ian Beckett. *Modern Insurgencies and Counter-Insurgencies: Guerrillas and Their Opponents Since 1750*. London: Routledge, 2001.

Sean Stuart Carwardine. "Defending the Nest: The History and Analysis of Airfield Defence Policy in the Royal Australian Air Force." Thesis, University of New England, Armidale, Australia. https://rune.une.edu.au.

Shannon W. Caudill, ed. *Defending Air Bases in an Age of Insurgency*, vol. I. Maxwell AFB, AL: Air University Press, 2014. https://media.defense.gov.

Shannon W. Caudill, ed. *Defending Air Bases in an Age of Insurgency*, vol. II. Maxwell AFB, AL: Air University Press, 2019. https://www.airuniversity.af.edu.

Anthony M. Coston. "Is U.S. Army Rear Area and Base Security Doctrine Sound for Sustaining Operations on the Noncontiguous Nonlinear Battlefield?" Thesis, School of Advanced Air and Space Studies, Maxwell Air Force Base, Alabama, May 2003. https://www.hsdl.org.

Roger P. Fox. *Air Base Defense in the Republic of Vietnam, 1961–1973*. Washington, DC: Office of Air Force History, United States Air Force, 1979. https://media.defense.gov.

Adam Freedman. *Air Force Protection: An Inconvenient Truth?* Defense Research Paper, Joint Services Command and Staff College, Royal Air Force, July 2019. Copies available by request from author, adam.freedman866@mod.gov.uk.

David Galula. *Counterinsurgency Warfare: Theory and Practice*. Westport, CT: Praeger Security International, 1964.

Benjamin E. Hettinga. *The Defense of Tan Son Nhut, 31 January 1968: A Study in the Nature of Air Base Security*. Dayton, OH: Air Force Institute of Technology, 2002. https://apps.dtic.mil.

Bruce Hoffman. *Insurgency and Counterinsurgency in Iraq*. Santa Monica, CA: RAND, 2004. https://www.rand.org.

David Kilcullen. *The Accidental Guerilla: Fighting Small Wars in the Midst of a Big One*. New York: Oxford University Press, 2009.

M. J. E. MacEachern. *Synchronizing Security Effects on Our Air Bases: Moving from An Ad Hoc Approach to Force Protection*. JSCP 45 Service Paper, Canadian Forces College, 2018. https://www.cfc.forces.gc.ca.

Mao Zedong. *On Guerrilla Warfare*. Translated by Samuel B. Griffith. Mineola, NY: Dover Publications Inc., 2005.

Joseph A. Milner. *Integrated Defense: Lessons Learned from Joint Base Balad*, Air Force Research Institute Paper 2012-3. Maxwell AFB, AL: Air University Press, 2013. https://media.defense.gov.

Nicholas J. Petren. "Expeditionary Air Base Defense: Historical Cases and Modern Implications." Thesis, School of Advanced Air and Space Studies, Maxwell Air Force Base, Alabama, June 2017. https://apps.dtic.mil.

Project CHECO. Southeast Asia Report #51, Special Report: Attack on Cam Ranh—25 August 1971, 15 December 1971, Box 0016, Folder 0463, Sam Johnson Vietnam Archive Collection, Vietnam Center and Sam Johnson Vietnam Archive, Texas Tech University. https://www.vietnam.ttu.edu. Accessed 16 June 2020.

Project CHECO. Southeast Asia Report #222, Special Report: Attack Against Tan Son Nhut, 13 April 1966, 08 July 1966, Box 0002, Folder 0001, Sam Johnson Vietnam Archive Collection, Vietnam Center and Sam Johnson Vietnam Archive, Texas Tech University, https://www.vietnam.ttu.edu. Accessed 16 June 2020.

Thomas Ricks. *The Gamble: General David Petraeus and the American Military Adventure in Iraq, 2006–2008*. New York: Penguin Press, 2009.

David A. Shlapak and Alan J. Vick. "*Check Six Begins on the Ground*": *Responding to the Evolving Ground Threat to US Air Force Bases*. Santa Monica, CA: RAND, 1995. http://www.rand.org.

Alan J. Vick. *Air Base Attacks and Defensive Counters: Historical Lessons and Future Challenges*. Santa Monica, CA: RAND, 2015. http://www.rand.org.

———. *Snakes in the Eagle's Nest: A History of Ground Attacks on Air Bases.* Project Air Force. Santa Monica, CA: RAND, 1995. https://www.rand.org.

Appendix C

Notable Airfield Attacks

1. **Camp Simba, Kenya, 5 January 2020**. Destroyed: 6 (one US Havilland Dash 8, two US helicopters, and one Kenyan Cessna). Damaged: 6 (US contractor-operated civilian aircraft). Killed in action (KIA): 3 (one US Army soldier, 2 US contractor pilots). Wounded in action (WIA): 2. The insurgent group al-Shabaab began an early morning attack by firing mortars as a team infiltrated the base from the thick jungle bordering the base. Using rocket propelled grenades and small arms, insurgents destroyed the US Havilland Dash 8 as it taxied and pressed their attack deep into the camp before being repelled.[1]
2. **Camp Bastion, Afghanistan, 14 September 2012**. Destroyed: 6 aircraft (all US). Damaged: 2 (both US). KIA: 2 (both US). WIA: 9 (Coalition). Fifteen Taliban insurgents launched a five-hour attack on "one of the largest and best-defended posts in Afghanistan."[2]
3. **Pakistan, 23 May 2011**. Destroyed: 2 aircraft (Pakistani Navy P-3 Orions) and one helicopter. Damaged: None. KIA: 18. WIA: 16. Insurgents cut through fencing in an unmonitored area and then attacked the P-3 Orions with rocket-propelled grenades. The attackers then began firing at any observed personnel in the area and continued to move deeper into the installation.[3]
4. **Sri Lanka, 24 July 2001**. Destroyed: 11 (8 military, 3 civilian airliners). Damaged: 14 (11 military, 3 civilian airliners). The terrorist organization the Liberation Tigers of Tamil Eelam (LTTE), also known as the Tamil Tigers, made an audacious attack on the Bandaranaike International Airport and its adjoining Sri Lankan air force base. Using suicide squad tactics, terrorists infiltrated the military runway through storm drains on 24 July 2001. Their attack destroyed or damaged 25 civilian and military aircraft and revealed the weakness of the base's strategic and tactical intelligence collection, analysis, dissemination, and review as well as its force protection.[4]

5. **El Salvador, 7 February 1982**. Destroyed: 14 aircraft. Damaged: 5 aircraft. El Salvador's insurgent forces attacked the El Salvador government's main operating base with 100 guerillas. The operation was "well-planned and executed operation . . . demonstrated the tactical superiority" of the insurgents against the government's base defense force. Strategic effect: The US deepened its commitment to the El Salvadoran government by completely replacing and modernizing the El Salvadoran Air Force.[5]
6. **Muñiz Air National Guard Base, Puerto Rico, 12 January 1981**. Destroyed: 11 (10 A-7D and one F-104). On 12 January 1981, shortly after midnight, eleven terrorists from the Popular Army of Puerto Rico (also known as "The *Macheteros*") infiltrated the base by boat and entered the parking ramp by cutting a hole cut in the perimeter fence. In under eight minutes, the group placed approximately 25 parcels containing four sticks of Iremite with detonators and incendiary charges that were time delayed allowing for escape.[6]
7. **Tan Son Nhut, Vietnam, 1 March 1968**. Destroyed: 7 aircraft (4 US, 3 Republic of Vietnam [RVN]). Damaged: 75 (74 US, 1 RVN). KIA: 9 (all US). WIA: 162 (151 US, 11 RVN). The enemy did all this with only 16 mortar rounds.[7]
8. **Da Nang, Vietnam, 15 July 1967**. Destroyed: 10 aircraft (all US). Damaged: 50 (49 US, 1 RVN), KIA: 8 (all US). WIA: 175 (all US). Notes: The enemy fired a total of 83 mortar rounds.[8]
9. **Tan Son Nhut, Vietnam, 13 April 1966**. Destroyed: 2 aircraft (both RVN). Damaged: 62 (all US), KIA: 9 (7 US, 2 RVN). WIA: 111 (all US). The enemy massed fires with a total of 243 mortar rounds.[9]
10. **Bien Hoa AB, Vietnam, 1 November 1964**. Destroyed: 5 aircraft (all US). Damaged: 22. KIA: 4 (all US). WIA: 72 (all US). Enemy forces launched a midnight mortar attack in which Viet Cong moved to within 440 yards of the base perimeter, staged six 81-millimeter mortars, and fired approximately 80 high-explosive rounds. They were able to depart before any South Vietnamese external response teams could locate them. This attack also had the strategic

effect of galvanizing the Joint Chiefs of Staff in recommending military escalation to President Johnson, which set the US on the path of the prolonged Vietnam conflict.[10]

Notes

1. Gibbons-Neff, Schmitt, Savage, and Cooper, "Chaos as Militants Overran Airfield."
2. Amos, Memorandum for record: Accountability Determination of US Commanders for the 14–15 September 2012 Attack, 3.
3. Atlantic Council, "Karachi Airport Attack Shows Vulnerabilities."
4. Gunaratna, "Intelligence Failures Exposed," 14–17.
5. Corum and Johnson, *Airpower in Small Wars*, 334–35.
6. Thomas, "Armed Puerto Rican Groups Focus Attacks on Military."
7. Fox, *Air Base Defense in the Republic of Vietnam.*
8. Fox.
9. Fox.
10. Fox.

Appendix D

Relevant Quotations about Air Base Defense

"It is easier and more effective to destroy the enemy's aerial power by destroying his nests and eggs on the ground than to hunt his flying birds in the air."[1]

—Italian general Giulio Douhet, 1921

"Every man in Air Force uniform ought to be armed with something—a rifle, a tommy-gun, a pistol, a pike, or a mace; and every one, without exception, should do at least one hour's drill and practice every day. Every airman should have his place in the defence scheme. . . . It must be understood by all ranks that they are expected to fight and die in the defence of their airfields. . . The enormous mass of non-combatant personnel who look after the very few heroic pilots, who alone in ordinary circumstances do all the fighting, is an inherent difficulty in the organization of the Air Force. . . . Every airfield should be a stronghold of fighting air-groundmen, and not the abode of uniformed civilians in the prime of life protected by detachments of soldiers."[2]

—Sir Winston Churchill, British prime minister, 1941

"In developing this expeditionary force culture, force protection is a key issue. The traditional mindset that has developed over the years is an inside-the-fence mentality about force protection. This inside-the-fence mentality said it was the Air Force's business to watch inside the fence—it was up to us to coordinate with or depend on others for whatever was to happen outside the fence. We had joint agreements that said the Army would watch us outside the wire, and that they would help train our people to have the capability inside the wire. But these agreements, as it turns out, were only valid during times

of declared war. It has become apparent that we are going to have to take on some of this capability ourselves."[3]

—Gen John P. Jumper, USAF, commander, United States Air Forces in Europe, and later USAF chief of staff, 1998

"After we stood up 50 expeditionary bases in [Southwest Asia] and after we've had attacks on the bases, after we have had rockets and mortar attacks on the bases, after we've had aircraft hit on arrival and departure with surface-to-air missiles and small-arms fire, and after we've looked at what does it take to secure an airfield in an expeditionary sense, this security force business takes on a whole different light."[4]

—Gen T. Michael Moseley, chief of staff, USA, 2006

"The senior Airman at any location has got to be equipped to lead the base defense. We also need Defense Force Commanders who know their business and can effectively shape the perspectives of the senior Airman on scene to ensure an effective defense."[5]

—Maj Gen Thomas H. Deale, USAF, Retired, former wing commander, Operation Enduring Freedom, 2014

"We could improve senior leader training in regards to base defense. There isn't anything in the predeployment training that I received that specifically prepared me for my responsibilities in base defense. Having experience helps a lot, and I credit my time as a wing commander in Korea as essential. You have to have some basic knowledge of how things work. You get that through personal experiences accumulated over the course of a career. One thing we must do is continue the left seat and right seat exchanges of information and orientation prior to deployment and change of command. In combat, you do not have time for on-the-job training. You may be attacked at any moment and as such, you must be ready to assume commander responsibilities from day one; your Airmen rightly expect that from their leaders."[6]

—Maj Gen Thomas H. Deale, USAF, Retired, former wing commander, Operation Enduring Freedom, 2014

The commanding general "did not adequately assess the force protection situation at Bastion Airfield and failed to devote the resources to actively participate in a layered, integrated, defense-in-depth force protection plan. He and his staff unreasonably minimized the force protection threats which, in turn, exposed his command to unnecessary risk."[7]

—Gen James Amos, USMC, commandant of the Marine Corps

"We must not ignore the ultimate truth about the Khobar Towers tragedy: a determined and resourceful adversary, armed with a massive amount of explosives and given a setting that made surveillance easy and defense challenging, exploited one of the few, but patent, vulnerabilities of a highly fortified compound. In the period leading up to the attack, the compound's force protection posture was significantly enhanced. Nevertheless, vulnerabilities that had been identified in the months before the attack remained exposed at the time the terrorists acted. The commander, who had been made aware of these vulnerabilities, failed to take actions within his authority to address them."[8]

—William Cohen, Secretary of Defense

"U.S. forces in Vietnam are disposed in large fixed installations which always provide our forces with lucrative targets. Our forces are always certain that as long as the weapons hit the installation, the U.S. forces will lose equipment and manpower. Likewise, these large posts do not have sufficient forces to control the surrounding countryside, which makes our attacks easier."[9]

—North Vietnamese Army rocket company commander, 1968

"Whatever else you do, keep the initiative. In counterinsurgency, the initiative is everything. If the enemy is reacting to you, you control the environment. Provided you mobilize the population, you will win. If you are reacting to the enemy—even if you are killing or capturing him in large numbers—then he is controlling the environment and you will eventually lose. In counterinsurgency, the enemy initiates most attacks, targets you unexpectedly and withdraws too fast for you to react. Do

not be drawn into purely reactive operations: focus on the population, build your own solution, further your game plan and fight the enemy only when he gets in the way. This gains and keeps the initiative."[10]

—Dr. David J. Kilcullen, counterinsurgency expert and author, reserve lieutenant colonel, Australian Army

"Defending air assets on the ground in the midst of an insurgency has been a challenge over the course of history. One need only look at the Americans in Vietnam and the Russians in Afghanistan to see how airpower can be tested when its aircraft and people are sufficiently threatened in the performance of their mission. Sound air base defense (ABD) begins with ensuring that airpower leaders understand counterinsurgency (COIN) theory and how it applies to securing the terrain affecting air operations."[11]

—Dr. William T. Dean III, counterinsurgency expert and Air Command and Staff faculty

Notes

1. Douhet, *The Command of the Air*, 53–54.
2. Churchill, *The Second World War*, vol. 3, *The Grand Alliance*, 692–93.
3. Jumper, "Expeditionary Air Force: A New Culture for a New Century."
4. Grant, "The Security Forces Rewrite."
5. Then–Brig Gen Thomas H. Deale, vice commander, Carl A. Spaatz Center for Officer Education, interview with Col Shannon W. Caudill, 17 January 2014. Deale retired as a major general.
6. Deale, interview.
7. Amos, Memorandum for record, Accountability Determination of US Commanders for the 14–15 September 2012 Attack.
8. Cohen, *Personal Accountability for Force Protection at Khobar Towers*, 18.
9. Hay, *Vietnam Studies, Tactical and Materiel Innovations*, 149.
10. Kilcullen, "Twenty-Eight Articles," 11.
11. Dean, afterword to *Defending Air Bases in an Age of Insurgency*, vol. 1, 367.

Abbreviations

AFOSI	Air Force Office of Special Investigations
ARVN	Army of the Republic of Vietnam
BLS	Bastion, Leatherneck, and Shorabak
BSO	battlespace owner
BSZ	base security zone
CAOC	combined air operations center
CCIR	commander's critical information requirement
CIA	Central Intelligence Agency
COA	course of action
COIN	counterinsurgency
C-RAM	counter-rocket, artillery, mortar
DFC	defense force commander
EOC	emergency operations center
ESFS	Expeditionary Security Forces Squadron
FAS	Federation of American Scientists
FBI	Federal Bureau of Investigations
HUMINT	human intelligence
ID	integrated defense
IDF	indirect fire
IDP	integrated defense plan
IDRMP	integrated defense risk management process
ISAF	International Security Assistance Force
ISIS	Islamic State of Iraq and Syria
ISR	intelligence, surveillance, and reconnaissance
JBB	Joint Base Balad
JDOC	joint base defense operations center
JISE	joint intelligence support element
JSTARS	Joint Surveillance Target Attack Radar System
JTAC	joint terminal attack controller
JTTF	joint terrorism task force

LTTE	Liberation Tigers of Tamil Eelam
MWD	military working dog
NATO	North Atlantic Treaty Organization
NVA	North Vietnamese Army
OODA	observe-orient-decide-act
RAM	random antiterrorism measures
RPV	remotely piloted vehicles
SAM	surface-to-air missile
SF	security forces
UAV	unmanned aerial vehicles
VBIED	vehicle-borne improvised explosive device

Bibliography

Amos, Gen James F. Commandant of the Marine Corps. Memorandum for record. Subject: Accountability Determination of US Commanders for the 14–15 September 2012 Attack on the Camp Bastion, Leatherneck, and Shorabak (BLS) Complex, Helmand Province, Afghanistan. 30 September 2013. https://www.hqmc.marines.mil/.

"An Airman's Revenge: 5 Minutes of Terror." *New York Times*, 22 June 1994. http://www.nytimes.com/.

Associated Press. "Homeland Security Leaders Defend Memo on Veterans." *USA Today*, 19 April 2009. http://usatoday30.usatoday.com/.

———. "Israel: Iranian Troops Helping Hezbollah Attack." NBC News, 16 July 2006. http://www.nbcnews.com/.

Atlantic Council. "Karachi Airport Attack Shows Vulnerabilities in Pakistan's Anti-Terror Strategy." 9 June 2014, https://www.atlanticcouncil.org.

BBC. "Anders Breivik Describes Norway Island Massacre." BBC.co.uk, 20 April 2012. http://www.bbc.co.uk/.

Beckett, Ian. *Modern Insurgencies and Counter-Insurgencies: Guerrillas and Their Opponents Since 1750*. London: Routledge, 2001.

Berger, J. M., and Jonathon Morgan. *The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter*. The Brookings Project on U.S. Relations with the Islamic World, Analysis Paper no. 20, March 2015, https://www.brookings.edu.

British Parliament, House of Commons Defence Committee. *Afghanistan—Camp Bastion Attack*. Vol. 2, *Oral and Written Evidence*. Thirteenth Report of Session 2013–2014. HC 830. London: The Stationery Office Limited, 16 April 2004. https://publications.parliament.uk/.

Boyd, John R. "Destruction and Creation." In *A Discourse on Winning and Losing*, 315–325. Edited by Dr. Grant T. Hammond. Maxwell AFB, AL: Air University Press, March 2018. https://www.airuniversity.af.edu/.

Buonaugurio, Michael P. "Air Base Defense in the 21st Century: USAF Security Forces Protecting the Look of the Joint Vision." Master's thesis, USMC Command and Staff College, Quantico, 2011. http://www.dtic.mil/.

Canadian Broadcasting Corporation. "Terrorist Groups Recruiting through Social Media." *CBC News*, 10 January 2012. http://www.cbc.ca/.

Carwardine, Sean Stuart. "Defending the Nest: The History and Analysis of Airfield Defence Policy in the Royal Australian Air Force." Thesis, University of New England, Armidale, Australia. https://rune.une.edu.au.

Caudill, Shannon W., ed. *Defending Air Bases in an Age of Insurgency*, vol. I. Maxwell AFB, AL: Air University Press, 2014. https://media.defense.gov.

———. *Defending Air Bases in an Age of Insurgency*, vol. II. Maxwell AFB, AL: Air University Press, 2019. https://www.airuniversity.af.edu.

Chorn, Adrien, and Monica Michiko Sato. "Maritime Gray Zone Tactics: The Argument for Reviewing the 1951 U.S.–Philippines Mutual Defense Treaty." *New Perspectives in Foreign Policy* 18 (Summer 2019): 3–9. https://www.csis.org.

Christopherson, Todd. "Soldiers Fire First Precision-Guided Mortar in Afghanistan." *US Army Homepage*, 7 April 2011. http://www.army.mil/.

Churchill, Winston S. *The Second World War.* Vol. 3, *The Grand Alliance*. Boston, MA: Houghton Mifflin, 1985.

Cohen, William. *Personal Accountability for Force Protection at Khobar Towers*. 31 July 1997. https://www.hsdl.org/.

Constable, Pamela. "U.S. Military Scales Back Contacts with Afghans After 'Insider' Shootings." *Washington Post*, 24 October 2018. https://www.washingtonpost.com/.

Corbett, Sara. "Can the Cellphone Help End Global Poverty?" *New York Times*, 13 April 2008. https://www.nytimes.com/.

Corum, James S., and Wray R. Johnson. *Airpower in Small Wars: Fighting Insurgents and Terrorists.* Lawrence: University Press of Kansas, 2003.

Coston, Anthony M. "Is U.S. Army Rear Area and Base Security Doctrine Sound for Sustaining Operations on the Noncontiguous Nonlinear Battlefield?" Thesis, School of Advanced Air and Space Studies, Maxwell Air Force Base, Alabama, May 2003. https://www.hsdl.org.

Dahl, Kenneth R. "Summary Report of Det 3, 732 ESFS, Mission Accomplishments," Baghdad, Iraq, memorandum, 2 August 2006.

Dazio, Stefanie. "Airman Charged with Murder of Federal Officer at Courthouse." ABC News, 16 June 2020. https://abcnews.go.com/.

Dean, William, III. Afterword to *Defending Air Bases in an Age of Insurgency*, vol. I. Edited by Shannon Caudill. Maxwell AFB, AL: Air University Press, 2014. https://www.airuniversity.af.edu/.

Delgado, Alex. "CSAF Charts Air Force Defender Way Forward in Year of Integrated Base Defense." US Air Force, 2 October 2019. https://www.af.mil/.

Deliso, Meredith. "Timeline: The Impact of George Floyd's Death in Minneapolis and Beyond." *ABC News*, 10 June 2020. https://abcnews.go.com/.

Director of Central Intelligence. *Warsaw Pact Nonnuclear Threat to NATO Airbases in Central Europe: National Intelligence Estimate*. NIE 11/20-6-84. Washington, DC: Central Intelligence Agency, 25 October 1984. https://www.cia.gov/.

Douhet, Giulio. *The Command of the Air*. Translated by Dino Ferrari. With a new introduction by Joseph P. Harahan and Richard H. Kohn. Tuscaloosa, AL: University of Alabama Press, 2009.

Dreisbach, Tom, and Meg Anderson. "Nearly 1 in 5 Defendants in Capitol Riot Cases Served in the Military," *All Things Considered*, National Public Radio, 21 January 2021. https://www.npr.org.

Elliott, David W. P., and Mai Elliott. *Documents of an Elite Viet Cong Delta Unit: The Demolition Platoon of the 514th Battalion—Part 1: Unit Composition and Personnel*. Santa Monica, CA: RAND Corporation, May 1969. http://www.rand.org/.

Esler, Dave. "What a Business Aviation Flight Department Needs to Know About UAS." *Aviation Week*, 25 September 2015. http://aviationweek.com/.

Everstine, Brian. "AFRICOM: U.S. Forces Were Not Prepared for Manda Bay Attack." *Air Force Magazine*, 30 January 2020. https://www.airforcemag.com.

Federal Bureau of Investigation. "Massachusetts Man Charged with Plotting Attack on Pentagon and US Capitol and Attempting to Provide Material Support to a Foreign Terrorist Organization." Press release, 28 September 2011. https://archives.fbi.gov/.

Federation of American Scientists. "About FAS." FAS.org. Accessed 29 January 2013. https://fas.org/about-fas/.

Fox, Roger P. *Air Base Defense in the Republic of Vietnam, 1961–1973*. Washington, DC: Office of Air Force History, 1979.

Freedman, Adam. *Air Force Protection: An Inconvenient Truth?* Defense Research Paper, Joint Services Command and Staff College, Royal Air Force, July 2019. Copies available by request from author, adam.freedman866@mod.gov.uk.

Galula, David. *Counterinsurgency Warfare: Theory and Practice*. Westport, CT: Praeger Security International, 1964.

Garrett, LTG William B., III, US Army, Investigating Officer, and Maj Gen Thomas M. Murray, US Marine Corps, Deputy Investigating Officer. To Commander, US Central Command. Enclosure 3, Executive Summary of the Army Regulation (AR) 15-6 Investigation of the 14–15 September 2012 Attack on Camp Bastion, Leatherneck, and Shorabak (BLS) Complex, Helmand Province, Afghanistan, 1 October 2013. https://www.hqmc.marines.mil/.

Gibbons-Neff, Thomas, Eric Schmitt, Charlie Savage, and Helene Cooper. "Chaos as Militants Overran Airfield, Killing 3 Americans in Kenya." *New York Times*, 22 January 2020. https://www.nytimes.com.

Global Security. "Company History." GlobalSecurity.org. Accessed 13 March 2013. http://www.globalsecurity.org/.

Grant, Rebecca. "The Security Forces Rewrite." *Air Force Magazine* 89, no. 1 (1 January 2006). https://www.airforcemag.com/.

Gunaratna, Rohan. "Intelligence Failures Exposed by Tamil Tiger Airport Attack." *Jane's Intelligence Review* 13, no. 9 (September 2011): 14–17. http://www.island.lk/.

Halliday, Josh. "David Cameron Considers Banning Suspected Rioters from Social Media." *The Guardian*, 11 August 2011. https://www.theguardian.com/.

Handcocks, Paula. "ISIS Threat to US Air Bases, South Korea Intelligence Agency Warns." CNN, 20 June 2016. http://www.cnn.com/.

Hay, John H., Jr. *Vietnam Studies, Tactical and Materiel Innovations*. Washington, DC: Department of the Army, 1974. https://history.army.mil/.

Helmer, Daniel. "Hezbollah's Employment of Suicide Bombing During the 1980s: The Theological, Political, and Operational Development of a New Tactic." *Military Review*, July–August 2006. https://www.armyupress.army.mil/.

Hettinga, Benjamin E. *The Defense of Tan Son Nhut, 31 January 1968: A Study in the Nature of Air Base Security*. Dayton, OH: Air Force Institute of Technology, 2002. https://apps.dtic.mil.

Hoffman, Bruce. *Insurgency and Counterinsurgency in Iraq*. Santa Monica, CA: RAND, 2004. https://www.rand.org.

Hossain, Md Sazzad. "Social Media and Terrorism: Threats and Challenges to the Modern Era." *South Asian Survey* 22, no. 2 (2018): 136–55. https://doi.org/fmw4.

Johnson, M. Alex, and Pete Williams. "Cops: Weeks of Planning Went into Shootings at Colo. Batman Screening." NBCNews.com, 20 July 2012. http://usnews.nbcnews.com/.

Joint Chiefs of Staff. *DOD Dictionary of Military and Associated Terms*. June 2020. https://www.jcs.mil.

———. *Joint Publication 3-13.4, Military Deception*. 26 January 2012. http://jfsc.ndu.edu/.

Jumper, John P. "Expeditionary Air Force: A New Culture for a New Century." Transcript. Air Force Association Symposium, Orlando, FL, 26 February 1998.

Kilcullen, David J. *The Accidental Guerilla: Fighting Small Wars in the Midst of a Big One*. New York: Oxford University Press, 2009.

———. "Twenty-eight Articles: Fundamentals of Company-level Counterinsurgency." *Small Wars Journal* 1 (March 2006). https://smallwarsjournal.com/.

Lancefield, Neil. "3,000 Arrests in London Riots Investigation." *Independent*, 7 October 2011. https://www.independent.co.uk/.

Lieberman, Joseph I., and Susan M. Collins. *A Ticking Time Bomb: Counterterrorism Lessons from the U.S. Government's Failure to Prevent the Fort Hood Attack*. Special Report. Washington, DC: US Senate Committee on Homeland Security and Governmental Affairs, February 2011. http://www.hsgac.senate.gov/.

Luck, Gary, and Michael Findlay. "Insights and Best Practices: JTF Level Command Relationships and Joint Force Organization." Focus Paper no. 4. Norfolk, VA: United States Joint Forces Command (November 2007). https://intelshare.intelink.gov/.

MacEachern, M. J. E. *Synchronizing Security Effects on Our Air Bases: Moving from An Ad Hoc Approach to Force Protection*. JSCP 45 Service Paper, Canadian Forces College, 2018. https://www.cfc.forces.gc.ca.

MacFarquhar, Neil, and Thomas Gibbons-Neff. "Air Force Sergeant with Ties to Extremist Group Charged in Federal Officer's Death." *New York Times*, 16 June 2020. https://www.nytimes.com

Mao Zedong. *On Guerrilla Warfare*. Translated by Samuel B. Griffith. Mineola, NY: Dover Publications Inc., 2005.

Martinez, Luis. "US General Was Wounded in Kandahar Attack." *ABC News*, 21 October 2018. https://abcnews.go.com/.

Miller, Lt Col Kenton. *3rd SPS Ground Defense Lessons Learned*. After action report. Bien Hoa AB, South Vietnam, 1968.

Milner, Joseph A. *Integrated Defense: Lessons Learned from Joint Base Balad*, Air Force Research Institute Paper 2012-3. Maxwell AFB, AL: Air University Press, 2013. https://media.defense.gov.

Montero, David. "Storm Area 51 Creator: 'I Sparked a Movement while I Was Bored at 2 a.m.'" *Los Angeles Times*, 12 September 2019. https://www.latimes.com.

Myers, Lisa. "Hezbollah Drone Threatens Israel." *NBC News*, 12 April 2005. http://www.nbcnews.com/.

Pawlyk, Oriana. "ISIS-linked Hackers Claim to Release Personal Information of US Drone Pilots." *Air Force Times*, 3 May 2016. https://www.airforcetimes.com/.

———. "Questions Remain as Families Mourn Victims of 2011 Green-On-Blue Kabul Attack." *Air Force Times*, 27 April 2016. https://www.airforcetimes.com/.

Petren, Nicholas J. "Expeditionary Air Base Defense: Historical Cases and Modern Implications." Thesis, School of Advanced Air and Space Studies, Maxwell Air Force Base, Alabama, June 2017. https://apps.dtic.mil.

Pifer, Stephen. "Crimea: Six Years After Illegal Annexation." Brookings, 17 March 2020. https://www.brookings.edu.

Project CHECO. Southeast Asia Report #51, Special Report: Attack on Cam Ranh—25 August 1971, 15 December 1971, Box 0016, Folder 0463, Sam Johnson Vietnam Archive Collection, Vietnam Center and Sam Johnson Vietnam Archive, Texas Tech University. https://www.vietnam.ttu.edu. Accessed 16 June 2020.

———. Southeast Asia Report #222, Special Report: Attack Against Tan Son Nhut, 13 April 1966, 08 July 1966, Box 0002, Folder 0001, Sam Johnson Vietnam Archive Collection, Vietnam Center and Sam Johnson Vietnam Archive, Texas Tech University, https://www.vietnam.ttu.edu. Accessed 16 June 2020.

Reuters. "ISIS Booby-trapped Drone Kills Troops in Iraq, Officials Say." *The Guardian*, 12 October 2016. https://www.theguardian.com.

Ricks, Thomas. *The Gamble: General David Petraeus and the American Military Adventure in Iraq, 2006–2008*. New York: Penguin Press, 2009.

Royal Australian Air Force Air Power Development Centre. "What Is Airmindedness?" *Pathfinder: Air Power Development Center Bulletin* 5, no. 151 (March 2011). https://airpower.airforce.gov.au/.

Schmitt, Eric. "Threats and Responses: Skirmish; US Marine is Killed in Kuwait as Gunmen Strike Training Site." *New York Times*, 9 October 2002. https://www.nytimes.com/.

Schwartz, Moshe. *The Department of Defense's Use of Private Security Contractors in Afghanistan and Iraq: Background, Analysis, and Options for Congress*. Congressional Research Service R40835. Washington, DC: Government Printing Office, 13 May 2011. https://crsreports.congress.gov/.

Sciutto, Jim, Catherine E. Shoichet, and Ashley Fantz. "U.S. General Killed in Afghanistan; Gunman Shot from 100 Yards, Officials Say." CNN, 8 August 2014. https://www.cnn.com/.

Shlapak, David A., and Alan J. Vick. *"Check Six Begins on the Ground": Responding to the Evolving Ground Threat to US Air Force Bases*. Santa Monica, CA: RAND, 1995. http://www.rand.org.

Special Inspector General for Iraq Reconstruction. *Quarterly Report to Congress*. Washington, DC: US Departments of Defense and State, 31 July 2006. https://cybercemetery.unt.edu/.

Starr, Barbara. "Shrapnel Hits Joint Chiefs Chairman's Plane at Afghan Base." CNN, 21 August 2012. https://www.cnn.com/.

Starr, Barbara, Chris Lawrence, and Joe Sterling. "ISAF: Insurgents in Deadly Attack in Afghanistan Wore US Army Uniforms." CNN, 15 September 2012. http://www.cnn.com/.

Thomas, Jo. "Armed Puerto Rican Groups Focus Attacks on Military." *New York Times*, 16 January 1981. https://www.nytimes.com.

Tirpak, John A. "Goldfein: USAF Needs 'to Return to Our Expeditionary Roots.'" *Air Force Magazine*, 18 September 2018. https://www.airforcemag.com/.

Tourist Guides of Crete Travel Agency. "Battle of Crete – The Island of the Brave." Accessed 21 May 2016. https://web.archive.org/.

Tunner, William H. *Over the Hump*. New York: Duell, Sloan, and Pearce, 1964.

Ucko, David H. "Lessons from Basra: The Future of British Counterinsurgency." *Survival* 52, no. 4 (21 July 2010): 131–58.

United States of America v. Dritan Duka. In US District Court, District of New Jersey, No. 07-M-2046 (JS). https://www.justice.gov.

US Air Force (USAF). *Air Force Doctrine Document (AFDD) 1: Air Force Basic Doctrine: Organization and Command*. 14 October 2011.

———. *Air Force Doctrine Document (AFDD) 1-1: Leadership and Force Development*. 8 November 2011.
———. *Air Force Doctrine Document (AFDD) 3-2: Irregular Warfare*. 15 March 2013.
———. *Air Force Doctrine Document (AFDD) 3-10: Force Protection*. 28 July 2011.
———. *Air Force Instruction (AFI) 31-101: Integrated Defense (ID)*. 24 March 2020.
———. *Air Force Policy Directive (AFPD) 31-1: Integrated Defense*. 28 October 2011.
US Army. "Army Programs: Counter-Rocket, Artillery, Mortar (C-RAM)." 2006. https://web.archive.org/.
Vick, Alan. *Air Base Attacks and Defensive Counters Historical Lessons and Future Challenges*. Santa Monica, CA: RAND Corporation, 2015. https://www.rand.org/.
———. *Snakes in the Eagle's Next: A History of Ground Attacks on Air Bases*. Santa Monica, CA: RAND Corporation, 1995. http://www.rand.org/.
Warrick, Joby. "Suicide Bomber Attacks CIA Base in Afghanistan, Killing at Least 8 Americans." *Washington Post*, 31 December 2009. https://www.washingtonpost.com/.
Williams, Timothy. "US Soldier Kills 5 of His Comrades in Iraq." *New York Times*, 11 May 2009. https://www.nytimes.com/.
Woods, Baynard, and Madhvi Pankhania. "Baltimore Timeline: The Year Since Freddie Gray's Arrest." *The Guardian*, 27 April 2016. https://www.theguardian.com/.
Woody, Christopher. "Drones Are Dropping Bombs on US Troops in Syria, and It's Not Clear Who's Doing It." *Business Insider*, 11 March 2020. https://www.businessinsider.in.

Index

active base defense, 11
Afghanistan, 3, 11, 15, 17, 18, 24, 32, 33, 35, 43, 44, 48, 49, 51, 63, 70
Air Force Incident Management Course, 8, 38
Air Force National Tactical Integration Cell, 31
Air Force Office of Special Investigations (AFOSI), 3
air support, 21, 31, 33
Army Air Force, 17, 28, 36
Army aviation units, 31
Army of the Republic of Vietnam (ARVN), 27
attack methodology, 39
Australian Air Power Development Centre, *xx*

Bagram Air Base, Afghanistan, 18, 24, 32
Bandaranaike International Airport, Sri Lanka, 27, 63
Barrackpore, India, 36
base familiarization, 39
base security zone (BSZ), 3, 11, 13, 17, 18, 20, 28, 39, 57, 59
Basra, Iraq, 13, 14
battlespace owner (BSO), 11, 13, 17–20, 28, 29
Bien Hoa, Vietnam, 64
Bishop, Brian, 20
black market, 36
Boston, 41, 44
British forces, 13, 14

Camp Bastion, Afghanistan (now called Camp Shorabak), 1, 3, 51, 63
campaign objectives, 17
Capitol riot, 37
Chattanooga, Tennessee, 41
Churchill, Winston, 23, 55, 67
coalition, 1, 7, 17-19, 24, 29, 35, 36, 39, 44, 48, 51, 63
coalition partners, 17, 24
Coast Guard, Philadelphia, 5
Cold War, 40, 51, 52
counterinsurgency (COIN), 13–15, 17, 29, 35, 61, 69, 70
counter-rocket artillery mortar (C-RAM), 20, 21
Crete, 23
crisis action team, 40
cybersecurity, 42

Deale, Thomas H., 15, 19, 24, 32, 51, 68
Decknick, John, 20
Department of State, 17, 18
Dover AFB, Delaware, 5
"Dover Effect," 5, 6, 9

Eagle Eyes program, 29
Emergency Operations Center (EOC), 3, 40
Europe, 13, 68

Failaka Island, Kuwait, 7
Fairchild AFB, Washington, 38
Federal Bureau of Investigations (FBI), 5
Floyd, George, 3
Fort Dix, New Jersey, 5
Fort Hood, Texas, 41, 48
Fort Monmouth, New Jersey, 5
Forward Operating Base Kushamond, Afghanistan, 44
455th Expeditionary Security Forces Squadron (ESFS), 32

Global Hawk, 31
Gray, Freddy, 3
Gulf War, 35

Helmand Province, Afghanistan, 51
host nation, 7, 57, 59

indirect fire (IDF), 18, 20, 28, 29, 31, 43, 44, 47, 49
insurgents, 11, 31, 33, 40, 43, 44, 48, 63
integrated defense (ID), 1, 3, 20, 23, 24, 28, 35, 41, 51, 55, 57–59, 62

integrated defense plan (IDP), 41, 42
intelligence, surveillance, and reconnaissance (ISR), 18
interlocking fields of fire, 3, 40
International Security Assistance Force (ISAF), *xvii*
Iraq, 3, 11, 13, 14, 17, 19, 23, 29, 31, 33, 35–37, 43–45, 49, 61, 62
ISIS, 37, 45
Islamic state, 37, 46
Italy, 19

Joint Base Balad (JBB), 17, 19, 20, 27–29, 31, 36, 40, 44, 62
joint defense operations center (JDOC), 19
joint intelligence support element (JISE), 17
joint personnel, 23, 24
Joint Surveillance Target Attack Radar System (JSTARS), 31
joint terminal attack controller (JTAC), 21, 31
Joint Terrorism Task Forces (JTTF), 7

key terrain, 13, 40
Kilcullen, David, 14, 62, 70

Lakehurst Naval Air Station, New Jersey, 5
law enforcement, 3, 7, 13, 15, 29, 35-37, 39, 46–49, 59
lessons, 17, 29, 56, 62
Liberation Tigers of Tamil Eelam (LTTE), 27, 63
Little Rock, Arkansas, 41

maintenance operations center, 40
McDonnell Douglas AV-8B Harrier II, *xvii*
McGuire Air Force Base, New Jersey, 5–6
Mellberg, Dean A., 37
Miller, Kenton, 27
Mission Support and Operations Group, 32
mortar, 20, 44, 64, 68

Naval Station Philadelphia, 5
North Atlantic Treaty Organization (NATO), *xvii*, 37, 48, 51, 52
North Vietnamese Army (NVA), 27
Office of Air Force History, 27, 61
OH-58 observation helicopters, 32
101st Airborne, 27
Operation Enduring Freedom (OEF), 35, 68
Operation Iraqi Freedom (OIF), 13, 35
organizational climate, 3
outside the wire, 11, 21, 33, 35, 67

Persian Gulf, 7
persistent threat detection system, 32
Port of Philadelphia, 5

RAND Corporation, *xix*
random antiterrorism measures (RAM), 7
Raven-B, 32
Republic of South Vietnam, 19
risk management process, *xix*, 42
rocket-propelled grenade launcher, *xvii*
Romania, 19
Royal Air Force, 23, 61

San Bernardino, California, 37
security forces (SF), *xx*
shoulder-fired missiles, 43
suicide squad tactics, 27, 63
surface-to-air missile (SAM), 11, 32, 68
synchronization, 17–19, 32, 33

Tallil Air Base, Iraq, 19
Tamil Tigers, 27, 63
Tan Son Nhut Air Base, Republic of South Vietnam, 19
Task Force 1/455, 18
Tatar, Serdar, 6
terrorism, 7, 8, 42, 44, 46; domestic, 7, 42; gang activity, 42; homegrown, 5, 42; violent extremists, 42
Tet Offensive, 19, 27
3rd Security Police Squadron, 27
332nd Air Expeditionary Wing, 20, 27, 29
Tunner, William, 36

unmanned aerial vehicle (UAV), 11, 32; Predator, 32; Scan Eagle, 32
US Joint Forces Command, 18

Vietcong, *xviii*
Vietnam, 19, 27, 31, 43, 44, 49, 61, 62, 64, 69, 70
wing operations center, 40
World War II, 23, 36

How does an Airman define a fighting position? For a Soldier or Marine it's most likely a firebase. For a Sailor it's a ship. And for an Airman it's an air base. Our proficiency and commitment to defending our fighting positions should be no less than the Soldier, Sailor, or Marine. The people of the United States celebrate their Air Force because it relentlessly delivers kinetic effects to the nation's enemies, through a continuous evolution of stealth, standoff, and precision. The security of bases necessary to deliver these effects must be a core competency of our Air Force. Air-minded commanders who understand the extended security perimeter of an air base, the logistics of weapons, fuel, and 24/7 sortie generation must be trained with the heart and spirit of the Battlefield Airman. Read this book to understand what that means.

— Gen John P. Jumper, USAF, Retired, 17th Chief of Staff, United States Air Force

Defending Air Bases in an Age of Insurgency: Integrated Base Defense Principles for Commanders *is the final volume of the Air University Press trilogy on air base ground defense. The first two volumes present a uniquely comprehensive assessment of integrated base defense combat lessons learned and evolving requirements. Thus, volumes I and II were directed primarily at an audience comprised of professional air base defenders, analysts, and scholars. Volume III perfectly complements the first two volumes, offering 10 principles for base commanders who typically will not have Security Forces backgrounds. The 10 principles are crisp and pithy but also well-grounded in history, offering practical advice that all base commanders would be wise to heed. The three volumes in this set are an invaluable resource and belong on the bookshelves of every air base defender, base commander, and airpower analyst.*

— Dr. Alan Vick, senior political scientist, RAND Corporation, author of *Snakes in the Eagle's Nest: A History of Ground Attacks on Air Bases* and *Air Base Attacks and Defensive Counters: Historical Lessons and Future Challenges*

This is an essential guide for every commander on an air base who must protect Air Force assets in order to project airpower anytime and anyplace. Effective execution of mission command, agility, and a well-led, well-trained defense force will carry the day.

— Lt Gen Brad Webb, USAF, commander, Air Education & Training Command

---

Col Shannon W. Caudill, USAF, retired (BS, Norwich University; MSA, Central Michigan University; MMS, Marine Corps Command and Staff College; MSS, Air War College; George Walker Executive Leadership Fellow, University of Charleston, West Virginia) is a doctoral candidate at the University of Charleston, an adjunct professor of leadership at Air Command and Staff College and the University of Charleston, founder of Home Plate Consulting and Writing Services, LLC, and owner of the online book sale business Baseball in Georgia. As a career Air Force security forces officer, he has worked at the unit, major command, and Joint Staff levels; commanded three security forces squadrons; and accumulated 18 months of combat experience in Iraq. He has written numerous white papers and articles on terrorism, leadership, base defense, and law enforcement that have been published in *Air and Space Power Journal*, *Joint Force Quarterly*, *American Diplomacy*, and the *Guardian*—the Joint Staff's antiterrorism publication. He is the editor and coauthor of the Air University Press's three-volume monograph series, *Defending Air Bases in an Age of Insurgency*. In addition, he is coauthor of the history book *Baseball in Kennesaw*. As an educator, he has served on the resident and adjunct faculty of Air War College, Air Command and Staff College, Lake Region State College, North Dakota, and the University of Charleston, West Virginia.

AIR UNIVERSITY PRESS

9 781585 662418