NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

DO GOOD FENCES STILL MAKE GOOD NEIGHBORS?—INTEGRATING FORCE PROTECTION WITH HOMELAND SECURITY ON ARMY INSTALLATIONS

by

David S. Burdick

March 2009

Thesis Advisor:	Paul Stockton
Second Reader:	Chris Bellavita

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2009	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Do Good Fences Still Make Good Neighbors?—Integrating Force Protection with Homeland Security on Army Installations		**5. FUNDING NUMBERS**	
6. AUTHOR(S) David S. Burdick			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

Army installations have been uniquely affected by the Global War on Terrorism (GWOT) and homeland security initiatives as a result of the attacks on September 11, 2001. Unfortunately, most have not done enough in coordinating and integrating their antiterrorism plans with the crisis response and consequence management plans of their adjacent civilian municipalities. This thesis argues that fences and guards are not enough to protect Army installations against terrorist attack, or against any other natural or man-made disaster, nor do installations have the wherewithal to respond effectively on their own should disaster strike. Doctrine is clear, and regulations and policy have been published guiding the Army (and other military services) in providing Civil Support to state and local authorities during times of crisis; but what is less clear, or more precisely, non-existent, is the doctrine regarding how Army installations would receive and integrate support *from* local and state officials in response to disasters occurring on the installation. Now more than ever, Army installations require municipal support to effectively respond to terrorist attacks, natural disasters, and accidents. Indeed, Army installations must reach across their perimeter fences and embrace municipal partners in integrating force protection with homeland security.

14. SUBJECT TERMS Homeland Security, Homeland Defense, Force Protection, Antiterrorism, Civil Support, Emergency Management, Installation Management, Army Installations			**15. NUMBER OF PAGES** 107
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

DO GOOD FENCES STILL MAKE GOOD NEIGHBORS?—INTEGRATING FORCE PROTECTION WITH HOMELAND SECURITY ON ARMY INSTALLATIONS

David S. Burdick
Professor/Program Manager, Army Management Staff College
B.A., Brigham Young University, 1986

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND DEFENSE AND SECURITY)**

from the

**NAVAL POSTGRADUATE SCHOOL
March 2009**

Author: David S. Burdick

Approved by: Paul Stockton
Thesis Advisor

Chris Bellavita
Second Reader

Harold A. Trinkunas, PhD
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Army installations have been uniquely affected by the Global War on Terrorism (GWOT) and homeland security initiatives as a result of the attacks on September 11, 2001. Unfortunately, most have not done enough in coordinating and integrating their antiterrorism plans with the crisis response and consequence management plans of their adjacent civilian municipalities. This thesis argues that fences and guards are not enough to protect Army installations against terrorist attack, or against any other natural or man-made disaster, nor do installations have the wherewithal to respond effectively on their own should disaster strike. Doctrine is clear, and regulations and policy have been published guiding the Army (and other military services) in providing Civil Support to state and local authorities during times of crisis; but what is less clear, or more precisely, non-existent, is the doctrine regarding how Army installations would receive and integrate support from local and state officials in response to disasters occurring on the installation. Now more than ever, Army installations require municipal support to effectively respond to terrorist attacks, natural disasters, and accidents. Indeed, Army installations must reach across their perimeter fences and embrace municipal partners in integrating force protection with homeland security.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I count myself most fortunate to have been accepted by the Naval Postgraduate School and the Department of Homeland Security into this prestigious program of study—the first of its kind in the nation that brought together federal, state, and local first responders, emergency planners and managers, and other associated homeland defense and security officials to learn from each other, to develop and add to a body of knowledge that is expanding exponentially, and to form a network of personal and professional contacts that will ensure greater cooperation and ultimate success in facing the challenges of terrorist threats and other catastrophic disasters in the post-9/11 world. Thank you, Dr. Paul Stockton, founding Director of the Center for Homeland Defense and Security at the Naval Postgraduate School, for your wisdom, foresight, and dedication in bringing this program into being and establishing the proper climate to ensure our success, both academically and professionally.

I would not have arrived at this point were it not for the encouragement and continued support of Mr. Patrick Cathcart, Director of the Command Programs Department at the Army Management Staff College (AMSC), my boss, mentor, and friend. Thanks for giving me the opportunity not once, but twice, to work for you as part of a great team that is doing great things for Army installations and their leaders. Thanks also to Dr. Ursula Lohman, former Dean of Academics at AMSC, for her endorsement of my application to the program, and for establishing and maintaining a work climate that encourages continuing education and professional development, one that is still supported by our current commandant, Colonel Garland H. Williams. I also want to thank my colleagues in the Command Programs Department, our contract partners from Team IFPEX, and my colleagues at the Installation Management Command headquarters, its region offices, and its 100-plus installations worldwide who have, often unknowingly, shared a thought or idea that contributed in some way to this thesis, or to other papers written to fulfill requirements of this program.

The faculty and staff at the Naval Postgraduate School are the best of the best. Particular thanks go to Dr. Stockton and to Dr. Chris Bellavita for their advice and patience with me as I endeavored to complete this work, as well as to all the faculty and guest lecturers that provided wonderful insight into their particular areas of expertise, contributing to our education and understanding by taking us behind the scenes—not afraid to show us how the sausage is made. Thanks also to Heather Issvoran and the entire administrative staff that stood behind us, put up with our complaints, and shared in our successes. Special thanks also go to Greta Marlatt, the human backbone of the Homeland Security Digital Library. What she has created and expanded is nothing short of miraculous, and it continues to help me beyond this degree program in my day-to-day work at the Army Management Staff College.

I appreciate so much the friendships and professional relationships that developed among our class—Cohorts 0302 and 0303. I learned from each of you and thank you for your support and encouragement throughout the entire program. You are all true professionals and patriots whose collective purpose is enhancing the continued security of our nation and its citizens. I am confident that wherever you are serving, you're contributing in a significant way because of your participation in this program. I would be humbled and honored to serve with any of you.

Finally, I would not have been able to complete this program, including this thesis, without the support of a loving wife and family. Thanks Fiona, for your encouragement and faith in me when I first applied to this program, and for your continued support while I completed the coursework and thesis requirements. Thanks also to my wonderful kids, Scott and Regan, for your love and support, for your patience with me when I had to be away, and for your desire to always "do good and be good."

I. INTRODUCTION

A. BACKGROUND AND OBJECTIVES

Army installations have been uniquely affected by the Global War on Terrorism (GWOT) and homeland security initiatives as a result of the attacks on September 11, 2001. Unfortunately, most have not done enough in coordinating and integrating their antiterrorism and force protection plans with the crisis response and consequence management plans of their adjacent civilian municipalities. Army installations can no longer view themselves as island fortresses with respect to force protection. It is time to fill in the moat of misperception and gaps in communication separating Army installations from civilian municipalities. Now more than ever, Army installations require municipal support to effectively respond to terrorist attacks, natural disasters, and accidents. Indeed, Army installations must reach across their perimeter fences and embrace municipal partners in integrating force protection with homeland security.

For the past several years, the U.S. Army has made a concerted effort to *re-secure* its installations against a variety of threats, ranging from an overly inquisitive public to surprise terrorist attacks. The term "re-secure" is used intentionally, because for some time in our nation's past, Army installations were fortresses of a sort—heavily guarded and patrolled—with access granted only to those working within, plus their families (if they resided in post housing), as well as to those visitors pre-approved by the installation commanders. Following the advent of the post-Vietnam, all-volunteer force, the Army opened most of its installations (especially those within the continental U.S.) to the public. This effort at exposing typical Army life to average Americans was a great public relations initiative and a boon to recruiting. However, over the past quarter-century military commanders have been tragically reminded of their force protection responsibilities, beginning with the truck bombing of the U.S. Marine Corps contingent at the Beirut, Lebanon airport in 1983. The attack against the

U.S. Air Force at Khobar Towers in 1996, the attack against the U.S. Marine guards (and many civilians) at the two U.S. Embassies in Africa in 1998, and the attack against the USS Cole suffered by the U.S. Navy in 2000, are more recent reminders that resulted in a renewed military emphasis on force protection.

After the 9/11 terrorist attacks, which united Americans for the first time since World War II in an all out effort against a global threat, federal, state, and municipal officials throughout the country began embracing the notion of homeland security. The Defense Department launched GWOT, with retaliatory attacks against al Qaeda and the Taliban in Afghanistan, and the war of liberation in Iraq; while back home, the creation of both the Department of Homeland Security and the Department of Defense's Northern Command (NORTHCOM) have had far reaching implications for federal, state, and municipal officials charged with defending the homeland.

B. REVIEW OF RELEVANT LITERATURE

This thesis is offered as a catalyst, provoking others to contribute to an emerging body of knowledge on *municipal support to military installations*—more specifically, how support from local municipalities enhances the ability of Army installations to deter and defend against attacks, and to respond effectively should they occur. The literature available on the subject of Army installations and homeland security is focused on the reverse situation—defense support of civil authorities. Most of these sources are military publications, RAND Corporation publications, or General Accounting Office (GAO) reports.

C. HYPOTHESIS/POLICY OPTIONS

Over the past quarter century, the Army's installation force protection program has focused almost exclusively on antiterrorism—actions necessary to prevent or deter a terrorist attack, primarily emphasizing the physical security of installations and facilities. Although this suggests that the Army has been proactive in its approach, history shows differently. Army antiterrorism policy and

corresponding programs have, in fact, been driven by reaction to previous attacks, resulting in an inefficient and inconsistent application of resources and personnel amid cycles of complacency (Figure 1).

The 1983 attack on the U.S. Marine Corps Headquarters in Beirut, hastened the publication of Army Regulation (AR) 190-52, Terrorism Counteraction, a regulation oriented on the law enforcement aspects of responding to terrorist attacks (e.g., hostage negotiations and special reaction team operations). In three short years, with no intervening attacks against military targets, complacency set in. A 1986 Department of the Army Inspector General (DAIG) inspection led to increased antiterrorism emphasis, and revision of the regulation. The 1988 version, AR 525-13, Combating Terrorism, refocused the Army's energy toward deterring and preventing terrorist attacks, rather than reacting to them after they occur. Again, complacency struck and another DAIG inspection in 1990 was followed by another regulation revision in 1992.

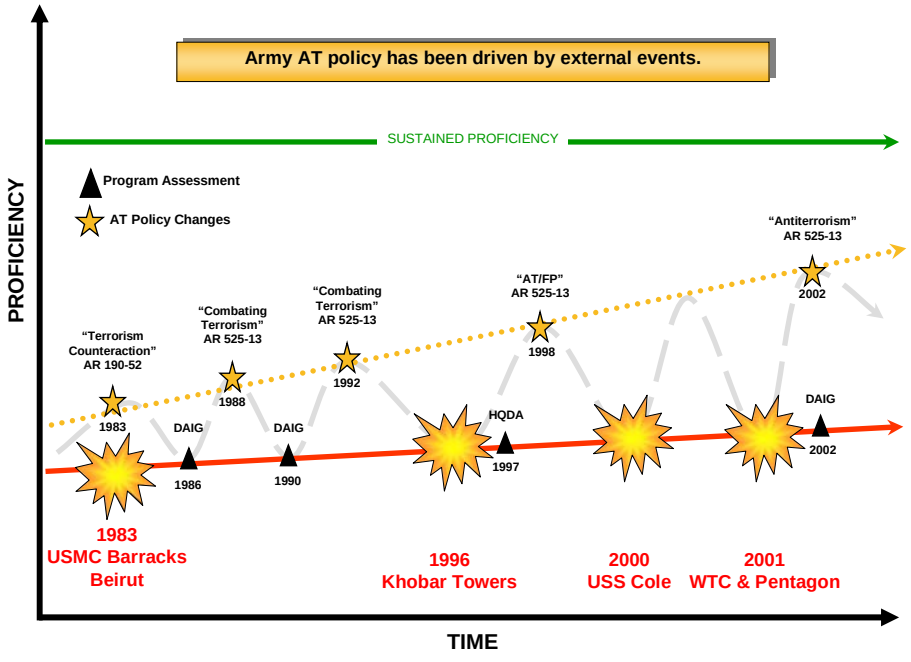

Figure 1. History of the U.S. Army Antiterrorism Program[1]

[1] Craig Benedict, "Army Antiterrorism Program Status," unpublished briefing from HQ, Department of the Army, G-3/5/7 (DAMO-ODL), presented at the Garrison Pre-command Course, Army Management Staff College, Fort Belvoir, VA, August 5, 2004, slide 16.

The Downing Commission Report following the 1996 Khobar Towers attack was critical of many aspects of the military's combating terrorism program. Among other things, this report recommended more command emphasis on antiterrorism, which it described as a "focus on offensive and defensive means to preempt, deter, or thwart terrorist attacks on U.S. servicemen and women, their families, and facilities and mitigate damage when attacks succeed."[2] A follow-on assessment of its own combating terrorism program by Headquarters, Department of the Army (HQDA) led to another revision of AR 525-13, including renaming it Antiterrorism/Force Protection. This version of the regulation introduced the AT/FP acronym which led to confusion in terminology that still exists to this day.

There are several problems with the Army's approach to installation force protection over the last 25 years. First, as demonstrated in the preceding paragraphs, the Army has struggled with terminology. What is force protection? What is antiterrorism? Secondly, the Army's emphasis within antiterrorism has been on only two of its four aspects: prevention and deterrence. Hundreds of millions of dollars have been spent annually on fences, lighting, surveillance cameras, security guards, and other access control barriers in an effort to make Army installations more secure against possible terrorist attacks. Although well intentioned and beneficial to the Army's antiterrorism goals, these visible and tangible actions have only addressed part of the need. With much of the less available funding being spent in a reactive fashion on physical security, little attention has been paid on response and recovery actions after an attack occurs. While it could be argued that if the first two are successful, more emphasis on these latter two aspects is not necessary, former Army Chief of Staff, General Eric K. Shinseki, cautioned over six months before the terrorist attack on the USS Cole in October 2000:

---

[2] *Report to the President and Congress on the Protection of U.S. Forces Deployed Abroad*, Annex A: The Downing Investigation Report, (Washington, DC: Headquarters, Department of Defense, August 30, 1996), 7; available on the Internet at http://www.fas.org/irp/threat/downing/report.pdf (accessed on February 25, 2005).

> Commanders must, as the law and available resources permit… establish procedures to enable effective response to save lives and contain damage if an attack does occur. Traditionally, AT/FP programs have relied on physical security measures to deter and defend against possible attack. Use of such measures should certainly continue. But there is another dimension of antiterrorism: of actively using information technology and human expertise to gain an understanding of terrorist motives and operational patterns, and actively engaging in the environment in which terrorists may operate.[3]

Although some minor improvements have occurred, the Army has made little real progress in this other dimension of antiterrorism: specifically, an organic intelligence capability that uses both human and technological means to assess a potential enemy's capacity to execute an attack against a specific installation.

A third problem is a lack of command influence in the antiterrorism and force protection areas. Army installation commanders have the responsibility for antiterrorism and force protection on their respective installations with the day-to-day execution of these programs delegated to their garrison commanders. Competing priorities (led by the fact that the U.S. is currently a nation still at war), limited resources both in dollars and personnel, and complacency (due to several consecutive years without a successful terrorist attack against the U.S. at home or abroad), have caused commanders to divert resources and their personal attention away from antiterrorism and force protection, towards other, more pressing priorities. As a result, required antiterrorism planning, vulnerability assessments, and training exercises are not being executed to standard, nor is there any uniformity across the Army with respect to antiterrorism and force protection doctrine, as none has yet been developed.

The emergence of "homeland security" (the term itself and the cabinet department) into the daily lexicon of average Americans poses another challenge for Army installations. What is the relationship between antiterrorism, force protection, and homeland security? Are homeland defense and homeland security different terms, or just different ways of saying the same thing? How

[3] *United States Army Antiterrorism and Force Protection Installation Commanders' Guide*, (Washington, DC: Headquarters, Department of the Army, March 2000), 3.

well do Army installations respond to crises that are not the result of terrorist attacks? How do the efforts of the Department of Homeland Security with respect to the emergency response capabilities of municipalities square with the force protection requirements and response capabilities of Army installations? How should the National Incident Management System (NIMS) be incorporated into Army installation force protection programs?

I begin this research effort believing that the Army has an acknowledged role in homeland security that is focused on two elements: homeland defense and civil support. In both of these elements, Army installations provide base operations and other logistical support to tenant units called upon to execute these missions. Additionally, the Army has a force protection mission, defined broadly as the security of its installations, to include the soldiers and family members residing on post, and the civil servants and contractors working there. Where the Army has heretofore maintained a separation between homeland security and force protection, I will argue that force protection must be linked to homeland security, and that this linkage requires special emphasis from installation and garrison commanders.

It is time for the Army to take a step back from its singular focus on antiterrorism, and seek to integrate its installation force protection programs with the emergency response programs of adjacent municipalities. Looking beyond the physical security aspects of antiterrorism, and their own internal resources and capabilities, Army installations must coordinate intelligence analysis and dissemination, individual security awareness, and crisis response and consequence management activities with their respective municipal partners using an all-hazards approach. Indeed, whether an installation is attacked, or suffers a natural disaster, accident, or severe weather event, *municipal support to military installations* will be absolutely essential in quickly restoring military operational capability, and in returning services, infrastructure, and supporting facilities to normalcy as rapidly as possible.

Since the 9/11 attacks, the Army has made some progress in these areas at the corporate or headquarters level. In response to Department of the Army Inspector General (DAIG) and Government Accountability Office (GAO) reports rendered over the past decade, the Army has refined its process for allocating antiterrorism funds, developed an antiterrorism strategic plan, and revised its antiterrorism regulation. The advent of NORTHCOM, and its Army component, US Army, North (ARNORTH) has improved the Army's ability to respond to all-hazards emergencies and to provide support to FEMA and other civil authorities when needed. The consolidation of Army installation management under a single command has also contributed to improved standardization and execution of antiterrorism and force protection programs.

The aim of this research effort is to show that although significant energy and resources have been expended at the corporate level of the Army to improve antiterrorism and force protection policy; these efforts have not translated into fully implemented and responsive programs at the installation level, where soldiers, their families, and the installation's civilian staff are directly affected. Furthermore, the Army is only now beginning to embrace the all-hazards emergency management approach espoused by the Department of Homeland Security, and in various stages of implementation in municipalities throughout the U.S. This thesis includes a discussion of how the Army Management Staff College (AMSC) led the Army's efforts to integrate installation force protection with municipal homeland security by developing and implementing a training and exercise program that seeks to move installations beyond deterring and preventing terrorist attacks to anticipating, responding to, and recovering from all-hazards crisis events that could strike at any moment. This comprehensive program includes over 30 hours of antiterrorism, force protection, and emergency response curriculum added to its Command Programs resident courses since early 2002, as well as the on-site Installation Force Protection Exercise (IFPEX) program for garrison commanders and staffs, launched in the fall of 2006.

D. METHODOLOGY AND SOURCES

The vehicle for supporting the argument that Army installation force protection must be integrated with municipal homeland security is a case study of Carlisle Barracks' experience with the IFPEX program. Carlisle Barracks is the home of the U.S. Army War College, and is located in south central Pennsylvania. The garrison commander at Carlisle Barracks used the IFPEX program to enhance his installation's ability to respond, in conjunction with local municipal partners, to a severe weather event scenario, and later to a simulated terrorist attack using a vehicle-borne improvised explosive device.

Since its inception, almost 70 Army installations world-wide, representing the Active Component, the Army Reserves, and the Army National Guard, have completed the IFPEX program. The IFPEX experience provided each of these installations a greater appreciation of the challenges they face in effectively coordinating antiterrorism/force protection and crisis response/consequence management plans and actions with their adjacent municipalities. More importantly, installation staffs and their municipal colleagues have built relationships of trust and understanding, and improved procedures and practices that will serve them well when faced with an actual crisis event.

Before discussing the Carlisle Barracks case, it is necessary to acquaint the reader with how the service and support functions of Army installations are structured. The following chapter introduces the major players within Army installation management, and what their responsibilities and relationships are. Additionally, the role of the U.S. Army Installation Management Agency (IMA) is explained.

Chapter III discusses force protection on Army installations (as opposed to the protection of forces deployed in combat theaters), and the distinction made by DoD between antiterrorism and force protection. The "Commander's Eight Critical Antiterrorism Tasks," contained in Army Regulation 525-13, are examined and correlated to similar functions performed by local municipalities within their emergency management structures.

In Chapter IV, Homeland Security is defined from a military perspective and distinguished from Homeland Defense. The U.S. Northern Command (USNORTHCOM) is introduced and its missions summarized, followed by a discussion of how the Army mission of force protection contributes to homeland security. The chapter concludes with a discussion of the Army's effort to embrace the National Incident Management System (NIMS) to facilitate improved cooperation with local first responders and emergency managers in executing Defense Support of Civil Authorities missions and when receiving support from municipalities during crises occurring on Army installations.

The Carlisle Barracks case study is contained in Chapter V. This chapter provides the historical context for the development of the IFPEX program, which traces its roots back to the weeks immediately following the 9/11 attacks. This chapter also contains a review of how the force protection curriculum of the Command Programs courses at the Army Management Staff College transitioned from an antiterrorism focus to the more desirable all-hazards approach to emergency management.

As governor of California, former president Ronald Reagan once said, "Governments tend not to solve problems, only rearrange them."[4] The concluding chapter will emphasize that in homeland security, we must do more than proverbially rearrange deck chairs on the *Titanic*. More than seven years after the 9/11 attacks, with the war in Iraq and other GWOT activities continuing indefinitely, it is imperative that Army installations fully embrace the integration of force protection and homeland security, working in close partnership with their respective municipalities to deter and prevent terrorist attacks, and to mitigate the potentially disastrous effects of any that may occur.

Homeland Defense and Civil Support missions are performed primarily by the Army; however, Army installations also require significant support from civilian municipalities to execute their internal force protection responsibilities. There are elements of civilian homeland security programs, particularly in

[4] Statement made in 1973; available on the Internet at http://www.allthingswilliam.com/presidents/reagan.html (accessed on December 14, 2004).

criminal intelligence collection, analysis, and dissemination; first response efforts; and consequence management that can enhance the force protection efforts of installations. Likewise, there are elements of Army antiterrorism programs such as access control, public education and awareness, vulnerability assessments, threat intelligence, and emergency management training and exercises that would be beneficial to municipalities. In these exchanges, the scales are tipped against Army installations—municipalities do not require as much from installations as they are asked to provide to them. While good fences do make good neighbors, Army installations must reach across them now more than ever to develop and enhance these essential relationships with their municipal partners.

II. ARMY INSTALLATIONS

A. BASIC FUNCTIONS AND FUNDING

Army installations provide three basic functions in support of the overall Army mission: power projection (training and deploying forces from the installation to the fight), force protection (installation security and defense), and sustainment of the force (resources, people, infrastructure, and facilities). While no two Army installations are alike, their garrison commanders are each responsible for these six base operations (BASOPS) areas: resource management, civilian personnel management, facilities and infrastructure management, environmental stewardship, morale, welfare and recreation (MWR) programs, and force protection.

Funding for installations is distributed through the Operations and Maintenance, Army (OMA) account (Figure 2). Funds in the *Mission* "bag" pay for such things as training, readiness, and contingency operations (most of the power projection category), while those in the *Base Support* "bag" fund facilities, infrastructure, and other support functions (mostly in the force protection and sustainment categories). Prior to October 2002, OMA funds were controlled by the Major Army Commands (MACOMs), allowing those commanders to shift funds back and forth between the Mission and Base Support bags, based on where their needs were greatest.

As there were (and still are) never enough funds to fully fund both sides in any given fiscal year, MACOM commanders would routinely migrate funds from Base Support to Mission accounts to ensure that their forces were ready for war, or any other contingency. Rarely did funds migrate the other way (from Mission to Base Support), leaving facilities and support programs under-funded and impacting retention rates as soldiers and their families began to demand (deservedly so) a higher quality of life in exchange for their service to the nation. The migration of funds also led to many purchasing and accounting

inefficiencies, and contributed to a persistent perception throughout the Army of "have" and "have-not" installations, depending solely on how MACOM commanders allocated resources.

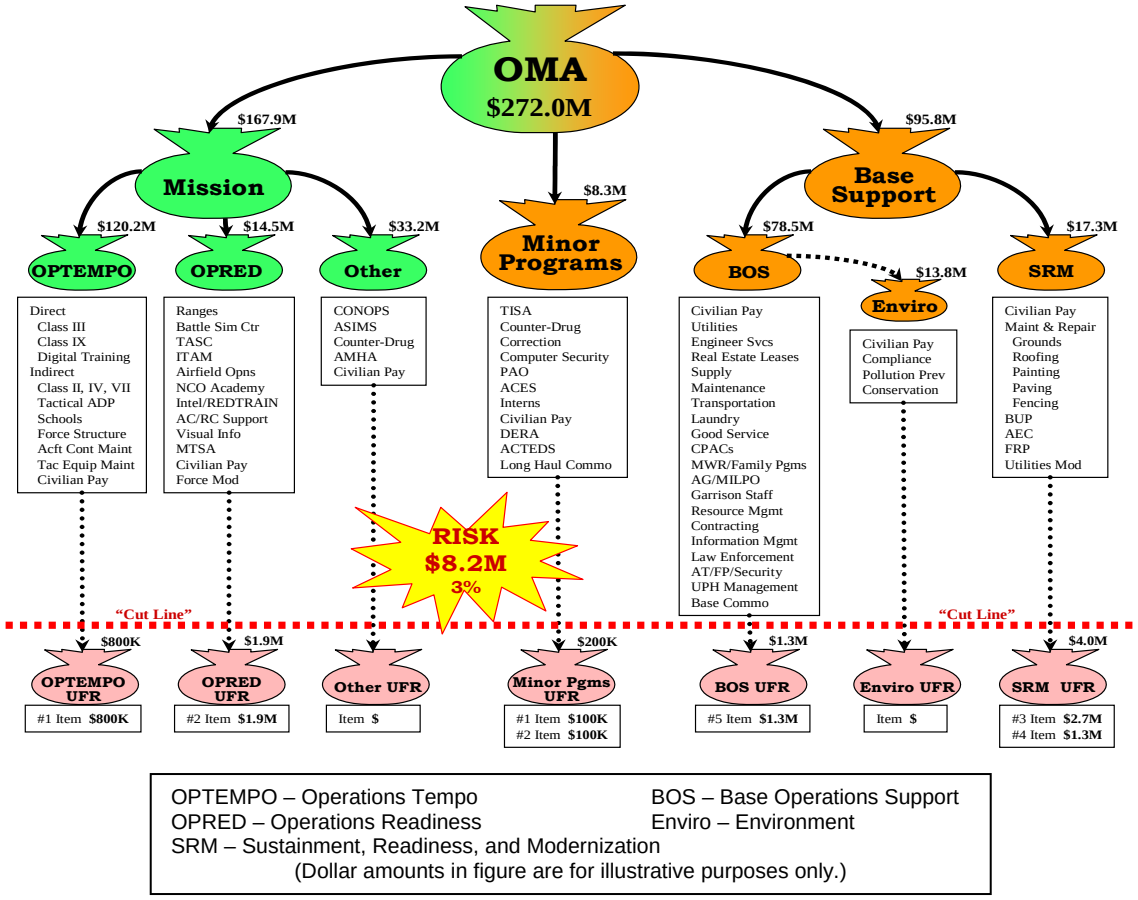

Figure 2. Operations and Maintenance, Army (OMA) Funding[5]

B. INSTALLATION ORGANIZATION

1. Major Army Command (MACOM) Oversight

Prior to October 2002, administration of Army installations was primarily a decentralized process (Figure 3). Under the Chief of Staff of the Army (CSA), MACOMs were responsible for command and control of both their subordinate mission elements and the installations they were assigned to. On each

[5] George Kopacki, "Your Base Support Resource Environment," unpublished lecture slides from Garrison Pre-command Course curriculum (FY04), Army Management Staff College, Fort Belvoir, VA, slide 6.

installation, garrison commanders provided base support to their tenant mission element units in accordance with their installation commander's desires and the procedures and standards of their respective MACOMs, as disseminated by their BASOPS staff sections.

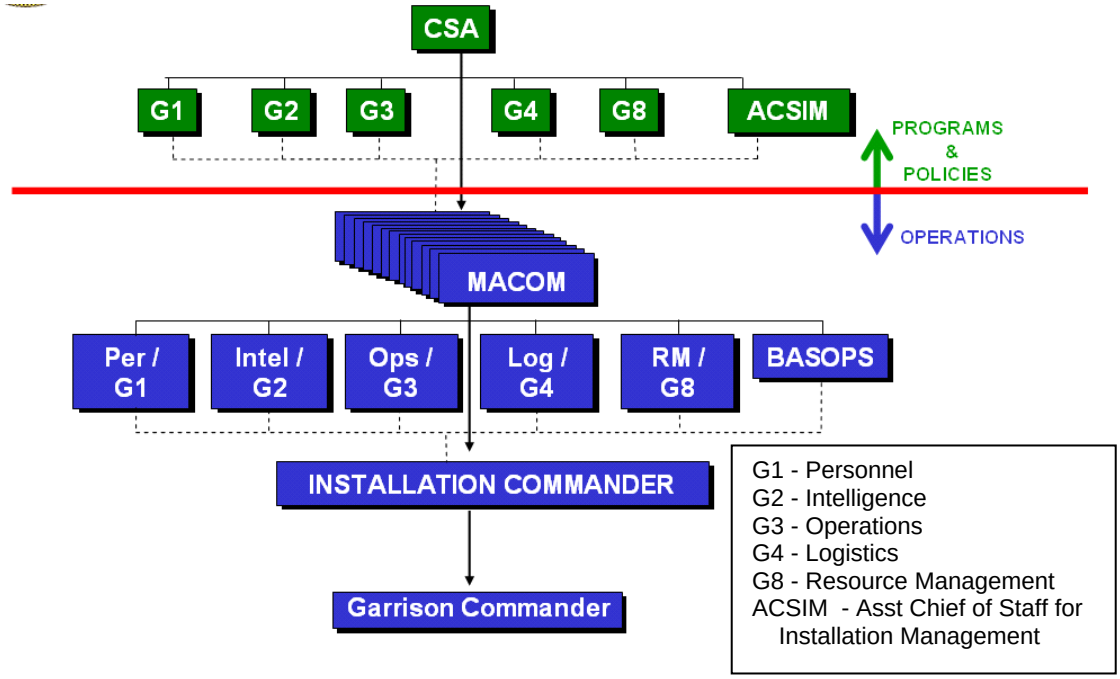

Figure 3. Installation Command Structure (before October 02)[6]

2. Installation Management Agency (IMA) Oversight

On October 1, 2002, the Army activated the Installation Management Agency (IMA), centralizing command and control of Army installations worldwide (Figure 4). At that time, MACOMs were relieved of the responsibility of administering installations so they could focus more fully on training and deploying forces to fight wars and meet other contingency requirements. Garrison commanders now report to IMA headquarters through one of seven regional directors. The IMA director reports to the Assistant Chief of Staff for

[6] Philip E. Sakowitz, "Army Transformation of Installation Management," unpublished information briefing from the US Army Installation Management Agency, presented at the Garrison Pre-command Course, Army Management Staff College, Fort Belvoir, VA, November 19, 2002, slide 34.

Installation Management (ACSIM) who answers to the CSA. General officer Senior Mission Commanders (known before as Installation Commanders) are now the second-line supervisors (senior-raters in Army parlance) of the garrison commanders.

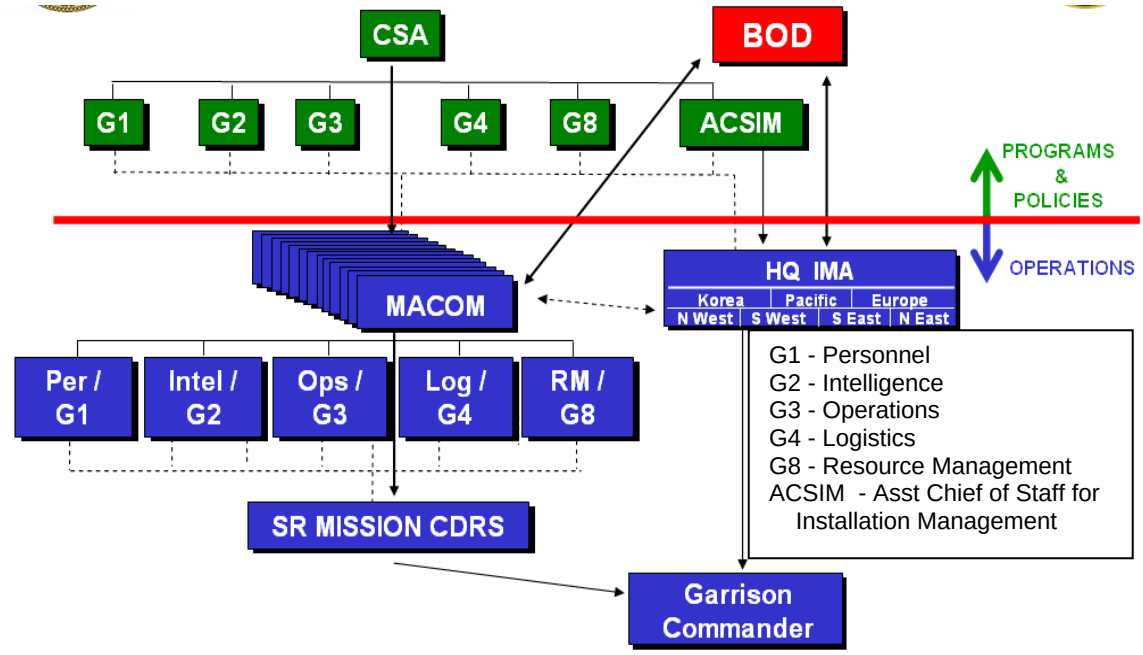

Figure 4. Installation Command Structure (after Oct 02)[7]

Another innovation of this new structure was the creation of a board of directors (BOD) composed of selected MACOM commanders and other key Army leaders. This board establishes broad installation management policy and provides guidance on standard levels of support and resource allocation. In this way, MACOM commanders are still involved to a degree in installation management business, but in a way that supports the efficiencies that come through standardization and centralized planning. The IMA organization provides a corporate structure focused on installation management that

[7] Philip E. Sakowitz, "Army Transformation of Installation Management," unpublished information briefing from the US Army Installation Management Agency, presented at the Garrison Pre-command Course, Army Management Staff College, Fort Belvoir, VA, November 19, 2002, slide 14.

- Supports mission commanders;
- Controls migration of base support funds;
- Achieves efficiencies; increases effectiveness;
- Provides common standards; the means and methods to manage installations;
- Leads Army Transformation.[8]

With IMA, senior Army leadership hoped to be able to provide more resources to Army installations, return uniformed soldiers currently assigned to installation and garrison duties to combat units where they are needed, and standardize service delivery across installations to eliminate "have" and "have-not" perceptions among soldiers, family members, and civilian staff.

[Note to reader: In October 2006, IMA underwent a reorganization that resulted in the creation of the U.S. Army Installation Management Command (IMCOM). IMCOM completely replaced IMA and added two new subordinates: the Family and Morale, Welfare, and Recreation Command (FMWRC), and the Army Environmental Command (AEC). The Assistant Chief of Staff for Installation Management (ACSIM) was "dual-hatted" as the Commanding General of IMCOM. The former Director of IMA was designated Deputy Commanding General, IMCOM, and runs the day-to-day IMCOM headquarters command and control of Army installations, while the Commanding General spends a majority of his time functioning as ACSIM. Additionally, in September 2007, a revision of Army Regulation 10-87 removes the term Major Army Command and the acronym MACOM from the Army lexicon and designates each former MACOM as an Army Command (ACOM), an Army Service Component Command (ASCC), or a Direct Reporting Unit (DRU).[9] IMCOM has been

[8] Ronald L. Johnson (Major General), "State of IMA," unpublished briefing from US Army Installation Management Agency, presented at the Army Garrison Commanders Conference, Fort Bliss, TX, November 16, 2004, slide 4.

[9] *Army Commands, Army Service Component Commands, and Direct Reporting Units* [Army Regulation 10-87], (Washington, DC: Headquarters, Department of the Army, September 4, 2007), "Summary of Change" page; available on the Internet at http://www.army.mil/usapa/epubs/pdf/r10_87.pdf (accessed on September 20, 2007).

designated as a DRU. Throughout the remainder of this work, the acronym IMCOM will be used in place of IMA, except for references cited that have "IMA" in their original title. The acronym MACOM will continue to be used throughout to refer to ACOMs, ASCCs, and DRUs as this change is not germane to the context herein, and many references cited have not yet been updated to reflect these recent changes in organization titles.]

C. GARRISON OPERATIONS

1. Standard Garrison Organization

Garrison commanders are assisted in their installation management responsibilities by a functional staff of experts—military officers or non-commissioned officers, civil servants, and contractors. In essence, an installation commander is like the mayor of a city, the garrison commander is like a city manager, and the garrison staff is similar to the municipal staff working for a city manager or mayor. The garrison staff supports the garrison commander and is responsible for administrating the six BASOPS areas previously mentioned. The staff is organized according to the Standard Garrison Organization (SGO), prescribed by the IMA in May 2004 (Figure 5). There are corresponding staff sections at the IMA regional and headquarters levels that provide technical support and oversight to the garrison staff. Additionally, certain garrison staff sections have coordinating relationships with similar sections on the Senior Mission Commander's staff (e.g., the garrison DPTMS with the mission element G3 [operations] or the garrison DOL with the mission element G4 [logistics].

2. Installations as Flagships

How the Army Runs, a U.S. Army War College publication, asserts, "Installations are the Army's 'face' to the nation and the world."[10] Upon assuming his duties as Army Chief of Staff, General Peter J. Schoomaker made "Installations as Flagships" one of his 16 immediate focus areas. In a February

[10] How the Army Runs, A Senior Leader Reference Handbook, 2003-2004, (Carlisle, PA: US Army War College, 2003), 381; available on the Internet at http://www.carlisle.army.mil/usawc/dclm/linkedchapters.htm (accessed on December 14, 2004).

2004 press release about the focus areas, Army officials stated, "Installations must be resourced to be holistic communities and secure sanctuaries, but also deployment platforms with robust reach-back capabilities."[11]

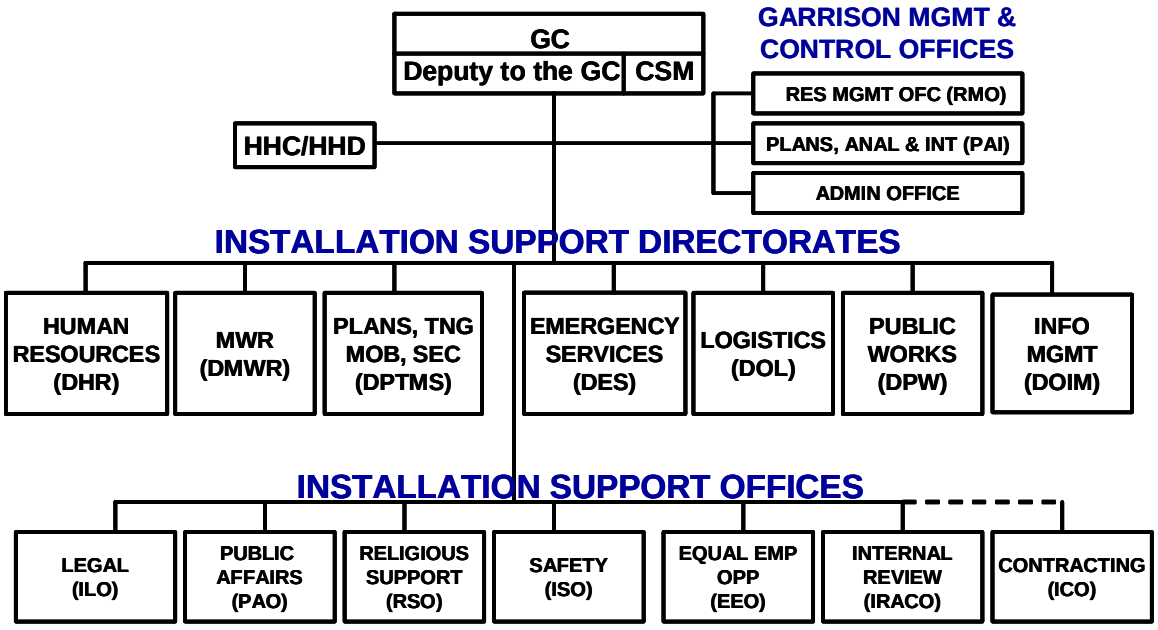

Figure 5. Standard Garrison Organization[12]

In this effort, garrison commanders play an important public relations role with respect to the local municipalities where approximately two-thirds of the soldiers, and all of the civil servants and contractors working on the installation, live. Not only are their significant economic benefits for municipalities located near Army installations, but installations are also becoming increasingly reliant on municipalities for support in their force protection programs.

[11] Marcia Triggs (Sergeant First Class), "Focus: Installations to serve as flagships," Army News Service press release, February 3, 2004; available on the Internet at http://www4.army.mil/ocpa/read.php?story_id_key=5635 (accessed on December 14, 2004).

[12] Ronald L. Johnson (Major General), "State of IMA," slide 9.

THIS PAGE INTENTIONALLY LEFT BLANK

III. ANTITERRORISM OR FORCE PROTECTION

A. FORCE PROTECTION

The definition of "force protection" as it relates to the military has evolved over the past decade since the 1996 Khobar Towers terrorist attack. The second edition (1998) of Joint Pub 3-07.2, *Joint Tactics, Techniques, and Procedures for Antiterrorism*, provides the following definition of force protection:

> Security program designed to protect Service members, civilian employees, family members, facilities, and equipment, in all locations and situations, accomplished through planned and integrated application of combating terrorism, physical security, operations security [OPSEC], personal protective services, and supported by intelligence, counterintelligence, and other security programs.[13]

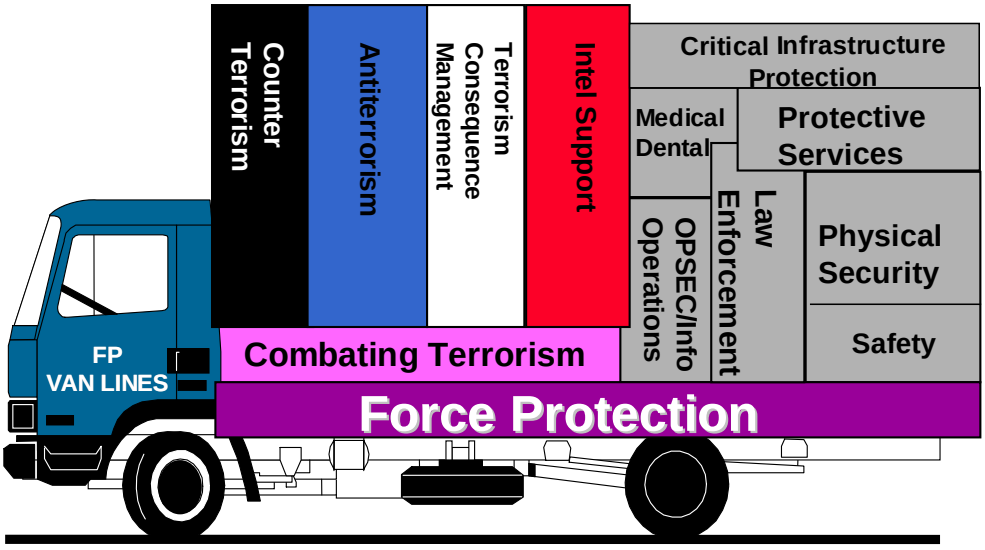

Figure 6. Force Protection Moving Van[14]

[13] Joint Tactics, Techniques, and Procedures for Antiterrorism [Joint Pub 3-07.2], (Washington, DC: Office of the Chairman, Joint Chiefs of Staff, March 17, 1998), GL-3; available on the Internet at http://www.dtic.mil/doctrine/jel/new_pubs/jp3_07_2.pdf (accessed on January 20, 2005).

[14] David S. Burdick, "Introduction to Antiterrorism and Force Protection," unpublished lecture slides from Garrison Pre-command Course curriculum (FY04), Army Management Staff College, Fort Belvoir, VA, slide 4.

In this definition, force protection might be viewed as a moving van that carries within it all of the other supporting programs administered by various staff sections within a military command (Figure 6). The Combating Terrorism Program is further broken down into four sub-programs: counterterrorism, antiterrorism, terrorism consequence management, and intelligence support. Since Khobar Towers, the Army has focused its force protection efforts primarily on antiterrorism, which is discussed further in the next section of this chapter.

The attack on the USS Cole in October 2000, followed a year later by the 9/11 attacks on the World Trade Center towers and the Pentagon, caused senior military officials to rethink the definition of force protection, especially as it pertains to security of military forces "in transit," as the USS Cole was when it was attacked. The revised DoD definition of force protection reads:

> Actions taken to prevent or mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities, and critical information. These actions conserve the force's fighting potential so it can be applied at the decisive time and place and incorporate the coordinated and synchronized offensive and defensive measures to enable the effective employment of the joint force while degrading opportunities for the enemy. Force protection does not include actions to defeat the enemy or protect against accidents, weather, or disease.[15]

This definition is best depicted by the force protection umbrella (see Figure 7). Arrayed under the umbrella's protection are the various coordinated and synchronized actions needed to protect DoD personnel, resources, facilities, and critical information.

It is interesting to note that this definition suggests a looser view of force protection as a collection of separate actions that are coordinated, rather than a security program of its own that integrates subordinate programs into the whole. Another major difference is the new definition's intent to "prevent and mitigate

[15] *DoD Antiterrorism Handbook* [DoD O-2000.12-H], (Washington, DC: Office of the Assistant Secretary of Defense, Special Operations and Low Intensity Conflict, February 9, 2004), 28; available on the SIPRNET from the Antiterrorism Enterprise Portal (ATEP) at http://www.atep.smil.mil (accessed on January 21, 2005).

hostile actions" instead of the old definition's mandate to "protect…in all locations and situations." The new definition also excludes "accidents, weather, or disease" presumably because they are not considered hostile actions. (This may be a bit short-sighted as the U.S. Intelligence Community would likely agree that a terrorist organization, or some other sympathetic nation, group, or individual might successfully manipulate so-called non-hostile events for hostile purposes.)

Figure 7. DoD Force Protection Umbrella[16]

[16] Rick Pressnell (Major), "Army Antiterrorism Program," unpublished briefing from HQ, Department of the Army, G-3/5/7 (DAMO-ODL), presented at the Garrison Pre-command Course, Army Management Staff College, Fort Belvoir, VA, September 30, 2003, slide 6.

At the time of this writing, the Joint Staff (for the Joint Chiefs of Staff) are proposing yet another definition of force protection:

> All measures and means taken to minimize the vulnerability of DoD personnel, facilities, equipment, and operations to all hazards in order to preserve the operational effectiveness of the force. Force protection is an inherent mission supported by diverse but complementary efforts including, at a minimum, antiterrorism, counterterrorism, CBRN [chemical, biological, radiological, nuclear] Defense, DCIP [DoD Critical Infrastructure Program], IO [information operations], law enforcement operations, physical security, HRP [high-risk personnel], crisis and consequence management, force health protection, and intelligence support.[17]

This proposed definition corrects the omission of the current definition by once again describing force protection as a concept including the spectrum of non- hostile activities such as a natural disasters and hazardous material (HAZMAT) response. It also defines force protection in terms of a more concrete minimum grouping of related functions (Figure 8).

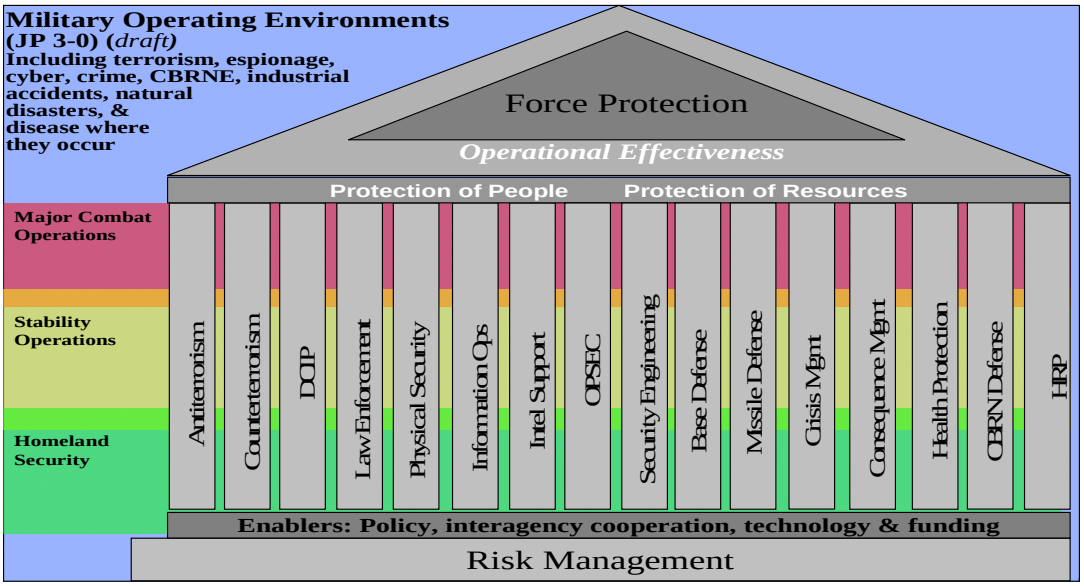

Figure 8. Proposed Force Protection Architecture[18]

[17] "The Revised Force Protection Concept," unpublished briefing slides from the Joint Staff, Deputy Directorate for Antiterrorism and Homeland Defense (DD AT/HD), received via e-mail from HQ, Department of the Army, G-3/5/7 (DAMO-ODF), April 7, 2005, slide 2.

[18] Ibid., slide 3.

B. ANTITERRORISM

Reviewing the major terrorist attacks against the U.S. over the past twenty years reveals some interesting points about the evolution of the Army's (and the entire Armed Forces') force protection and antiterrorism policy and procedures (Table 1). In each of the events cited in the table, the attack that occurred was not from the perceived threat that military or law enforcement officials planned defenses against. In every instance except for the 9/11 attacks, the destructive device was a vehicle-borne improvised explosive device (VBIED). Consequently, Army antiterrorism efforts have been properly directed toward deterring or preventing a terrorist attack from a VBIED. However, as U.S. experience against insurgent forces in Iraq and Afghanistan has shown, this is not as easy as it would seem for the world's lone superpower.

	Beirut	World Trade Center	Oklahoma City	Khobar Towers	East Africa	USS COLE	WTC & Pentagon
Perceived Threat	Sniper	None	None	Small Bomb	Small Bomb	Pierside Attack	Truck Bomb
Destructive Mechanism	Vehicle Bomb	Vehicle Bomb	Vehicle Bomb	Vehicle Bomb	Vehicle Bomb	Vehicle Bomb	Sky-jacked Airliners
Delivery Method	Truck	Van	Truck	Truck	Vans	Boat	Airplane
Place of Attack (Origin)	Mid East	NYC (Mid East)	Oklahoma	Mid East	Africa (Mid East)	Mid East	U.S. (Mid East)
Intel Assessed Threat (Threat Level)	General Threat (High)	None (Negligible)	None (Negligible)	General Threat (High)	General Threat (High)	General Threat (High)	None (Negligible)
Key Lesson	ROE Application	International CONUS Attack	Domestic CONUS Attack	Counter-surveillance & Standoff	Transnational Regional Threat	Determine Hostile Intent	Anticipate Out-of-the-box Threats

Table 1. Historical Perspective of Selected Terrorist Attacks[19]

The 1998 version of AR 525-13, now titled Antiterrorism/Force Protection, introduced the AT/FP acronym as well as this definition of antiterrorism (AT):

> Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and

[19] *DoD Antiterrorism Handbook* [DoD O-2000.12-H], 20.

> containment by local military forces. The AT Program is one of several security-related programs that fall under the overarching Force Protection and Combating Terrorism programs. An AT Program is a collective effort that seeks to reduce the likelihood that Department of Defense affiliated personnel, their families, facilities, and materiel will be subject to a terrorist attack, and to prepare to respond to the consequences of such attacks should they occur.[20]

This definition was carried over into the subsequent version of AR 525-13, renamed *Antiterrorism*—a way for the Army to continue to emphasize prevention and mitigation of hostile attacks on its installations and units and to try to eliminate the earlier confusion in terminology by de-linking antiterrorism and force protection.

This current version of AR 525-13 (January 4, 2002), along with defining "antiterrorism," organized commanders' antiterrorism responsibilities into eight critical tasks:

- Critical task 1: Establish an Antiterrorism Program
- Critical task 2: Collection, analysis, and dissemination of threat information
- Critical task 3: Assess and reduce critical vulnerabilities (conduct AT assessments)
- Critical task 4: Increase antiterrorism awareness in every soldier, civilian, and family member
- Critical task 5: Maintain installation defenses in accordance with FPCON [force protection conditions]
- Critical task 6: Establish civil/military partnership for WMD crisis
- Critical task 7: Terrorist threat/incident response planning
- Critical task 8: Conduct exercises and evaluate/assess AT plans[21]

---

[20] Antiterrorism [Army Regulation 525-13], (Washington, DC: Headquarters, Department of the Army, January 4, 2002), 42; available on the Internet at https://akocomm.us.army.mil/usapa/epubs/dr_pubs/dr_b/pdf/r525_13.pdf?feedAHP=Y (accessed on February 25, 2005).

[21] Ibid., 10-17.

In the sections that follow, each task will be discussed and related to similar functions performed in municipalities.

1. Critical Task 1: Antiterrorism Program

Critical Task 1 of AR 525-13 states: "Commanders will communicate the spirit and intent of all AT policies throughout the chain of command or line of authority by establishing AT Programs that provide standards, policies, and procedures to reduce the vulnerabilities from terrorist attacks."[22] As a lack of command emphasis and operational focus on AT was cited in the report from the FY2002 DAIG Army Antiterrorism Program Inspection as the most important root cause of AT program ineffectiveness, this critical task seeks to address this issue up front. To further emphasize command involvement in installation AT programs, the Installation Management Command (IMCOM) published its AT Strategic Plan, "Protecting our Flagships of Readiness," in July 2006. This IMCOM AT Strategic Plan is patterned after the Department of the Army's AT Strategic Plan, which complies with the DoD AT Strategy. It provides the roadmap for all Army garrisons to follow as they develop their own AT plans and procedures. The IMCOM AT Strategic Plan specifies measurable standards that are evaluated during Force Protection Assessment Team (FPAT) visits made periodically by the Department of the Army's AT staff. IMCOM is also developing its own assessment capability that will evaluate compliance of Army installations with the standards, policies, and procedures set forth in its AT strategic plan.

The IMCOM AT strategy correlates somewhat with various state-level contingency plans, policies, and procedures that have been established since the 9/11 attacks for responding to a terrorist incident at any given municipality. Similarly crafted response plans at the local municipality level correspond to installation-level AT plans developed by the garrisons. Although the DoD, Army, and IMCOM strategies loosely devolve from the *National Defense Strategy* and *National Military Strategy*, they more closely align with the *National Response*

[22] *Antiterrorism* [Army Regulation 525-13], 11.

Plan and the *National Strategy for Homeland Security*, sharing this common origin with the state and municipal response plans.

2. Critical Task 2: Threat Information

AR 525-13 directs that "Commanders at installation level and above will have a fully integrated foreign, domestic, and criminal intelligence AT intelligence program focused and based on priority intelligence requirements (PIR), that provides the appropriate threat information to protect personnel, family members, facilities, material, and information in all locations and situations."[23] Garrison Commanders are expected to have a system in place that enables them to collect, analyze, and disseminate terrorist threat information. They are further expected to use threat information to recommend to their respective installation commanders what the appropriate force protection condition (FPCON) should be.

Finding 11 of the Downing Commission Report on the Khobar Towers attack, stated that "the lack of an organic intelligence support capability in U.S. Air Force Security Police units adversely affects their ability to accomplish the base defense mission."[24] The report went on to indicate that "in contrast, U.S. Army Military Police battalions have an assigned intelligence section."[25] While this is true, the duties performed by these "intelligence sections" are focused on the functions of the MP Corps in support of combat and combat-like operations rather than installation base operations that garrison commanders are engaged in day-to-day. This distinction is important to note because today, the Army finds itself in the same predicament as the Air Force was in at Khobar Towers over a decade ago—there is no organic intelligence support capability within an Army garrison organization capable of providing the kind of intelligence needed to combat the threats it expects to face in a post-9/11 world.

---

[23] *Antiterrorism* [Army Regulation 525-13], 12.

[24] *Report to the President and Congress on the Protection of U.S. Forces Deployed Abroad*, Annex A: The Downing Investigation Report, 54.

[25] Ibid.

At the national level, attempts have been made to rectify the problem of intelligence. At its inaugural annual antiterrorism conference in 2000, the Army introduced the concept of "intelligence fusion" to address the intelligence shortfalls identified in the Downing Commission Report. The Antiterrorism Operations and Intelligence Cell (ATOIC) was created that same year as a Headquarters, Department of the Army (HQDA) element designed to fuse criminal information with tactical intelligence to form a single threat picture. The missions of ATOIC are:

- Provide strategic and tactical warning and maintain visibility of terrorist threats to the U.S. Army worldwide;
- Analyze terrorist-related intelligence and review criminal information *(fusion)* [italics in original]*;*
- Support antiterrorism and force protection through participation in assessment teams and policy review;
- Monitor and report worldwide threat conditions.[26]

ATOIC intelligence products are provided to the senior leadership of the Army to aid in their force protection decision making and are available to all Army commanders on their classified Internet web site. A parallel effort emerged after the 9/11 attacks beginning with the formation of the Department of Homeland Security, and culminating with the creation of the Terrorist Threat Integration Center (TTIC), which has since become the National Counterterrorism Center (NCTC).

Originally, "elements of the Department of Homeland Security, the FBI's Counterterrorism Division, the Director of Central Intelligence's Counterterrorist

[26] David S. Burdick, "Intelligence Fusion," unpublished lecture slides from Garrison Pre-command Course curriculum (FY04), Army Management Staff College, Fort Belvoir, VA, slide 7.

Center, and the Department of Defense [formed] a Terrorist Threat Integration Center to fuse and analyze all-source information related to terrorism."[27] Under its current guise,

> NCTC serves as the primary organization in the United States Government for integrating and analyzing all intelligence pertaining to terrorism possessed or acquired by the United States Government (except purely domestic terrorism); serves as the central and shared knowledge bank on terrorism information; provides all-source intelligence support to government-wide counterterrorism activities; establishes the information technology (IT) systems and architectures within the NCTC and between the NCTC and other agencies that enable access to, as well as integration, dissemination, and use of, terrorism information.[28]

Like ATOIC, NCTC's intelligence products are available on the Internet; however, the NCTC web site is unclassified and available to a wider public audience.

Since AR 525-13 requires garrison commanders to have a fully integrated foreign, domestic, and criminal intelligence program, yet does not provide an organic intelligence capability to the garrison organization, how is this to be accomplished? The ultimate solution is for the Army to authorize and fund an appropriate number of intelligence analyst positions within the garrison staff for every installation. While IMCOM is pursuing this with HQDA, garrisons are encouraged to try to develop some sort of intelligence capability from within their own resources, as well as leverage capability from adjacent civilian municipalities. This is accomplished through an ad hoc organization known as a "Threat Working Group," or "Intelligence Fusion Cell." These groups are often chaired by the garrison's antiterrorism officer and include representatives from the garrison provost marshal office, the supporting Criminal Investigation Division (CID) resident agency, the supporting military intelligence detachment, the garrison security office, the garrison directorate of logistics, and the garrison directorate of public works, as well as select municipal, state, and federal

[27] "Fact Sheet: Strengthening Intelligence to Better Protect America," (Washington, DC: The White House, January 28, 2003); available on the Internet at http://www.whitehouse.gov/news/releases/2003/01/20030128-12.html (accessed on October 29, 2007).

[28] "What We Do," National Counterterrorism Center web site home page; available on the Internet at http://www.nctc.gov/about_us/what_we_do.html (accessed on October 29, 2007).

agencies and organizations such as local police, local public works and utilities, state criminal investigation offices, and the FBI.

The Intelligence Fusion Cell provides intelligence support to the garrison commander and provides a venue for the exchange of pertinent criminal and terrorist intelligence information among installation, municipal, state, and federal agencies and organizations. Essentially, the fusion cell provides the garrison commander with a common operational picture of his/her areas of operations and interest, contributing to successful decision making with respect to FPCON, incident or event response, and the overall security and well-being of solders, family members, and civilian staff working and living on the installation.

With respect to intelligence gathering and analysis, the capabilities of municipalities reside in their police departments and are limited primarily to criminal intelligence. Like military installations, municipalities have seen the need for developing an intelligence fusion capability to provide the missing terrorist threat information. Most municipalities participate in FBI-sponsored state or regional Joint Terrorism Task Forces (JTTFs), where threat information from federal and state agencies is shared with municipal officials. These efforts have met with some controversy, and all levels of government have been pressured to carefully weigh the needs of public security against the public's reasonable expectation that government will guarantee individual privacy and civil liberties. The Patriot Act legislation has been the subject of much debate during the past few years with convincing arguments made in support of both sides. Garrison commanders and staffs must also use caution in their intelligence operations, for reasons that pre-date the Patriot Act. DoD Directive 5200.27, Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense, states: "DoD policy prohibits collecting, reporting, processing, or storing information on individuals or organizations not affiliated

with the Department of Defense,"[29] unless the information is essential to the accomplishment of these specific DoD missions:

- Protection of DoD functions and property
- Personnel security of members of the Armed Forces, retirees, members of the Reserve Components, and DoD civilian personnel
- Operations related to civil disturbance, but only when authorized by the Secretary of Defense to obtain essential information to meet operational requirements in response to "a distinct threat of a civil disturbance exceeding the law enforcement capabilities of State and local authorities[30]

This directive further states that "where collection activities are authorized to meet an essential requirement for information, maximum reliance shall be placed upon domestic civilian investigative agencies, Federal, State, and local."[31]

Essentially, the DoD is not to be used to "spy" on U.S. citizens or others not affiliated with DoD, except where specifically authorized for particular DoD purposes. Military Intelligence units are not authorized to gather the kind of domestic intelligence garrison commanders need to develop threat assessments and make FPCON recommendations. In striving for a balance between protecting civil liberties and enabling the military to obtain the information it needs about threats against its installations, facilities, or personnel, garrison commanders must leverage the knowledge and capabilities of civilian investigative agencies such as the FBI, state bureaus of investigation, and local police departments to satisfy the intent of Critical Task 2. This is successfully accomplished where garrisons have developed and nurtured good working relationships with these civilian agencies.

[29] *Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense* [DoD Directive 5200.27], (Washington, DC: Under Secretary of Defense for Policy, January 7, 1980), 2; available on the Internet at http://www.dtic.mil/whs/directives/corres/pdf/520027_010780/520027p.pdf (accessed on February 23, 2007).

[30] *Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense* [DOD Directive 5200.27], 4.

[31] Ibid., 2.

3. Critical Task 3: Critical Vulnerabilities

Vulnerability assessments are used to determine the installation's ability to protect personnel, information, and critical resources by detecting or deterring threat attacks. If that is not possible, then these assessments may be used to protect the installation by delaying or defending against threat attacks. Garrison commanders are required by AR 525-13 to conduct a self-assessment of their overall antiterrorism (AT) Programs within 60 days of assumption of command, and annually thereafter. Garrison commanders are also required to conduct a comprehensive vulnerability self-assessment at least once every three years. This comprehensive self-assessment must include the following functional areas:

- Physical security
- Engineering
- Operations, training, and exercises
- Military intelligence
- Criminal intelligence
- Command and control
- Law enforcement
- Threat options
- Operations security (OPSEC)
- Medical
- Executive protection, or protection of high risk personnel[32]

These self-assessments are best conducted by use of an ad hoc team formed by the garrison commander and usually led by the antiterrorism officer. Members of the team would normally include structural and facilities engineers, physical security inspectors, law enforcement and access control personnel, medical experts, information and communications managers, intelligence and

[32] *Antiterrorism* [Army Regulation 525-13], 13.

security officers, and human and resource managers. This team surveys the entire installation and organizes its findings in accordance with the functional areas previously listed.

Installation vulnerabilities are also discovered and documented by external assessment teams. After the Khobar Towers attacks, the Joint Chiefs of Staff established the Joint Services Integrated Vulnerability Assessment (JSIVA) program to assist installations from all military services in identifying and mitigating vulnerabilities. JSIVA teams are functionally oriented as depicted in Figure 9, and include a representative from the office of the Chairman, Joint Chiefs of Staff (CJCS) to provide policy guidance and other assistance to the installations they assess.

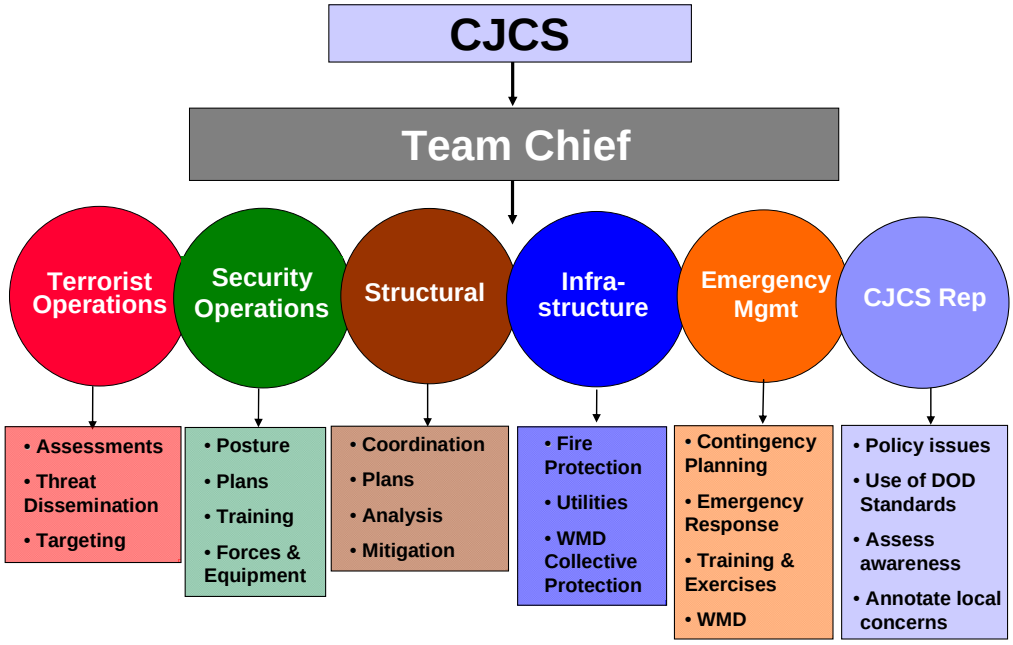

Figure 9. JSIVA Team Composition[33]

[33] Barry Cheyne, "Combat Support Assessments," unpublished briefing from Defense Threat Reduction Agency (DTRA), presented at the Garrison Pre-command Course, Army Management Staff College, Fort Belvoir, VA, October 14, 2004, slide 9.

JSIVA teams spend five days at each installation they assess and provide an exit brief to the garrison commander and staff before they depart. They also provide a classified written report of vulnerability assessment findings and observations to the garrison commander within 30 days of their visit.

HQ, IMCOM also provides external assessments of its garrisons by means of the Higher Headquarters Assessment Team (HHAT) program. HHAT teams are organized functionally, following the pattern of JSIVA teams and perform essentially the same functions. Garrisons will typically receive either a JSIVA or an HHAT assessment once every three years. Although both teams assess the same areas in the same manner, the JSIVA team only references DoD policy, instructions, and directives. In contrast, HHAT teams augment DoD guidance with reference to HQDA policy, regulations, and doctrine, bringing their assessment "closer to home" for garrison commanders and their staffs.

It is not enough to simply conduct a self-assessment, or receive an external assessment of installation vulnerabilities. Garrison commanders must take the results of these assessments and work to mitigate the vulnerabilities identified. HQDA has developed a web-based tool called CVAMP, the Core Vulnerability Assessment Management Program, to assist commanders with this, as well as enable these vulnerabilities to be more visible to senior leadership higher up in the chain of command. Most importantly, CVAMP provides an automated means for submitting and justifying funding requests, streamlining the process and providing a tracking mechanism for managing vulnerabilities from initial identification through mitigation, or perhaps elimination.

Outside the military, the 2006 National Infrastructure Protection Plan (NIPP) provides policy guidance to federal, state, and local government entities, as well as to the private sector, which is responsible for much of the nation's critical infrastructure.

> The NIPP provides the coordinated approach that will be used to establish national priorities, goals, and requirements for CI/KR [critical infrastructure/key resource] protection…to reduce vulnerability, deter threats, and minimize the consequences of

> attacks and other incidents. It establishes the overarching concepts relevant to all CI/KR sectors identified in HSPD-7 [Homeland Security Presidential Directive-7], and addresses the physical, cyber, and human considerations required for effective implementation of comprehensive programs. The plan specifies the key initiatives, milestones, and metrics required to achieve the Nation's CI/KR protection mission. It sets forth a comprehensive risk management framework and clearly defined roles and responsibilities for…Federal, State, local, tribal, and private sector security partners.[34]

Army installations and their adjacent municipalities should ensure that their respective vulnerability assessments and risk management efforts are coordinated. A nuclear power facility near an Army installation is a potential vulnerability to the installation as well as to the adjacent city and county. Likewise, freight rail lines running through an Army installation and the adjacent city and county would be a vulnerability to the entire area should a passing train load of hazardous materials somehow derail or suffer some type of attack that would cause toxic substances to be dispersed into the air or water system.

4. Critical Task 4: Antiterrorism Awareness

In the immediate days, weeks, and months following the 9/11 attacks, U.S. citizens came together as a nation as they haven't since the Pearl Harbor attack of December 7, 1941. No sacrifice was too great as we looked for ways to help, and the president challenged us to continue to live our lives as normally as possible, albeit with extra vigilance. America responded—its citizens rallied behind deploying troops and awareness of the dangers that al Qaeda and other terrorist groups pose became a part of everyday conversation. School children rehearsed lock-down procedures and there was a run on duct tape and plastic at local building supply retailers.

In this seventh year after the 9/11 attacks, America has become war weary and the lack of further attacks on American soil has allowed a spirit of complacency to set in, frustrating efforts to maintain a posture of antiterrorism

[34] National Infrastructure Protection Plan, (Washington, DC: Department of Homeland Security, 2006), i; available on the Internet at http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf (accessed on January 25, 2008).

awareness in daily life. This attitude is prevalent across the nation, to include Army installations, challenging garrison commanders to "ensure that all personnel are aware of the terrorist threat and adequately trained in the application of protective measures."[35] Commanders accomplish this critical task by completing the following subordinate tasks:

- Ensure antiterrorism training is an integral part of unit training plans, major training exercises/events, and a special interest item at training management reviews
- Enhance the general awareness of terrorism issues (Command Information Program, public affairs office effort, etc.)
- Assign antiterrorism officers… to provide training to unit members and advise the commander on antiterrorism matters
- Ensure antiterrorism officers are formally trained and certified
- Conduct annual antiterrorism awareness training
- Provide senior level leadership with antiterrorism knowledge [facilitate their attendance at one of the inter-service executive level antiterrorism seminars conducted three times each year by the Joint Staff]
- In significant and high threat areas, ensure personnel receive training concerning hostage survival[36]

The Army awareness philosophy is to educate its population concerning the nature of the terrorist threat, and provide practical means to recognize terrorist surveillance, steps to take to avoid being targeted by terrorists, and protective actions to implement if an attack occurs. In contrast to the Army philosophy, the Department of Homeland Security takes an all-hazards approach, sponsoring the "Ready" Internet site (http://www.ready.gov/), designed to help Americans prepare for any emergency, but emphasizing severe weather

[35] *Antiterrorism* [Army Regulation 525-13], 14.

[36] *Antiterrorism* [Army Regulation 525-13], 14.

and natural disaster events. The approach is not focused as much on deterrence and prevention as the Army's is, but rather stresses preparation for, and response to, an emergency event. Both approaches are necessary and the challenge for garrison commanders and municipal leaders is to counter the climate of complacency with an aggressive awareness campaign that helps the entire population detect, deter, prepare for, and respond to any type of emergency situation.

5. Critical Task 5: Installation Defenses

An inherent responsibility of any command in the military is the protection of one's forces so that they can be employed to execute their assigned missions. Protection of an Army installation is the responsibility of the Senior Mission Commander, typically the senior general officer assigned to the installation. The day-to-day execution of this responsibility belongs to the garrison commander who must "ensure that antiterrorism specific security procedural and physical measures are employed to protect personnel, information, and material resources from terrorist threats."[37]

One only needs to attempt to enter an Army installation to see that garrison commanders take this responsibility seriously. Hundreds of millions of dollars have been invested in the ongoing development and improvement of a comprehensive access control program that includes a combination of contractor and DoD civilian security guards, military and DoD police officers, military working dog units, barriers, bollards, fences, lighting, surveillance cameras, vehicle searches, and identification checks. This program provides a visible deterrent to any would-be attackers and provides a psychological feeling of comfort and security for those that live and work on Army installations, especially those family members who have fathers, mothers, and spouses deployed to combat theaters.

Along with the access control program, garrison commanders are providing extra protection for locations and facilities within the installations that

[37] *Antiterrorism* [Army Regulation 525-13], 15.

have been designated as critical assets or high risk targets, to include areas of high population concentration. Additionally, individuals designated as high risk personnel due to their rank or position, or the symbolic nature of their responsibilities, are provided protection beyond that provided to the general installation population. Random antiterrorism measures are also implemented at access control points and other select locations on Army installations to thwart enemy surveillance attempts to detect patterns or routines in security procedures that could be exploited.

Municipalities would have some difficulty with this task, as it is virtually impossible to completely control access into a city or town. Specific high value or critical locations could be protected, traffic controlled or diverted, and surveillance cameras employed (although not without court challenges concerning violations of civil liberties), but nothing to the extent of that done on Army installations. For this reason, municipalities focus more on response to an emergency event, rather than defense against one.

6. Critical Task 6: Civil/Military Partnership

This critical task gets to the heart of the argument of this paper—the successful defense of Army installations against terrorist attacks, and response to them should they occur, requires close and enduring partnerships with adjacent municipalities. There are four elements to this task as outlined in AR 525-13:

- Commanders will ensure antiterrorism plans are coordinated with local community officials to ensure a complete understanding of how and what military or civilian support will be rendered in the event of a WMD [weapons of mass destruction] crisis.
- It is imperative that commanders attempt to establish Memoranda of Understandings (MOUs) and/or Memoranda of Agreements (MOAs) with the local authorities to foster relationships that facilitate the shared use of critical resources. [Commanders and

civilian authorities will quickly discover that the effects of a catastrophic WMD event immediately overwhelm the capabilities of their organic assets.]

- It is highly encouraged that commanders include local agencies, that is, police, FBI, fire and medical authorities in committee meetings and working groups to assist in the development and execution of antiterrorism plans.
- Commanders will ensure that any support provided to civilian law enforcement agencies complies with AR 500–51 [ensuring that soldiers are not used in violation of the Posse Comitatus Act (18 USC § 1385)].[38]

As Figure 10 suggests, the ability of Army installations and adjacent municipalities to support one another in response to an emergency event varies according to the capabilities of each entity. From the installation perspective, a small installation adjacent to a small town, each with minimal assets and capability to contribute, would be viewed as having "limited" capacity to respond to a crisis and would therefore need the assistance of regional, state, or federal assets. A smaller installation with minimal assets and capability adjacent to a larger city with greater resources and capability would be viewed as "dependent" on that city to augment the installation as necessary during a crisis. An installation and adjacent city with roughly the same level of resources and capability would be viewed as "mutually supporting" each other in responding to a crisis situation. Finally, an installation with a large amount of assets and capability adjacent to a small town with minimal assets and capacity would be viewed as "self-sufficient," unlikely to request assistance from the adjacent municipality during a crisis. Depending on which situation installations find themselves in, garrison commanders and staffs develop, rehearse, and employ different tactics, techniques, and procedures in conjunction with their municipal partners to ensure an effective response to an emergency or crisis event.

[38] *Antiterrorism* [Army Regulation 525-13], 16.

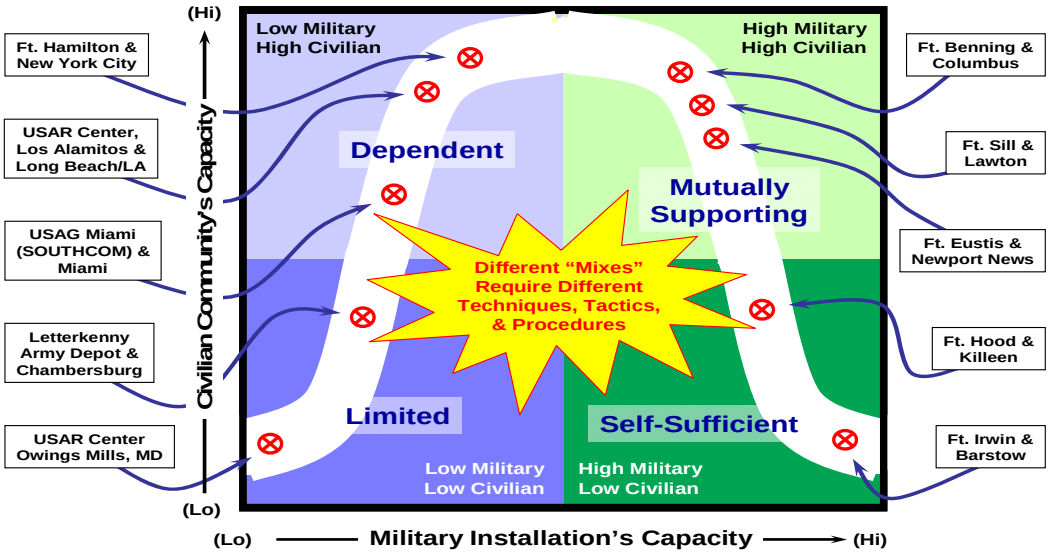

Figure 10. Emergency Response Capacity[39]

Since the 9/11 attacks, Army installations have met with varying levels of success in developing or enhancing effective working relationships with their municipal partners. One way to break the ice might be to use the graph in the above figure as a means to chart their collective emergency response capacity based on an assessment of available resources, training, facilities, and overall readiness to respond to a crisis. As either entity obtains additional resources, training, facilities, etc. that would affect their capacity, their place on the graph can be updated. Likewise, if either entity loses resources, or if training, facilities, or overall readiness suffers, that change can be updated on the graph as well. This drill helps each partner recognize the circumstances where it may become necessary to call upon regional, state, or federal assistance to mitigate the adverse effects of a crisis event or other emergency situation. Collaborative emergency response working groups are essential for facilitating communication and information exchange on a routine basis, before a crisis occurs.

[39] David S. Burdick, "Antiterrorism Critical Tasks," unpublished lecture slides from Garrison Pre-command Course curriculum (FY02), Army Management Staff College, Fort Belvoir, VA, slide 33.

One specific example of installations and municipalities that have been successful in developing and maintaining effective emergency response partnerships is found in the Tidewater area of Virginia, where three Army installations (Fort Monroe, Fort Eustis, and Fort Story), and the Installation Management Command's Northeast Region headquarters, are members of the Hampton Roads Emergency Management Committee (HREMC, http://www.hremc.org/). This committee, whose membership includes representatives from all military installations in the region along with 19 local municipal governments, public health, Red Cross, and regional, state, and private sector partners, promotes

> the inter-jurisdictional and inter-agency coordination of emergency management issues and foster emergency preparedness in the Hampton Roads area. Its purpose is to provide a working group for the exchange of information, experience and technology among the Hampton Roads Emergency Management officials and individuals with responsibilities in emergency management in the Hampton Roads area.[40]

While admittedly, the HREMC is focused mostly on hurricane preparedness and response, the fact that such an organization exists and meets regularly to discuss and coordinate emergency management issues suggests that the region, to include its Army installations, would be able to respond effectively to other emergencies, including a terrorist or other type of WMD attack.

7. Critical Task 7: Response Planning

In our post 9/11 culture of constant threat awareness and increased emphasis on emergency preparedness, this critical task is shared by Army installations and local municipalities. AR 525-13 directs commanders to "develop reactive plans that prescribe appropriate actions for reporting terrorist threat information, responding to threats/actual attacks, and reporting terrorist

[40] Hampton Roads Emergency Management Committee web site home page; available on the Internet at http://www.hremc.org/ (accessed on January 28, 2008).

incidents."[41] Municipalities are focused mostly on "responding to threats/actual attacks" as well as severe weather and natural disaster events. Garrison commanders have also expanded on the regulatory mandate and plan response actions for severe weather and natural disasters as well.

Terrorist threat and incident response planning must be "affordable, effective, and attainable; tie security measures together; and integrate security efforts by assigning responsibilities, establishing procedures, and ensuring subordinate plans complement each other."[42] As installations rely more and more on municipal first responders, it is incumbent on garrison commanders to ensure that their response plans are coordinated with appropriate municipal officials to include the integration of installation evacuation plans with those of their respective municipal, regional, and state plans. Additionally, garrison commanders of installations within the continental U.S. (CONUS) are required to:

- Notify the local FBI office concerning threat incidents occurring at Army installations, facilities, and activities;
- Take appropriate action to prevent loss of life and/or mitigate property damage before the FBI response force arrives;
- Take appropriate action…to resolve the incident [If the FBI declines jurisdiction]…, [coordinating] the military response with Criminal Investigation Command elements, [and] state and local law enforcement agencies, as appropriate.[43]

Garrison commanders of installations outside the continental U.S. (OCONUS) have two slightly different requirements:

- Where practicable, involve host nation security and law enforcement agencies in AT reactive planning and request employment of host nation police forces in response to threat attacks;

[41] *Antiterrorism* [Army Regulation 525-13], 16.

[42] Ibid.

[43] *Antiterrorism* [Army Regulation 525-13], 16.

- Coordinate reactions to incidents of a political nature with the U.S. Embassy and the host nation, subject to instructions issued by the combatant command CINC with geographical responsibility.[44]

The newly published *National Response Framework* (NRF), replacing the *National Response Plan* (NRP), requires state, tribal, and local governments "to develop detailed, robust all hazards plans and hazard- or incident-specific annexes with supporting procedures and protocols to address their locally identified hazards and risks."[45] The NRF offers these key aspects of response planning:

- Acceptability – meets requirements within costs and timeframes
- Adequacy – complies with guidance, addresses critical tasks
- Completeness – incorporates major actions, objectives, and tasks
- Consistency & Standardization – fosters interoperability
- Feasibility – accomplishes critical tasks with resources available
- Flexibility – all hazards approach, decentralized decision making
- Interoperability & Collaboration – integrates complementary plans[46]

8. Critical Task 8: Exercises

The final critical task is perhaps the most important as it requires commanders to "put it all together" by conducting exercises to "validate the AT plan, identify weaknesses, synchronize the AT plan with other related crisis action/consequence management plans, and develop corrective actions."[47] These exercises provide the means for garrison commanders to ensure that the requirements of the other seven critical tasks are accomplished, not just because

---

[44] *Antiterrorism* [Army Regulation 525-13], 17.

[45] *National Response Framework*, (Washington, DC: Department of Homeland Security, January 2008), 74; available on the Internet at http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf (accessed on February 8, 2008).

[46] *National Response Framework,* 74-75.

[47] *Antiterrorism* [Army Regulation 525-13], 17.

they are included in an antiterrorism plan, but because they have been tested and shown to be operationally effective in accomplishing the overall security objectives that commanders have established and that their staffs will execute when necessary.

Unfortunately, exercises are easily neglected due to complacency, competing and shifting priorities, and budget, staffing, or time constraints. A successful exercise program requires the personal involvement of the commander to ensure that its execution is a priority of the command. Involved commanders insist that their exercises contain a means of evaluation and follow-up so that lessons learned are not lost, but rather incorporated into revisions of their plans, updates in policies and procedures, or requests for additional resources or personnel when needed to more effectively accomplish the antiterrorism mission.

The *National Response Framework* contains an exercise requirement for all levels of government. Exercises are training opportunities that enhance a municipality's ability to respond effectively to a crisis situation.

> Exercises provide opportunities to test plans and improve proficiency in a risk-free environment. Exercises assess and validate proficiency levels. They also clarify and familiarize personnel with roles and responsibilities. Well-designed exercises improve interagency coordination and communications, highlight capability gaps, and identify opportunities for improvement.[48]

Army garrisons and their adjacent municipalities must seize every opportunity to train and exercise together, developing the close working relationships that will be critical to executing a swift and effective response to terrorist attacks, major accidents, natural disasters, severe weather events, or any other emergency situation.

[48] *National Response Framework*, 31.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. HOMELAND DEFENSE AND HOMELAND SECURITY

A. TERMS OF REFERENCE

For many, the terms "Homeland Security" and "Homeland Defense" are used interchangeably to define the actions necessary to protect citizens of the United States from an enemy attack, specifically, in recent years, one promulgated by terrorists. Within the federal government, and especially within the Departments of Defense (DoD) and Homeland Security (DHS), these terms are very distinct, and describe very specific plans, activities, and actions. These terms also connote statutory and jurisdictional responsibilities for DoD and DHS.

1. Homeland Security

The terrorist attacks of 9/11 reacquainted Americans with feelings of anger and revenge not felt since the Japanese attack on Pearl Harbor in 1941. Like the civil defense programs of the 1950s and 60s, designed to protect citizens against the nuclear threats of the Cold War, the 9/11 attacks have given rise to a new form of civil defense, that of Homeland Security, which is defined in the *National Strategy for Homeland Security* as "a concerted national effort to prevent *terrorist* attacks *within* the United States [italics added], reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur."[49] This focus on terrorism sets Homeland Security apart from Homeland Defense, as Homeland Security is a "shared responsibility built upon a foundation of partnerships [among] Federal, State, local, and Tribal governments, the private and non-profit sectors, communities, and individual citizens,"[50] whereas Homeland Defense is a unique military mission with a broader scope of national defense responsibilities.

---

[49] *National Strategy for Homeland Security*, (Washington, DC: Homeland Security Council, October 2007), 3; available on the Internet at http://www.whitehouse.gov/infocus/homeland/nshs/NSHS.pdf (accessed on February 29, 2008).

[50] Ibid., 4.

In its *Strategy for Homeland Defense and Civil Support*, DoD affirms:

> The primary mission of the Department of Homeland Security [is] to prevent terrorist attacks within the United States. The Attorney General leads our Nation's law enforcement effort to detect, prevent, and investigate terrorist activity within the United States. Accordingly, the Department of Defense does not have the assigned responsibility to stop terrorists from coming across our borders, to stop terrorists from coming through U.S. ports, or to stop terrorists from hijacking aircraft inside or outside the United States (these responsibilities belong to the Department of Homeland Security). Nor does DoD have the authority to seek out and arrest terrorists in the United States (these responsibilities belong to the Department of Justice).[51]

Dr. Karen Guttieri, a professor at the Naval Postgraduate School, notes:

> The U.S. military traditionally has been uncomfortable contemplating domestic operations. For generations, American war fighters have met responsibility for national security through projection of power—taking the battle to the enemy. The military in general stayed out of the domestic sphere, leaving police forces and federal civilian agencies such as the Federal Bureau of Investigation and Bureau of Alcohol, Tobacco and Firearms to keep order at home.[52]

2. Homeland Defense

Like Homeland Security, Homeland Defense has taken on more significance during the past few years than it has at any other time since World War II. Today, the military defines Homeland Defense as "[t]he protection of U.S. sovereignty, territory, domestic population, and critical defense infrastructure against *external* [italics added] threats and aggression, or other threats as directed by the President."[53] From this it could be simplified that Homeland

---

[51] *Strategy for Homeland Defense and Civil Support*, (Washington, DC: Department of Defense, June 2005), 5; available on the Internet at http://www.defenselink.mil/news/Jun2005/d20050630homeland.pdf (accessed on March 9, 2008).

[52] Karen Guttieri, "Homeland Security and US Civil-Military Relations," *Strategic Insights* (Monterey, CA: Naval Postgraduate School Center for Contemporary Conflict, Volume II, Issue 8, August 2003); available on the Internet at http://www.ccc.nps.navy.mil/si/aug03/homeland.pdf (accessed on March 8, 2008).

[53] Definition from *Department of Defense Homeland Defense and Civil Support Joint Operating Concept,* (Colorado Springs, CO: US Northern Command (NORTHCOM), October 1, 2007), B-3; available on the Internet at http://www.au.af.mil/au/awc/awcgate/DoD/hls_joc.pdf (accessed on March 2, 2008).

Security deals with *internal terrorist* threats, while Homeland Defense deals with any *external* threats to national security. However, DoD acknowledges an overlap in Homeland Defense and Homeland Security, noting the following:

> Threats planned or inspired by "external" actors may materialize internally. The reference to "external threats" does not limit where or how attacks could be planned and executed. The Department [of Defense] is prepared to conduct homeland defense missions whenever the President, exercising his constitutional authority as Commander in Chief, authorizes military actions.[54]

Homeland Defense is not just concerned with defense against terrorist attacks, but rather defense against all threats directed at the U.S. Homeland Defense is, in essence, the military response to attacks against the continental U.S., Alaska, Hawaii, or against any U.S. territory or possession, such as the U.S. response against Japan after the Pearl Harbor attack, or against Afghanistan after the 9/11 attacks. Some might even stretch this definition to include preemptive strikes against potential enemies, thereby labeling the current war in Iraq a Homeland Defense operation. However, Homeland Defense does not fall under an Army installation's "force protection umbrella" since force protection as currently defined, "does not include actions to defeat the enemy."[55]

3. Civil Support

The military defines Civil Support as "Department of Defense support to U.S. civil authorities for domestic emergencies and for designated law enforcement and other activities."[56] Under the superseded Federal Response Plan, DoD provided Civil Support, known then as Military Support to Civil Authorities (MSCA), primarily in response to official requests from the Federal Emergency Management Agency (FEMA) on behalf of states or localities suffering from severe disasters such as hurricanes, tornados, floods, extreme

---

[54] *Strategy for Homeland Defense and Civil Support*, 5.

[55] *DoD Antiterrorism Handbook* [DoD O-2000.12-H], 28.

[56] *DoD Homeland Defense and Civil Support Joint Operating Concept*, B-1.

winter weather, or forest fires. Installation and garrison commanders also provided direct, immediate military support locally, but only to prevent death, extreme suffering, or severe property damage.

The integration of FEMA into the Department of Homeland Security (DHS) brought into question the definition of Homeland Security—does it include preventing or responding to severe disasters that are not the result of terrorism? The 2005 hurricanes (Katrina and Rita, among others) that devastated the U.S. Gulf Coast, and virtually destroyed a large portion of New Orleans, Louisiana, led to this belated recognition by the federal government:

> Certain non-terrorist events that reach catastrophic levels can have significant implications for homeland security. The resulting national consequences and possible cascading effects from these events might present potential or perceived vulnerabilities that could be exploited, possibly eroding citizens' confidence in our Nation's government and ultimately increasing our vulnerability to attack. [E]ffective preparation for catastrophic natural disasters and man-made disasters, while not homeland security *per se*, can nevertheless increase the security of the Homeland [italics in original].[57]

Under the recently adopted National Response Framework, DoD continues to provide Civil Support to states and localities in the form of direct, immediate response to local officials to prevent death, extreme suffering, or severe property damage, or in deliberate response to FEMA requests coordinated with NORTHCOM. Now known by its new acronym, DSCA (Defense Support of Civilian Authorities), most of the DoD support to Homeland Security since the 9/11 attacks has been Civil Support for domestic emergencies.

4. Emergency Preparedness

In the context of Homeland Security, Homeland Defense, and Civil Support, DoD defines Emergency Preparedness as "measures taken in advance of an emergency to reduce the loss of life and property and to protect a nation's institutions from all types of hazards through a comprehensive emergency

[57] *National Strategy for Homeland Security*, 3.

management program of preparedness, mitigation, response, and recovery."[58] Emergency Preparedness within DoD includes planning for and implementing robust redundancy systems to ensure continuity of operations (COOP) throughout an emergency event, as well as DoD's participation in national-level continuity of government (COG) planning to ensure that essential functions of government are sustained during a major attack or catastrophic crisis. Successful Emergency Preparedness within DoD "is defined as development and maintenance, in cooperation with the heads of other departments and agencies, of national security emergency plans, programs, and mechanisms that ensure effective mutual support between and among the military, civil government, and the private sector."[59]

B. U.S. NORTHERN COMMAND (USNORTHCOM)

While state and local governments have made great progress in advancing homeland security initiatives since the 9/11 attacks, the military has struggled somewhat in trying to achieve balance between its traditional war fighting role, ongoing peacekeeping and nation-building endeavors, and its relatively new homeland security support responsibilities. In October 2002, the Department of Defense established USNORTHCOM, a combatant command covering all of North America that "provide[s] command and control of Department of Defense (DoD) homeland defense efforts and coordinate[s] defense support of civil authorities."[60]

> USNORTHCOM's AOR [area of responsibility] includes air, land and sea approaches and encompasses the continental United States, Alaska, Canada, Mexico and the surrounding water out to approximately 500 nautical miles. It also includes the Gulf of Mexico and the Straits of Florida. The defense of Hawaii and [U.S.] territories and possessions in the Pacific is the responsibility of U.S. Pacific Command. The defense of Puerto Rico and the U.S. Virgin

[58] *DoD Homeland Defense and Civil Support Joint Operating Concept*, B-3.

[59] Ibid., 5.

[60] *About USNORTHCOM*, from the US Northern Command Internet web site; available on the Internet at http://www.northcom.mil/About/index.html (accessed on March 12, 2008).

> Islands is the responsibility of U.S. Southern Command. The commander of USNORTHCOM is responsible for theater security cooperation with Canada and Mexico.[61]

(As U.S. Pacific Command and U.S. Southern Command cover relatively few Army installations, this paper will confine itself to discussing the USNORTHCOM perspective on Homeland Defense, Homeland Security, and Civil Support, recognizing that similar challenges exist with respect to these missions within the other two commands.)

The establishment of USNORTHCOM is unique in that it is the first time in U.S. history that a single command exists with command and control responsibilities over all military forces within the continental United States. Placing this much military power in the hands of a single commander was not without its critics. Just as the nation's founders were fearful of a large standing army after the Revolutionary War concluded, many modern politicians, pundits, and citizens at large questioned the need for this new command, and wondered aloud whether it would become just another layer of bureaucracy in the already too bureaucratic military-industrial complex President Eisenhower cautioned against. To answer critics and mitigate some of their concerns, USNORTHCOM was established primarily as a planning and coordinating organization without permanently assigned subordinate combat or tactical units. Instead, USNORTHCOM consists of a headquarters with subordinate joint force task forces, headquarters, and service component elements that are also free of permanently assigned subordinate units (Figure 11).

> USNORTHCOM plans, organizes and executes homeland defense and civil support missions, but has few permanently assigned forces. The command is assigned forces whenever necessary to execute missions, as ordered by the president and secretary of defense.[62]

---

[61] *About USNORTHCOM* web site.

[62] Ibid.

Figure 11. USNORTHCOM Organization[63]

Another reason for this lack of permanently assigned combat or tactical forces is political in nature in that the forces NORTHCOM would likely have assigned to it under a presidential directive would come primarily from federalized National Guard units—a move that is upsetting to some of the governors of the 54 states, territories, and the District of Columbia, who have seen their National Guard units federalized and deployed multiple times to Iraq, Afghanistan, and other international venues in support of GWOT and other missions of U.S. national interest since the 9/11 attacks. Many governors would rather retain control of their National Guard units during a Homeland Security crisis, than see them federalized and placed under the command and control of USNORTHCOM. USNORTHCOM coordinates closely with the National Guard Bureau, a DoD element that articulates and advocates National Guard matters at DoD level on behalf of the states, territories, and the District of Columbia. USNORTHCOM also coordinates closely with the U.S. Coast Guard, now part of DHS, on maritime and port security matters.

As previously mentioned, one of USNORTHCOM's missions is Homeland Defense. It is focused on external threats to the nation itself, or threats from the

[63] Thomas E. Williams (LTC, Ret.), "The Five Levels of Response," unpublished briefing for Army Management Staff College (AMSC) Installation Force Protection Exercise Program (IFPEX) garrison seminar, November 1, 2007, slide 23.

air, land, or sea approaches. As Army installations are not combat organizations themselves, their garrison commanders are not involved directly in Homeland defense, except to support those combat units on their installations that would deploy for such missions.

The second USNORTHCOM mission is Civil Support, a mission that the military performs admirably as noted during past events such as the perennial forest fires in the Western U.S., the *Columbia* space shuttle disaster in February 2003, and the Hurricane Katrina response in the fall of 2005.

> USNORTHCOM's civil support mission includes domestic disaster relief operations that occur during fires, hurricanes, floods and earthquakes. Support also includes counter-drug operations and managing the consequences of a terrorist event employing a weapon of mass destruction. The command provides assistance to a Lead Agency when tasked by DoD. Per the Posse Comitatus Act, military forces can provide civil support, but cannot become directly involved in law enforcement.[64]

Figure 12 shows the relationship among Homeland Security, Homeland Defense, Civil Support, and Emergency Preparedness as seen from the DoD perspective. Within its area of operations USNORTHCOM is involved with each of the numbered missions, except for number 3, Airport Security, which falls completely within the realm of Homeland Security and is executed by the Transportation Security Administration (TSA). Another interesting observation concerning this paradigm is that there is no overlap between the Homeland Defense and Civil Support missions, although each of them overlaps Homeland Security. For policy-making, statutory, budgeting, and training reasons, DoD and USNORTHCOM try very hard to keep these two missions completely separate, while recognizing that each supports Homeland Security in their own way.

[64] *About USNORTHCOM*, web site.

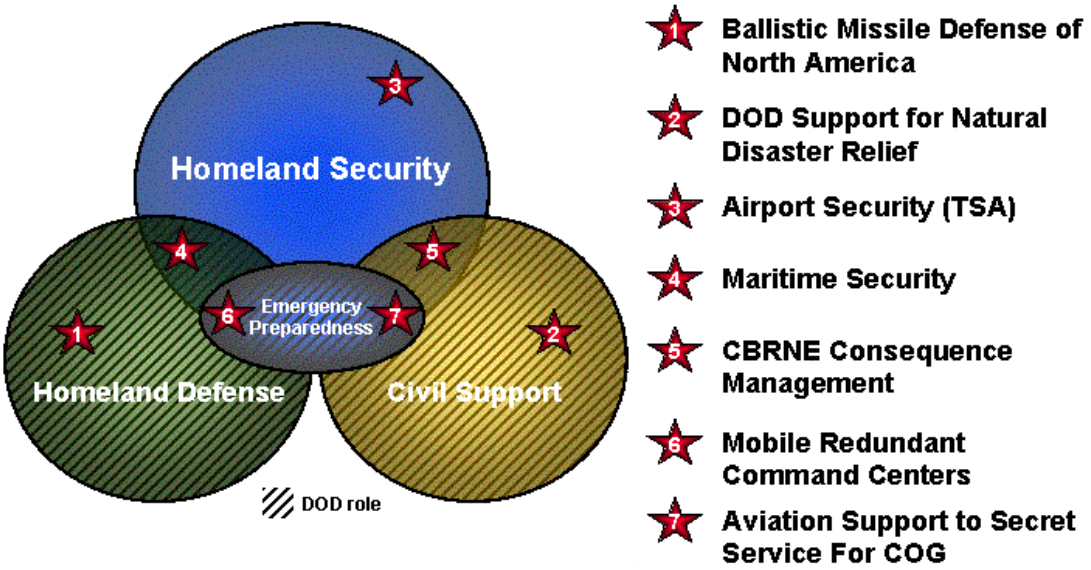

Figure 12. DoD Homeland Security Paradigm[65]

A final observation is that in keeping with the pure, terrorism-based definition of Homeland Security, as found in the *National Strategy for Homeland Security*, DoD places support for natural disaster relief completely within the Civil Support mission circle, whereas CBRNE (Chemical, Biological, Radiological, Nuclear, and High Explosives) Consequence Management falls in the overlap area between Civil Support and Homeland Security since a CBRNE attack would likely be terrorist related.

C. FORCE PROTECTION AND HOMELAND SECURITY

In reviewing USNORTHCOM's missions, one notes that Homeland Defense and Civil Support are focused outward—military elements providing overarching support directly to citizens at large (e.g., ballistic missile defense of North America), or targeted support to specific citizens, usually through another agency (e.g., response to natural disasters through FEMA or maritime security through the Coast Guard). To the average citizen, the assumption is that "when they (the military) are needed, they are there." What is often overlooked,

[65] *DoD Homeland Defense and Civil Support Joint Operating Concept*, 6.

especially prior to the 9/11 attacks, is how military crisis response capability is affected when attacks, disasters, or other crises occur on those installations municipalities expect to call on to respond to their own crises. The downsizing of the military after the first Gulf War, coupled with an increase in terrorist attacks directed against military targets (e.g., Khobar Towers, the USS Cole, and the Pentagon), revealed weaknesses and vulnerabilities in military force protection programs that had been previously neglected by commanders at all levels. Like the carefree adolescent believing he will live forever regardless of whether he exercises or eats right, only to grow up to become the overweight and out of shape, middle-aged adult, facing the reality of his inevitable mortality, the Army learned some lessons from these events and commanders quickly elevated force protection to “mission one.”

Force protection is an essential element of homeland security. Before military commanders can successfully execute homeland defense or civil support missions in support of homeland security, they must ensure that force protection has been addressed. Garrison commanders are charged with managing Army installations—the Army’s home—providing safety, security, quality of life, training support, and a capability to deploy forces anywhere in the world. Unfortunately, a garrison’s capacity to respond to an attack, severe weather event, natural disaster, or major accident on an Army installation, is limited due to modern budget realities and the high operations tempo of an Army at war. Although garrisons are significantly engaged in force protection and antiterrorism activities, there is no existing doctrine describing how military installations obtain and integrate support from municipalities during times of crisis. Installations have been left to themselves to identify and obtain necessary municipal support by means of memorandums of agreement (MOAs) or memorandums of understanding (MOUs). The good news is that since the 9/11 attacks, installations and municipalities have cooperated more closely with one another to develop and synchronize emergency response operations.

D. NATIONAL INCIDENT MANAGEMENT SYSTEM (NIMS)

On February 28, 2003, President George W. Bush issued Homeland Security Presidential Directive 5 (HSPD-5), *Management of Domestic Incidents*. This directive outlined the president's vision "to manage domestic incidents by establishing a single, comprehensive national incident management system."[66] In December 2005, Headquarters, Department of the Army (HQDA) tasked IMCOM and other major commands to:

> provide a plan of action which will adopt and implement procedures consistent with the NIMS and the Incident Command System (ICS) for Army Installations…which have firefighting and military or DoD police capabilities. The goal is to ensure all installations…are functionally aligned to provide or receive emergency response support from state and local first responders.[67]

This section provides additional explanation about NIMS, and outlines the structure and functions of the Incident Command System (ICS). This is followed by a discussion of the Installation Operations Center (IOC) and the functional alignment of its emergency response support responsibilities under NIMS.

1. Defining NIMS

NIMS is defined in HSPD-5 as a system providing "a consistent nationwide approach for Federal, State, and local governments to work effectively and efficiently together to prepare for, respond to, and recover from domestic incidents, regardless of cause, size, or complexity."[68] NIMS includes "a core set of concepts, principles, terminology, and technologies covering the Incident Command System (ICS); multi-agency coordination systems; unified command; training; identification and management of resources; qualifications and certification; and the collection, tracking, and reporting of incident information

---

[66] Homeland Security Presidential Directive 5 (HSPD-5), *Management of Domestic Incidents,* February 28, 2003, paragraph (1); available on the Internet at http://www.whitehouse.gov/news/releases/2003/02/20030228-9.html (accessed on March 13, 2008).

[67] Headquarters, Department of the Army Execution Order (HQDA EXORD) 693-05, *Plan of Action for Implementation of the National Response Plan and National Incident Management System,* 170003Z Dec 05, paragraph 3B.

[68] HSPD-5, paragraph (15).

and incident resources."[69] The comprehensive nature of NIMS is intended to provide for interoperability and compatibility among Federal, State, and local incident response capabilities.

NIMS contains seven components that provide the national framework for preparing for, preventing, responding to, and recovering from domestic incidents, regardless of cause, size, or complexity.[70] These components are command and management, preparedness, resource management, communications and information management, supporting technologies, and ongoing management and maintenance. A thorough reading of the DHS NIMS publication will provide ample clarity of each of these components; however, a lesson learned from the *Arlington County* [VA] *After-Action Report on the Response to the September 11 Terrorist Attack on the Pentagon* requires further discussion of an element of the command and management component—the Incident Command System.

2. The Incident Command System (ICS)

The NIMS command and management component comprises three key systems: the Incident Command System, Multi-agency Coordination Systems, and Public Information Systems. The ICS is of particular interest to garrisons as it is little understood outside the firefighting and law enforcement communities that originally developed and refined it over the past 30 years. During the response to the 9/11 attack on the Pentagon, Arlington County emergency management team members soon realized that the Emergency Operations Center (EOC) management structure defined by the county's Emergency Management Plan did not align with the ICS structure established by the Arlington County Fire Department at the incident scene itself.[71] First responders at the Pentagon did not have stove-piped counterparts at the county's EOC to

[69] HSPD-5, paragraph (15).

[70] *National Incident Management System* [NIMS], (Washington, DC: Department of Homeland Security, March 1, 2004), 3; available on the Internet at http://www.dhs.gov/xlibrary/assets/NIMS-90-web.pdf (accessed on March 13, 2008).

[71] *Arlington County* [VA] *After-Action Report on the Response to the September 11 Terrorist Attack on the Pentagon*, D-8; available on the Internet at http://www.arlingtonva.us/departments/Fire/edu/about/docs/after_report.pdf (accessed March 24, 2008).

reach back to for additional support and coordination. This challenge was quickly overcome and did not hinder the overall success of the operation, but it was experiences like this that led to the creation of NIMS with its flexible and adaptable ICS that can be used across a broad spectrum of contingencies and by all levels of government and private sector response.

The ICS provides a modular organizational structure that can be tailored for any incident.

> The incident command structural organization builds from the top down; responsibility and performance begin with the incident command element and the IC [incident commander]. When the need arises, four separate sections can be used to organize the staff. Each of these may have several subordinate units, or branches, depending on the management requirements of the incident. If one individual can simultaneously manage all major functional areas, no further organization is required. If one or more of the functions requires independent management, an individual is assigned responsibility for that function.[72]

Figure 13 shows the ICS structure in its most basic form. In keeping with the NIMS principle of using a common terminology, each box represents a "section" that performs specific functions. Each section may be further sub-divided depending on the scope and complexity of the incident.

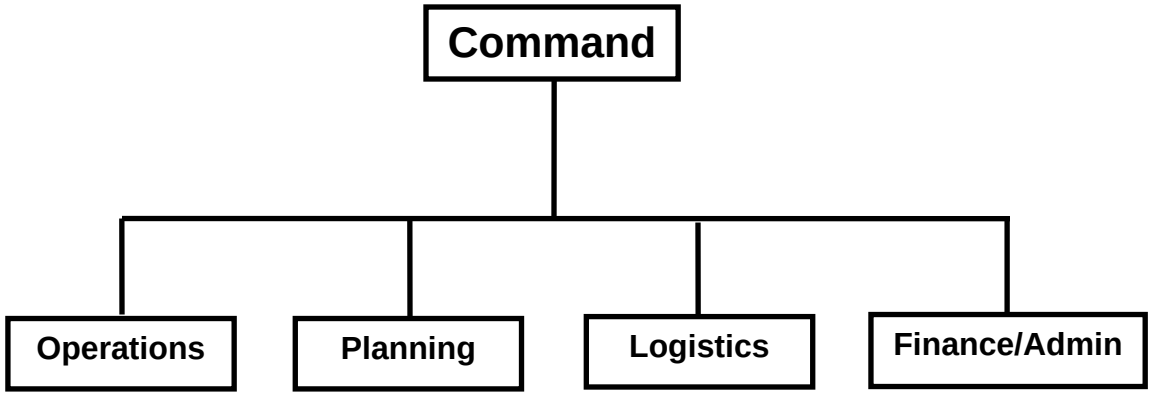

Figure 13. Basic ICS Structure[73]

[72] *National Incident Management System* [NIMS], 68.

[73] Ibid.

Functions of the Command Section are performed by the Incident Commander (IC) who is responsible for the overall management of an incident. The IC also approves any Incident Action Plans (IAP) developed and ensures their proper execution. Within the Command Section, the functions of Public Information, Safety, and Liaison are also performed by appointees directly answerable to the IC.

Public Information consists of that information that the IC disseminates to the pubic concerning the incident—not only the “five Ws” that the media wants answered, but more importantly, potentially life saving information such as what facilities/locations need to be evacuated, what evacuees should do, the condition of traffic flow in, out, and around the incident scene, and where citizens can go for assistance and further information. The Safety Officer ensures that all first responders and other visitors to the incident scene are properly protected from harm by following appropriate safety procedures, wearing proper protective equipment, and keeping the scene clear of extraneous personnel and equipment. The Liaison function is performed by representatives from organizations/ agencies external to the IC’s parent organization. The Liaison Officers are used to effectively coordinate response and recovery operations among responders from multiple jurisdictions and levels of government with the IC.

The Operations Section is concerned with the direct response to the incident. The Operations Section Chief manages all tactical activities at the scene under the direction of the IC. The Operations Section may be broken down into branches that are usually functional in nature (e.g., fire suppression, rescue, triage, and recovery). Branches may be further sub-divided into divisions (covering a specific geographic area) or groups (covering a specific functional assignment). The span of control is typically 1:5, so the section would have no more than five subordinate branches, and each branch would have no more than 5 divisions/groups to supervise.

> The Planning Section is responsible for collecting, evaluating, and disseminating tactical information pertaining to the incident. This section maintains information and intelligence on the current and forecasted situation, as well as the status of resources assigned to the incident.[74]

The Planning Section may be further divided into the following units, depending on need: Resources, Situation, Documentation, Demobilization, and Technical Specialist(s). These units assist the Planning Section Chief in gathering and analyzing all data regarding incident operations and assigned resources, developing alternatives for tactical operations, conducting planning meetings, and preparing incident action plans (IAP) for each operational period (shift).

The Logistics Section is responsible for all incident support requirements, to include "ordering resources through appropriate procurement authorities. It also provides facilities, transportation, supplies, equipment maintenance and fueling, food service, communications, and medical services for incident personnel."[75] The Logistics Section may be subdivided into six units: Supply, Ground Support, Facilities, Food, Communications, and Medical. These units may also be assigned to subordinate branches of the Logistics Section (e.g., Communications, Medical, and Food in a Service Branch, and Supply, Facilities, and Ground Support in a Support Branch).

A Finance/Administration Section is established by the IC when there is a specific need for financial reimbursement or administrative services to support incident management activities. This section monitors the sourcing and expenditure of funds in response to the incident and forecasts the need for additional funds. It also ensures that any statutory rules associated with certain funding are met. The Finance/Admin Section Chief may establish these functional units as needed: Compensation/Claims, Procurement, Cost, and Time.

---

[74] *National Incident Management System* [NIMS], 77.

[75] Ibid., 82.

3. The Installation Operations Center (IOC)

Unlike the ICS, which is an organization of functional areas used primarily by first responders at the scene of a crisis event, the Installation Operations Center (IOC) refers to the facility and organizational structure on an Army installation dedicated to the installation's response to a contingency event. The term *contingency* rather than *crisis* is significant as the IOC is used not only for crises, but for other significant installation events (e.g., terrorist attack, severe weather, natural disaster, mobilization and deployment, redeployment, or any other catastrophe or special event). The IOC is a garrison component that:

- Provides support to the IC at the scene of a contingency event;
- Orchestrates the execution of "collateral activities" relative to the contingency event (e.g., traffic control, personnel evacuation, public information, or long-term logistical support to first responders);
- Conducts consequence management operations to restore the installation to normal operations following crisis response or execution of a special event.

The IOC is staffed by key directorates within the IMCOM Standard Garrison Organization (SGO), augmented by liaison officers (LNOs) and other action officers from both on- and off-post organizations and agencies. The IOC may sometimes be co-located or absorbed within the senior mission element's operations center. Many garrisons with "stand-alone" IOCs have chosen to organize them using the five ICS functions. Figure 14 shows how the directorates and offices within the IMCOM Standard Garrison Organization (SGO, Figure 15) might be arrayed under the standard ICS structure. In keeping with the modular design of the ICS, one, some, or all of its sections may be organized and present at or near an incident scene on an Army installation. However, for most incidents likely to occur on installations it is assumed that only the command and operations sections/functions would be present at the actual incident scene, and that the other ICS functions of planning, logistics, and finance/administration would be performed within the IOC.

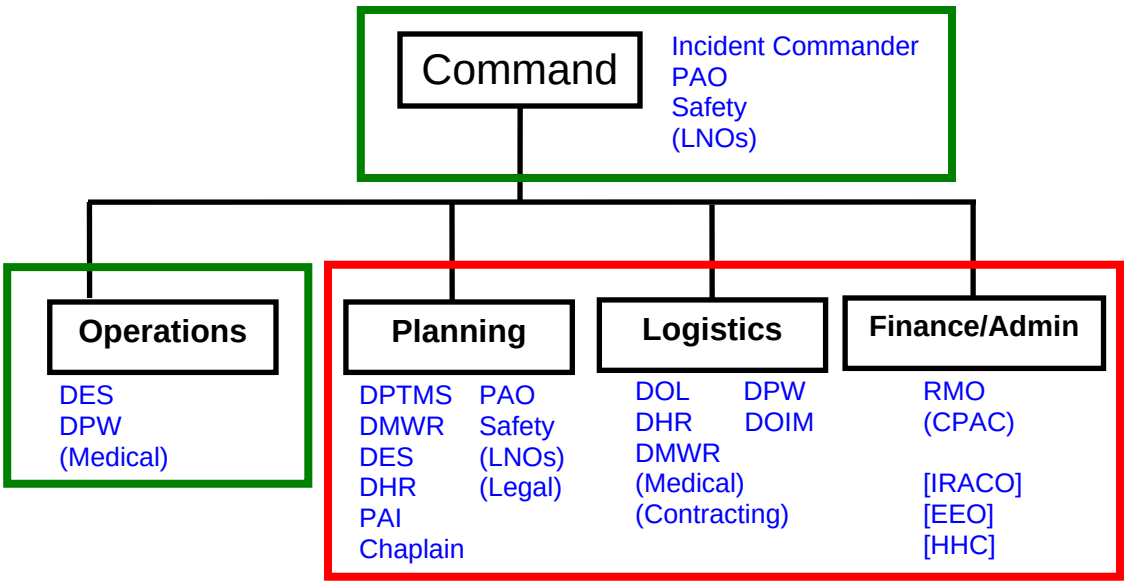

Figure 14. IMCOM SGO aligned with ICS Sections/Functions

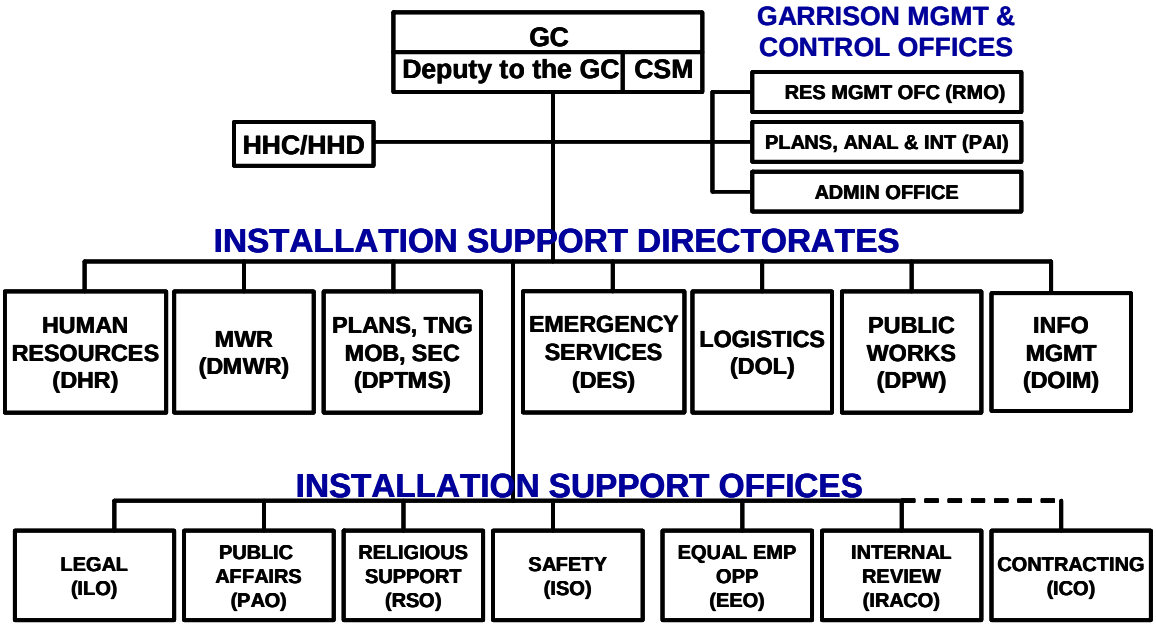

Figure 15. Standard Garrison Organization[76]

[76] Ronald L. Johnson (Major General), "State of IMA," slide 9.

The listing of SGO directorates under specific ICS sections is not absolute, but is done to show who would be engaged in doing the primary work of a particular ICS section/function. Notice that some SGO items are listed under more than one ICS function as they might perform either or both of those functions at some point during crisis response or consequence management. Also note that the garrison commander (GC), deputy to the garrison commander (DCG), and the garrison command sergeant major (CSM) are not shown within the Command section or in any other ICS section. This is intentional as the GC (assisted by the DCG and CSM) is responsible for the entire spectrum of garrison operations—all activities taking place at the scene of the incident (command and operations), those activities within the ICS (planning, logistics, and finance/admin), and all other ongoing garrison activities occurring anywhere else on the installation, much as a city mayor or city manager is responsible for all operations occurring within the city, even during response to an emergency situation or special event. Organizing the SGO under the ICS structure helps facilitate effective communications and information exchange among garrison staff sections that supports the first response efforts of the operations section and keeps the garrison commander situationally aware. This also contributes to flexible and timely decision making with respect to both crisis response and consequence management efforts.

Figure 16 takes a different approach, depicting an organizational and functional lay-out of a typical IOC designed to support current operations (i.e., support to the IC at the scene of a contingency event and the execution of "collateral activities"), and future operations (i.e., consequence management). Current Operations is led by the "Battle Captain," usually the DPTMS, or the Current Ops Officer within the DPTMS. Future Operations is led by the Deputy to the Garrison Commander (DGC). The GC does not have a "seat" in this IOC, which is intentional as it is not expected, nor desired, that the GC "run" the IOC. Rather, he/she should be free to move between the IOC, the incident scene, any

established joint operations or joint information center, and the mission element as necessary to maintain situational awareness and be available to provide information to the media, to victims/evacuees, and to the chain of command.

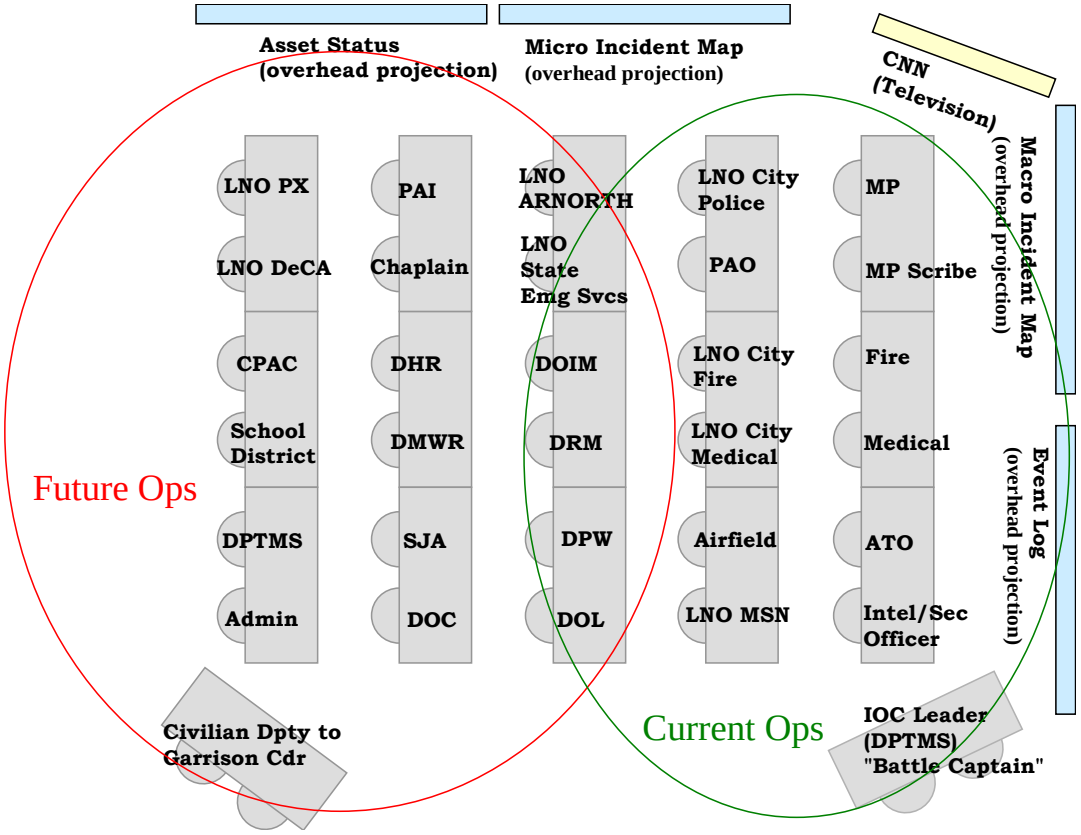

Figure 16. Typical IOC Organizational/Functional Lay-out

The overlapping current and future operations ovals indicate that there must be interaction and direct coordination between the DPTMS and the DGC. Also, some staff may find themselves working within both spheres, particularly those sitting in the center row: the Directorate of Logistics (DOL), the Directorate of Public Works (DPW), the Directorate of Resource Management (DRM), and the Directorate of Information Management (DOIM).

Several factors are considered when deciding how to organize and employ the IOC, and how to apply NIMS and ICS within it. The first consideration is historical effectiveness—has the IOC currently in place been

effective during past emergency operations? The next consideration is the garrison commander him- or herself—what organization best fits his/her command style, method of receiving and processing information, and decision-making methodology? A third consideration is local conditions or situation—what kinds of support or facilities are available from the mission element or from the municipal government? Will the installation face certain types of incidents (e.g., severe weather) more than others? A final consideration (although there may still be others) is resources—what funds and time are available to purchase equipment, hire and train personnel, and construct or renovate facilities?

While garrison commanders ponder these questions and work to achieve their ideal IOC structure and staffing in accordance with NIMS and ICS, the IOC will be employed as it currently exists to address the next crisis event, regardless of its size or scope. Garrison Commanders must strive, with the resources they have, to identify and train their IOC personnel in emergency response operations, to include NIMS and ICS, so that when they are needed, they will be ready—to support an incident occurring on one of their installations, with or without first response assistance from their respective municipal partners, or to provide civil support to those municipal partners when requested or when directed to do so.

V. CARLISLE BARRACKS CASE STUDY

A. INTRODUCTION

Carlisle Barracks is a small active-Army installation located in south central Pennsylvania approximately 20 miles west of Harrisburg, and 30 miles north of Gettysburg. It is the home of the U.S. Army War College, chartered to prepare senior officers and civil servants for strategic level leadership positions throughout the Department of Defense.

Like most military installations in September 2001, the garrison commander and staff at Carlisle Barracks had difficulty implementing the unprecedented, DoD-directed, world-wide upgrade to Force Protection Condition (FPCON) Delta, issued immediately after the 9/11 attacks occurred. This directive mandated a full lock-down of all DoD installations and facilities, requiring increased manpower to seal off all access control points, as well as the establishment of round-the-clock emergency operations centers to track incoming intelligence reports and coordinate the implementation of additional measures to both protect the force and prepare for anticipated combat operations. In the case of Carlisle Barracks, staff shortages led to the garrison commander recruiting some of the war college students (lieutenant colonels and colonels) to assist in staffing the emergency operations center during the days following the 9/11 attacks, until the FPCON Delta measures were relaxed.

This case study will trace the evolution of force protection training at Carlisle Barracks since the 9/11 attacks and show how the Army Management Staff College has been instrumental in helping Carlisle Barracks improve its ability to shift from a focus on antiterrorism to the broader all-hazards approach of an integrated force protection/homeland security program. This experience is typical of what most Army installations have gone through during the past seven years.

B. OPERATIONS GROUP ECHO

The Combined Arms Center at Fort Leavenworth, Kansas, trains brigade and battalion combat commanders in the art of war (particularly at the tactical and operational levels) through its Battle Command Training Program (BCTP). BCTP provides tailored seminars, computer-simulated decision-making exercises, and robust after-action reviews (AARs) that stimulate these commanders and their staffs to solve tactical problems, apply the Army's doctrine to challenging tactical situations, and promote a better overall appreciation of battle command and the complexities of war.

In the days immediately following the 9/11 attacks, General John Abrams, Commanding General of the Army's Training and Doctrine Command (TRADOC), conducted an inspection tour of the 15 installations under his command to see how well they had accomplished the DoD-directed increase to FPCON Delta. This tour culminated in a two-day conference hosted by General Abrams at Fort Leavenworth, Kansas, where the garrison commanders and select staff from each of the 15 TRADOC installations were invited to attend and share their successes and challenges in responding to the events of 9/11. During his tour, General Abrams found garrison commanders and their staffs to be "actively engaged, mission focused, and working hard to do the right thing,"[77] but there was no consistency in the way any of these installations approached their AT/FP responsibilities.

Concluding that this lack of consistency was attributable to a lack of uniform training, clear doctrine, and a dedicated flow of resources, General Abrams directed the BCTP staff to organize Operations Group Echo. This ad hoc group of military and civilian experts was tasked with adapting the BCTP model to Army installations, focusing particularly on terrorism. During the six months immediately following the 9/11 attacks, Ops Group Echo traveled throughout the U.S. conducting crisis decision-making seminars and table-top crisis response exercises, assessing the capabilities of each of the 15 TRADOC

[77] Robert A. Cline (Colonel), *Operations Group Echo Final AAR*, (Fort Leavenworth, KS: Battle Command Training Program, US Army Combined Arms Center, April 2002), 4.

installations to respond to a terrorist attack. As one of these TRADOC installations, Carlisle Barracks hosted a visit from Ops Group Echo in the fall of 2001 for their seminar, and again in March 2002 for their exercise.

The Ops Group Echo reports confirmed for General Abrams that although the TRADOC installations (including Carlisle Barracks) ultimately succeeded in implementing the DoD-directed FPCON Delta measures, they were woefully unprepared to respond effectively to a catastrophic attack similar to the one on 9/11 against the Pentagon. Specifically, Carlisle Barracks realized that the small troop clinic on post would not be adequate to treat victims of a mass casualty event; its crisis response team and emergency operations center were not robust enough to handle the demands of a large-scale crisis event; and the lack of AT/FP doctrine caused gaps in intelligence gathering and analysis, as well as in overall decision making within the emergency operations center.

In its final after action report, the commander of Ops Group Echo noted the following macro issues discovered during its six-month training and assessment period:

- A lack of regional efforts across the [military] services to support each other with intelligence, public affairs, first responder, and other resources;
- Training of our civilian staff members to execute the military decision-making process and evaluate chemical weapon employment is uneven;
- Our ability to share information to generate a common operating picture is diminished by numerous terminology conflicts between the civilian emergency management protocols and those we use in the military, and by conflicts in our own doctrine.[78]

[78] Robert A. Cline (Colonel), *Operations Group Echo Final AAR*, (Fort Leavenworth, KS: Battle Command Training Program, U.S. Army Combined Arms Center, April 2002), Executive Summary.

Recognizing that these shortcomings were not unique to TRADOC installations, General Abrams used the findings from Ops Group Echo to launch a similar training program for all Army installations. As Ops Group Echo continued its seminar and exercise visits to the TRADOC installations, General Abrams had already enlisted the help of the Army Management Staff College, directing them to design, develop, and deliver a BCTP-type AT/FP experience for all Army installations.

C. COMMAND PROGRAMS

1. History

The Army Management Staff College (AMSC) at Fort Belvoir, Virginia is responsible to "educate and prepare Army civilian and military leaders to assume leadership and management responsibilities throughout the [Army] in order to support the Soldier on the ground."[79] Command Programs, one of AMSC's two academic departments, is charged with preparing military and select civilian leaders for installation management responsibilities at any of the Installation Management Command's garrisons world-wide, and at special Army garrisons belonging to other Army Commands, Army Service Component Commands, or Direct Reporting Units.

Command Programs offers courses for three key leaders on Army installations: the garrison commander (Garrison Pre-command Course), the garrison command sergeant major (Garrison Command Sergeants Major Course), and the general officer senior commander (General Officer Senior Commanders Course). These courses present instruction in city management-like topics grouped under the following five headings: financial management, human resources management, facilities and infrastructure management, environmental stewardship, and morale, welfare, and recreation management.

[79] Garland H. Williams (Colonel), "Welcome to AMSC," from the Army Management Staff College Internet home page; available on the Internet at http://www.amsc.belvoir.army.mil/about/ (accessed on March 19, 2008).

After the 1996 Khobar Towers attack, AT/FP was added as a sixth topic area. From that time until the 9/11 attacks, only one hour of a three-week long (120 hour) Garrison Pre-command Course was dedicated to AT/FP. This one hour consisted of an overview briefing presented by a civilian contractor from the Army's AT/FP office in the Pentagon. At the time of the 9/11 attacks, the Carlisle Barracks garrison commander had limited AT/FP experience, having recently graduated from this version of the Garrison Pre-command Course. His command sergeant major had even less, as AT/FP was not a formal part of the curriculum in the Garrison Command Sergeants Major Course at that time (nor was it included in the General Officer Senior Commanders Course).

2. Post-9/11 Changes

As the U.S. reacted to, and recovered from, the 9/11 attacks General Abrams, in conjunction with the ongoing Ops Group Echo training efforts, seized an opportunity to enhance the amount and quality of individual AT/FP education provided to installation and garrison leaders. As a result of his influence, AMSC Command Programs was authorized to recruit an AT/FP subject-matter expert (this author) to join its faculty team in early 2002. At that time, the length of its Garrison Pre-command Course was extended by one week and this author was assigned to design, develop, and deliver AT/FP curriculum primarily to enhance the readiness of garrison commanders to execute their AT/FP responsibilities as outlined in the newly updated (January 2002) Army Regulation (AR) 525-13, *Antiterrorism.* Over the course of a couple of months, the one-hour AT/FP briefing evolved into almost 40 hours of additional classes and practical exercises focused on the previously discussed Commanders' Eight Critical Antiterrorism Tasks required by AR 525-13.

Over the past six years, this focus on AT/FP has grown to embrace an all-hazards approach with emphasis on emergency and consequence management for a wide spectrum of situations including severe weather, natural disasters, man-made disasters (i.e., terrorist attacks and CBRNE events), and special events (e.g., military ceremonies, Olympics and other major sports events, and

state funerals, presidential inaugurations, and other political or governmental events). Garrison commanders are instructed in, and engage in discussions on, how their installations provide Civil Support to their respective adjacent municipalities in support of Homeland Security as well as how those municipalities support their installations when necessary. Guest speakers from local, state, and federal levels reinforce classroom discussions on these topics, and practical consequence management exercises provide an opportunity for garrison commanders to think through their decision-making processes as situations unfold in a controlled, non-threatening atmosphere of learning.

While the Garrison Pre-command Course saw the greatest change in curriculum with the additional time and AT/FP and emergency management focus, the other courses went through changes of their own as well. The Garrison Command Sergeants Major Course was initially extended by one day, then later to two weeks, to provide time to present many of the same classes and practical exercises that the garrison commanders receive, so that they can better support their garrison commanders during emergency situations. The General Officer Senior Commanders Course remained one-week in length; however, some time was carved out of its schedule to include a practical exercise on general officers' installation command responsibilities during emergency situations.

D. INSTALLATION FORCE PROTECTION EXERCISE (IFPEX) PROGRAM

1. Background

As previously mentioned, the immediate success of Ops Group Echo in identifying gaps in AT/FP readiness, and providing training and exercise opportunities for garrison commanders and their staffs to better prepare for, and respond effectively to, terrorist attacks or incidents, prompted General Abrams to task AMSC Command Programs to replicate the Ops Group Echo experience for all Army installations. AMSC eagerly accepted this challenge, and this author was part of the team that designed the Installation Force Protection Exercise (IFPEX) Program in accordance with the BCTP and Ops Group Echo models.

The program concept was turned into a performance work statement (PWS) and a contract solicitation went out for bid during the summer of 2002, as General Abrams entered retirement. A contract was awarded in October 2002, however, shifting priorities within TRADOC leading up to the invasion of Iraq, caused General Abrams' successor to rescind funding for IFPEX in December 2002. Without a funding sponsor and mandate to continue the project, AMSC was forced to terminate the IFPEX contract in January 2003, before the first seminar ever occurred.

Undaunted by this funding setback and lack of a senior command sponsor for IFPEX, AMSC, in conjunction with the now maturing Installation Management Command (IMCOM), leveraged a recent Inspector General (IG) assessment of AT/FP shortcomings throughout the Army to convince the Army's Deputy Chief of Staff, Operations (G3) that IFPEX was still a necessary training requirement, deserving its full financial support. In part, the DAIG report noted that "the IFPEX program model represents a valuable collective FP training initiative for Army installations. This important Army training program requires immediate emphasis to resolve conflicts regarding policy, resource, and training requirements."[80] The G3 concurred and agreed to provide sufficient funding to IMCOM to execute the IFPEX program through AMSC. AMSC re-solicited bids from contractors to perform the IFPEX mission, eventually awarding a contract in September 2006.

2. Concept

Major General John Macdonald, Deputy Commanding General of IMCOM, outlines the IFPEX concept as follows:

> Every new Garrison Commander (GC) [participates] in a two-day seminar 150-180 days after change-of-command, with a Command Post Exercise (CPX) to follow within 60-90 days. Events are tailored to the specific needs of the GC and the conditions at each specific site…. I encourage Garrisons to involve local municipal, county, and state emergency management, police, fire, and medical representatives in IFPEX events. They are very instructive

[80] *FY2002 Army Antiterrorism Program Inspection (Phase I – Active Army)*, (Washington, DC: Department of the Army Inspector General, March 6, 2003), 5-21.

> for all participants by enabling them to collectively work the details of how to respond to an emergency event as it unfolds, and describing and discussing these ideas during training.[81]

Although Major General Macdonald's concept of IFPEX requires every garrison commander to participate in a training seminar and follow-on CPX, available funding from G3 limited the number of participating installations to 68. These 68 IMCOM-selected installations are divided in half, so that 34 installations receive a seminar and CPX event in alternating years, allowing most garrison commanders to go through the IFPEX experience once as a new commander and again as a more seasoned one.

For smaller installations, Army Reserve centers, and National Guard armories not selected to receive the on-site IFPEX Seminar and CPX, a web-based, exportable force protection training package is available at the AMSC Internet web site at http://www.amsc.belvoir. army.mil. The IFPEX link at this site (requires Army Knowledge Online [AKO] access) contains a series of functional lessons and scenarios or vignettes that commanders can use to teach and test their staffs in a way that mimics the seminars and CPXs. Some garrison commanders have also found this site useful to help them prepare their staffs for upcoming IFPEX Seminar and CPX events. The site content is reviewed and updated about every 100 days, so along with providing a training vehicle, it is also a great source for obtaining evolving doctrine, lessons learned, best practices, and new information.

The IFPEX seminars provide Garrison Commanders a unique opportunity to train with their staffs in a variety of subject areas. The IFPEX contractor team (Team IFPEX) tailors the seminar experience to the needs of the garrison, consulting directly with the commander as he/she selects seminar sessions from among the following topics (* indicates those selected by Carlisle Barracks):

- *Installation AT/FP Planning
- Vulnerability Assessment/Analysis

[81] "Installation Force Protection (IFPEX) Program," informational brochure from the Army Management Staff College, November 2007.

- Intelligence Fusion
- *Installation Operations Center Operations
- *Command and Control for Incident Response
- Media Relations in Crisis Management
- Quick Reaction Force (QRF) Operations
- Communications and Information Assurance
- Chemical, Biological, Radiological, Nuclear and High Yield Explosives (CBRNE) Detection and Survey
- Personnel and Facility Decontamination
- *Law Enforcement Rules/Responses
- Legal Aspects of AT/FP
- *Medical Force Protection Plans
- *Response to Accidents, Weather, and Natural Disasters
- *Five Levels of Crisis Response

All seminars include two practical exercises and a facilitated After Action Review (AAR), providing immediate feedback to the garrison as it prepares for its coming IFPEX CPX.

The IFPEX CPX provides an opportunity for the garrison to demonstrate what was learned during the seminar as well as other capabilities sharpened during the intervening months since the seminar. The CPX begins with a scenario-driven, all-hazards based exercise tailored to highlight topics that the commander previously selected for emphasis during the seminar. A retired Army General Officer serves as Senior Mentor for the CPX, coaching the garrison commander and deputy in their responsibilities. The CPX concludes with functional “hot washes” in the areas of command and control; operations, plans, and intelligence; logistics, resources and administration; and first responders, followed by a collective AAR for the entire garrison command and staff team. A

final written report, to include an overall emergency response performance rating on a scale of 1 to 10, is provided to the garrison commander within 30 days after the conclusion of the CPX.

3. Carlisle Barracks

Carlisle Barracks held its first IFPEX seminar from October 31 to November 1, 2007. In addition to selecting the topics noted above, the garrison commander established the following overall goals for the seminar:

- Assist in building the command and staff team;
- Focus on command and staff processes;
- Stimulate thinking about doctrine, AT/FP planning, the complexity of crisis response and consequence management, leadership styles, and garrison standard operating procedures (SOPs).[82]

It was obvious to Team IFPEX that the garrison commander and staff at Carlisle Barracks had accomplished much since their Ops Group Echo seminar and CPX experience of 2001-02. At the seminar, Team IFPEX noted that the garrison had established memorandums of understanding (MOUs) with several municipal agencies and was included in local county emergency management support planning. The garrison has a good severe weather plan for snowstorms and is leaning forward in planning for a pandemic flu event. The team also observed effective use of video surveillance across the installation, redundant communications means within the Installation Operations Center (IOC), and an installation-wide mass notification system for emergencies.

Unique to Carlisle Barracks is its superb intelligence collection and analysis capability, available only because the garrison commander elected to dedicate a staff member to this function even though such a duty position does not currently exist in the IMCOM Standard Garrison Organization. This intelligence analyst enhances the garrison's ability to develop and maintain a

[82] *Installation Force Protection Exercise (IFPEX), U.S. Army Garrison Carlisle Barracks – Final Report*, (Fort Belvoir, VA: Army Management Staff College Team IFPEX, March 4, 2008), Enclosure 3.

better common operating picture because he built relationships that resulted in effective collaboration with local, state, and federal law enforcement and security organizations to obtain relevant intelligence concerning Carlisle Barracks on a routine basis.

At the conclusion of the seminar, Team IFPEX challenged Carlisle Barracks to focus on mitigating the 20 identified shortcomings during the weeks between the seminar and subsequent CPX. Significant among these shortcomings were the following:

- No Internet connectivity with county emergency management office and no workstation for a county liaison officer within the IOC;
- Lack of integrated training among garrison staff within the IOC;
- Ineffective SOPs for information management and information sharing, particularly casualty tracking;
- Confusion over proper role of law enforcement dispatch desk relative to the IOC during incident response;
- The need to establish a "battle captain" position within the IOC and identify who is to fill that position.[83]

Team IFPEX returned to Carlisle Barracks for its CPX, February 20-21, 2008. The garrison commander requested two consecutive four-hour CPXs rather than the more typical single, six-hour event, and asked that one event address a weather emergency and the other a terrorist attack. Over 25 garrison staff participated with their commander in this exercise along with several members of the adjacent Cumberland County Emergency Operations Center. Because Carlisle Barracks is a small installation, it relies heavily on Cumberland County to augment its meager first response capability.

[83] *IFPEX, U.S. Army Garrison Carlisle Barracks – Final Report*, Enclosure 3.

The first day's exercise began at 8:00 a.m. with the National Weather Service issuing a tornado warning for the installation and surrounding towns. At 8:15 a.m., tornados struck the post, uprooting trees, breaking limbs, and damaging private and public property, specifically the post exchange and commissary. Traffic on the U.S. highway just outside the installation's main entrance was slowed due to downed power lines, trees, and malfunctioning traffic signals, affecting the flow of emergency response assets from the county to the installation. The garrison's ability to effectively command and control this crisis situation was challenged as the IOC dealt with the resulting casualties, severe property damage, jurisdictional concerns, and multi-organizational coordination issues at local, state, and federal levels.

The second day's exercise continued the scenario, focusing on the consequence management activities required to return the installation to normal operations. As this planning and execution was underway, a domestic terrorist organization decided to take advantage of the confusion caused by the previous day's natural disaster and detonate a VBIED at the main entrance to Carlisle Barracks. The IOC also received reports that unknown suspicious males were seen on the installation and suspicious backpacks were discovered near Root Hall, the home of the Army War College. This attack further challenged an already stressed commander and staff with additional mass casualties, more property damage, and an intelligence dilemma affecting the security of the installation's main tenant.

As Team IFPEX conducted its functional hot washes and facilitated the final AAR, several garrison strengths emerged from the discussions:

- Competent, well trained garrison staff with good internal SOPs;
- Commitment to adopting the National Incident Management System (NIMS), demonstrated primarily by organizing the IOC in accordance with the Incident Command System (ICS);
- Superb working relationships with external agencies, especially Cumberland County, Pennsylvania;

- Significant progress since the seminar in improving the garrison's AT/FP posture through designating a battle captain, effective use of intelligence capability, and refinements to achieving a common operating picture within the IOC.[84]

Challenges the garrison must recognize and attempt to mitigate were also identified during Team IFPEX's facilitated hot wash and AAR discussions:

- The IOC needs to be relocated into a larger room to optimize its functionality during emergency situations;
- A lack of military resources available to the garrison for FP requirements [Carlisle Barracks does not have any large troop units in residence, only the senior officer students attending the War College.];
- Close proximity of the local community to installation facilities [Carlisle Barracks is immediately adjacent to the town of Carlisle—there is no stand-off distance between installation perimeter and civilian population in town.];
- Carlisle Barracks relies almost exclusively on the surrounding community [Cumberland County] for first response during a crisis.[85]

The decision of the garrison commander to conduct two four-hour exercises proved to be a great benefit to the IOC staff as it had time after the first day's hot wash discussions to make immediate improvements that affected the second day's performance. They were better able to identify and track significant activities and conduct casualty reporting and tracking with more fidelity. Update briefs were more succinct and useful to the commander. Information management was significantly improved and relations with the media were enhanced. Recalling that the garrison had employed war college students in

[84] *IFPEX, U.S. Army Garrison Carlisle Barracks – Final Report*, Enclosure 1.

[85] Ibid.

their IOC in the immediate aftermath of the 9/11 attacks, the garrison now has plans and training procedures in place to formally integrate student volunteers into the IOC when necessary. By the conclusion of the CPX, Carlisle Barracks had demonstrated that it is prepared to respond well to crisis events and Team IFPEX rated the garrison's ability to conduct emergency response operations as 8 out of 10.

4. Impact of IFPEX

In its first 18 months, 40 seminars and 25 CPXs were completed and IFPEX has already proven to be extremely successful as a training program for garrison commanders and their staffs. It has served as a forcing function to help garrisons design (or improve), and staff Installation Operations Centers (IOCs) for emergency response management. It has caused garrisons to develop new, or enhance existing, relationships with municipal first responders, local hospitals, and emergency management planners, as well as with state or regional Emergency Planning and Liaison Officers (EPLOs), Defense Coordinating Officers and Elements (DCOs and DCEs), and other state and federal partners (e.g., public health agencies, state bureaus of investigation, and the FBI), all of whom have a role in supporting the installation, should it suffer an attack or other catastrophic natural or man-made disaster. These relationships have further helped garrisons begin to fulfill the HQDA directive to integrate NIMS and ICS into their emergency response planning by identifying challenges that need to be worked through concerning command and control, resources, and common language and terminology.

Some trends that have been identified as a result of IFPEX include garrison emergency response plans that are not completely executable (usually due to faulty planning assumptions that cannot be realized when tested during an exercise), shortfalls in intelligence analysis capability (garrisons are not currently authorized intelligence analysts, but IFPEX is forcing the issue that they are required, using Carlisle Barracks as one example), lack of equipment to enable communications compatibility among all first responders and the IOC (again,

IFPEX has caused garrisons to look at purchasing radio systems that will facilitate communications among military and municipal fire, police, and other emergency responders and planners), and difficulty in achieving a common operating picture among all participants during a crisis event (IFPEX is prompting garrisons to look at web-based software applications like *WebEOC* to enable information sharing and improve situational awareness among IOC staff, first responders at the incident command post and incident scene, municipal partners, and senior leaders on the installation).

Perhaps the IFPEX trend with the greatest long-term impact for Army installations is one of training. The IFPEX experience uncovered a need for standardized training of directors and other key staff in the Directorate of Plans, Training, Mobilization, and Security (DPTMS) within the garrison staff. Most of those occupying this critical staff position have never been formally trained in their roles and functions. This is not to say that they are inexperienced—far from it. Many have been chiefs of Operations sections during past active duty military careers, or have had some other type of operations experience that qualifies them to perform as a DPTMS director. However, IFPEX has discovered, as evidenced in the many varied ways garrisons conduct emergency operations planning and execution (as well as the other functions of the DPTMS), that there is no place for a current, or up and coming, DPTMS directors to receive specific education and training in this position, so that one might ultimately see emergency operations occurring somewhat similarly at various Army garrisons, much as one would expect to see infantry, armor, or artillery operations being conducted similarly across different brigades throughout the Army. To address this trend, AMSC proposed the development of a two-week course that would provide baseline instruction in all the roles, responsibilities, and functions of the DPTMS director. This proposal was accepted jointly by the Commanding General of IMCOM and the Director of Training for Headquarters, Department of the Army, giving AMSC the green light to proceed. In January 2008, just 62 days after receiving authorization to design the course, AMSC conducted the DPTMS

pilot course to 32 students. The reception given this pilot course by the students was phenomenal, and AMSC recently received funding sponsorship from IMCOM to add this course to its catalog, providing two offerings each fiscal year for 36 students each.

VI. CONCLUSION

The 9/11 attacks, tragic as they were, came with a silver lining of sorts in that the Army has come to recognize and admit openly what it always knew to be true—that fences and guards are not enough to protect its installations against terrorist attack, or against any other natural or man-made disaster, nor do installations have the wherewithal to respond effectively on their own should disaster strike. The doctrine is clear and regulations and policy have been published guiding the Army (and other military services) in providing Civil Support to state and local authorities during times of crisis, although the advent of the Homeland Security mission and cabinet department, as well as the creation of U.S. Northern Command caused this doctrine to be modified slightly over the past five years or so. What is less clear, or more precisely, non-existent, is the doctrine regarding how Army installations would receive and integrate support from local and state officials in response to disasters occurring on the installation.

The DoD perspective regarding the relationships among Homeland Security, Homeland Defense, Civil Support, and Emergency Response has provided the basis for the Army to develop doctrine for its installations in receiving civil support when required. The tendency in the absence of doctrine is for garrison commanders and staffs to fall back on what most of them are comfortable with—their past experience in combat arms or combat support units. This will not work effectively over the long term for Army installations. New doctrine is needed that will, by necessity, be radically different from that used in the tactical Army. Army installations must embrace the new National Response Framework (NRF) and the National Incident Management System (NIMS), and develop its emergency response doctrine around the common language and principles that the Department of Homeland Security has prescribed for all other federal, state, and local entities. This will be a difficult paradigm shift as Army garrisons are organized like other military units, but are expected to function like cities and counties, for indeed that is what the installation is—the Army's hometown.

The Army Management Staff College has been an instrumental catalyst in bringing about the changes necessary for garrisons to be successful in integrating their existing Antiterrorism and Force Protection missions with the Homeland Security concept mandated by the president after the 9/11 attacks. Through its on-campus Command Programs' courses for senior installation leaders and the on-site IFPEX program for garrison staffs, the message is being delivered and understood that while fences are a necessary part of securing an Army installation, they should not be a barrier to effective partnership between the garrison and the local municipal entity. As the IFPEX program matures, one could expect to see more elaborate exercises involving an installation and municipal operations center operating in tandem with an incident command post at the scene of a simulated disaster. One might also see improved communications and coordination of effort and resources between installation and municipality, perhaps even a staff exchange program where persons performing similar functions in each organization switch places for 30 days to help gain a better understanding of how each organization contributes to the success of the other.

Sooner, rather than later, the issue of doctrine must be addressed. The Army Management Staff College, given the proper personnel and resources, would be the proper organization to accomplish this daunting task. As an academic organization, it is removed from the day-to-day operations tempo that has heretofore prevented IMCOM from drafting this doctrine itself. However, the close relationship AMSC has with IMCOM headquarters and the garrisons keeps AMSC well grounded so as to avoid the "ivory tower" mentality that often pervades academic institutions. As this emergency management doctrine is developed, it could be readily evaluated and corrected with the aid of over 100 senior installation leaders that attend AMSC's Command Programs courses each year.

The Army has made great improvements in its force protection posture over the past decade since the Khobar Towers attack and is in the process of integrating homeland security with force protection. In the seventh year since the

9/11 attacks, complacency is one of our greatest threats. This must be countered with continued action and progress, even when an immediate threat is not evident. We would be wise to heed the words of Confucius:

> The superior man, when resting in safety, does not forget that danger may come. When in a state of security he does not forget the possibility of ruin. When all is orderly, he does not forget that disorder may come. Thus his person is not endangered, and his States and all their clans are preserved.[86]

[86] Quote from "The Quotations Page," available on the Internet at http://www.quotationspage.com/subjects/security/ (accessed on March 23, 2008).

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

About USNORTHCOM. From the U.S. Northern Command Internet web site; available on the Internet at http://www.northcom.mil/About/index.html (accessed on March 12, 2008).

Acquisition of information concerning persons and organizations not affiliated with the Department of Defense [DOD Directive 5200.27]. Washington, DC: Under Secretary of Defense for Policy, January 7, 1980. Available on the Internet at http://www.dtic.mil/whs/directives/corres/pdf/520027_010780/520027p.pdf (accessed on February 23, 2007).

Antiterrorism [Army Regulation 525-13]. Washington, DC: Headquarters, Department of the Army, 4 January 2002. Available on the Internet at https://akocomm.us.army.mil/usapa/epubs/dr_pubs/dr_b/pdf/r525_13.pdf?feedAHP=Y (accessed on February 25, 2005).

Arlington County [VA] after-action report on the response to the September 11 terrorist attack on the Pentagon. Available on the Internet at http://www.arlingtonva.us/departments/Fire/edu/about/docs/after_report.pdf (accessed on March 22, 2008).

Army commands, army service component commands, and direct reporting units [Army Regulation 10-87]. Washington, DC: Headquarters, Department of the Army, September 4, 2007. Available on the Internet at http://www.army.mil/usapa/epubs/pdf/r10_87.pdf (accessed on September 20, 2007).

Benedict, Craig. “Army antiterrorism program status.” Unpublished briefing from HQ, Department of the Army, G-3/5/7 (DAMO-ODL), presented at the Garrison Pre-command Course, Army Management Staff College, Fort Belvoir, VA, August 5, 2004.

Burdick, David S. “Antiterrorism critical tasks.” Unpublished lecture slides from Garrison Pre-command Course curriculum (FY02), Army Management Staff College, Fort Belvoir, VA.

———. “Intelligence fusion,” unpublished lecture slides from Garrison Pre-command Course curriculum (FY04), Army Management Staff College, Fort Belvoir, VA.

———. “Introduction to antiterrorism and force protection,” unpublished lecture slides from Garrison Pre-command Course curriculum (FY04), Army Management Staff College, Fort Belvoir, VA.

Cheyne, Barry. “Combat support assessments.” Unpublished briefing from Defense Threat Reduction Agency (DTRA), presented at the Garrison Pre-command Course, Army Management Staff College, Fort Belvoir, VA, October 14, 2004.

Cline, Robert A. (COL). *Operations Group Echo final AAR.* Fort Leavenworth, KS: Battle Command Training Program, US Army Combined Arms Center, April 2002.

DOD antiterrorism handbook [DOD O-2000.12-H]. Washington, DC: Office of the Assistant Secretary of Defense, Special Operations and Low Intensity Conflict, February 9, 2004. Available on the SIPRNET from the Antiterrorism Enterprise Portal (ATEP) at http://www.atep.smil.mil (accessed on January 21, 2005).

Department of Defense homeland defense and civil support joint operating concept. Colorado Springs, CO: U.S. Northern Command (NORTHCOM), October 1, 2007. Available on the Internet at http://www.au.af.mil/au/awc/awcgate/DoD/hls_joc.pdf (accessed on March 2, 2008).

“Fact sheet: strengthening intelligence to better protect America.” Washington, DC: The White House, January 28, 2003. Available on the Internet at http://www.whitehouse.gov/news/releases/2003/01/20030128-12.html (accessed on October 29, 2007).

FY 2002 army antiterrorism program inspection (phase I – active army). Washington, DC: Department of the Army Inspector General, March 6, 2003.

Guttieri, Karen. “Homeland security and U.S. civil-military relations.” *Strategic insights.* Monterey, CA: Naval Postgraduate School Center for Contemporary Conflict, Volume II, Issue 8, August 2003. Available on the Internet at http://www.ccc.nps.navy.mil/si/aug03/homeland.pdf (accessed on March 8, 2008).

Hampton Roads Emergency Management Committee web site home page. Available on the Internet at http://www.hremc.org/ (accessed on January 28, 2008).

Headquarters, Department of the Army execution order (HQDA EXORD) 693-05. *Plan of action for implementation of the national response plan and national incident management system,* 170003Z December 2005.

Homeland security presidential directive 5 (HSPD-5), *Management of domestic incidents,* February 28, 2003. Available on the Internet at http://www.whitehouse.gov/news/releases/2003/02/20030228-9.html (accessed on March 13, 2008).

How the Army runs, a senior leader reference handbook, 2003-2004. Carlisle, PA: U.S. Army War College, 2003. Available on the Internet at http://www.carlisle. army.mil/usawc/dclm/linkedchapters.htm (accessed on December 14, 2004).

"Installation force protection (IFPEX) program." Informational brochure from the Army Management Staff College, November 2007.

Installation force protection exercise (IFPEX), U.S. Army garrison Carlisle Barracks – final report. Fort Belvoir, VA: Army Management Staff College Team IFPEX, March 4, 2008.

Johnson, Ronald L. (Major General). "State of IMA." Unpublished briefing from U.S. Army Installation Management Agency, presented at the Army Garrison Commanders Conference, Fort Bliss, TX, November 16, 2004.

Joint tactics, techniques, and procedures for antiterrorism [Joint Pub 3-07.2]. Washington, DC: Office of the Chairman, Joint Chiefs of Staff, 17 March 1998. Available on the Internet at http://www.dtic.mil/doctrine/jel/ new_pubs/jp3_07_2.pdf (accessed on January 20, 2005).

Kopacki, George. "Your base support resource environment." Unpublished lecture slides from Garrison Pre-command Course curriculum (FY04), Army Management Staff College, Fort Belvoir, VA.

National incident management system [NIMS]. Washington, DC: Department of Homeland Security, March 1, 2004. Available on the Internet at http://www.dhs.gov/xlibrary/assets/NIMS-90-web.pdf (accessed on March 13, 2008).

National infrastructure protection plan. Washington, DC: Department of Homeland Security, 2006. Available on the Internet at http://www.dhs.gov/ xlibrary/assets/NIPP_Plan.pdf (accessed on January 25, 2008).

National response framework. Washington, DC: Department of Homeland Security, January 2008. Available on the Internet at http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf (accessed on February 8, 2008).

National strategy for homeland security. Washington, DC: Homeland Security Council, October 2007. Available on the Internet at http://www.whitehouse.gov/infocus/homeland/nshs/NSHS.pdf (accessed on February 29, 2008).

Pressnell, Rick (Major). “Army antiterrorism program.” Unpublished briefing from HQ, Department of the Army, G-3/5/7 (DAMO-ODL), presented at the Garrison Pre-command Course, Army Management Staff College, Fort Belvoir, VA, September 30, 2003.

Report to the President and Congress on the protection of U.S. forces deployed abroad, annex A: the Downing investigation report. Washington, DC: Headquarters, Department of Defense, August 30,1996. Available on the Internet at http://www.fas.org/irp/threat/downing/report.pdf (accessed on February 25, 2005).

Sakowitz, Philip E. “Army transformation of installation management.” Unpublished information briefing from the U.S. Army Installation Management Agency, presented at the Garrison Pre-command Course, Army Management Staff College, Fort Belvoir, VA, November 19, 2002.

Strategy for homeland defense and civil support. Washington, DC: Department of Defense, June 2005. Available on the Internet at http://www.defenselink.mil/news/Jun2005/d20050630homeland.pdf (accessed on March 9, 2008).

“The revised force protection concept.” Unpublished briefing slides from the Joint Staff, Deputy Directorate for Antiterrorism and Homeland Defense (DD AT/HD), received via e-mail from HQ, Department of the Army, G-3/5/7 (DAMO-ODF), April 7, 2005.

Triggs, Marcia (Sergeant First Class). “Focus: installations to serve as flagships.” *Army News Service* press release, February 3, 2004. Available on the Internet at http://www4.army.mil/ocpa/read.php?story_id_key=5635 (accessed on December 14, 2004).

United States Army antiterrorism and force protection installation commanders’ guide. Washington, DC: Headquarters, Department of the Army, March 2000.

“What we do.” National Counterterrorism Center web site home page. Available on the Internet at http://www.nctc.gov/about_us/what_we_do.html (accessed on October 29, 2007).

Williams, Garland H. (COL). “Welcome to AMSC.” From the Army Management Staff College web page. Available on the Internet at http://www.amsc.belvoir.army.mil/about/ (accessed on March 19, 2008).

Williams, Thomas E. (LTC, Ret.). “The five levels of response.” Unpublished briefing for Army Management Staff College (AMSC) Installation Force Protection Exercise Program (IFPEX) garrison seminar, November 1, 2007.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Commandant
   Army Management Staff College
   Fort Belvoir, Virginia

4. Commanding General
   U.S. Army Installation Management Command
   Arlington, Virginia