

**NAVY WARFARE PUBLICATION**

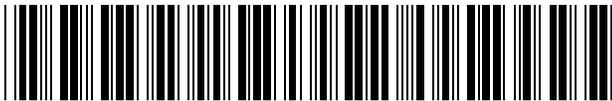
**NAVY DOCTRINE FOR  
ANTITERRORISM / FORCE  
PROTECTION**

**NWP 3-07.2 (REV. A)**

**DEPARTMENT OF THE NAVY  
OFFICE OF THE CHIEF OF NAVAL OPERATIONS**

**DISTRIBUTION RESTRICTION: DISTRIBUTION AUTHORIZED TO THE  
DEPARTMENT OF DEFENSE AND U.S. DOD CONTRACTORS ONLY  
FOR OPERATIONAL USE TO PROTECT TECHNICAL DATA OR  
INFORMATION FROM AUTOMATIC DISSEMINATION (17 MARCH 2004).  
OTHER REQUESTS SHALL BE REFERRED TO NAVY WARFARE  
DEVELOPMENT COMMAND, 686 CUSHING ROAD, NEWPORT, RI  
02841-1207.**

**PRIMARY REVIEW AUTHORITY:  
COMMANDER FLEET FORCES  
COMMAND**



0411LP1032410





DEPARTMENT OF THE NAVY  
NAVY WARFARE DEVELOPMENT COMMAND  
686 CUSHING ROAD  
NEWPORT RI 02841-1207

March 2004

LETTER OF PROMULGATION

1. NWP 3-07.2 (Rev. A), NAVY DOCTRINE FOR ANTITERRORISM/FORCE PROTECTION, is UNCLASSIFIED. Handle in accordance with the administrative procedures contained in NTTP 1-01.
2. NWP 3-07.2 (Rev. A) is effective upon receipt and supersedes NWP 3-07.2, NAVY DOCTRINE FOR ANTITERRORISM/FORCE PROTECTION. Destroy superseded material without report.
3. Distribution Restriction: Distribution authorized to the Department of Defense and U.S. DOD contractors only for operational use to protect technical data or information from automatic dissemination (17 March 2004). Other requests shall be referred to Navy Warfare Development Command, 686 Cushing Road, Newport, RI 02841-1207.
4. SECNAVINST 5510.31 provides procedures for disclosing this publication or portions thereof to foreign governments or international organizations.



JOHN M. KELLY



**PUBLICATION NOTICE**

**ROUTING**

1. NWP 3-07.2 (Rev. A), NAVY DOCTRINE FOR ANTITERRORISM / FORCE PROTECTION, is available in the Navy Warfare Library. It is effective upon receipt.
  
2. General Summary of Changes: NWP 3-07.2 (Rev. A), NAVY DOCTRINE FOR ANTITERRORISM / FORCE PROTECTION, supports the U.S. Navy's increased emphasis on antiterrorism / force protection. It has been significantly updated with specific information on organization, planning and operations.

---

---

---

---

---

---

---

---

---

---

Navy Warfare Library Custodian

Navy Warfare Library publications must be made readily available to all users and other interested personnel within the U.S. Navy.
--

*Note to Navy Warfare Library Custodian*

This notice should be duplicated for routing to cognizant personnel to keep them informed of changes to this publication.







# Navy Doctrine for Antiterrorism / Force Protection

## CONTENTS

*Page  
No.*

### CHAPTER 1 – INTRODUCTION

1.1	PURPOSE.....	1-1
1.2	SCOPE.....	1-1
1.3	DEFINITIONS.....	1-1
1.4	OVERVIEW OF LESSONS LEARNED .....	1-2
1.5	IMPACT ON COMMAND ACCOUNTABILITY .....	1-2
1.6	CONCLUSION.....	1-2

### CHAPTER 2 - TERRORIST THREAT

2.1	OVERVIEW .....	2-1
2.2	DEFINITION OF TERRORISM.....	2-1
2.3	ELEMENTS OF TERRORISTS GROUPS .....	2-1
2.3.1	Ideology .....	2-1
2.3.2	Goals .....	2-2
2.3.3	Characteristics.....	2-2
2.3.4	Organization.....	2-3
2.4	TERRORIST OPERATIONS.....	2-3
2.5	TERRORIST ATTACK PREPARATIONS.....	2-4
2.6	TERRORIST THREAT LEVELS .....	2-4
2.7	FORCE PROTECTION CONDITIONS .....	2-6
2.8	CONCLUSION.....	2-7

**CHAPTER 3 - INTELLIGENCE**

3.1 OVERVIEW ..... 3-1

3.2 DEFINITIONS..... 3-1

3.3 INTELLIGENCE AND TERRORISM ..... 3-1

3.4 ROLES AND RESPONSIBILITIES ..... 3-1

3.4.1 Maritime Intelligence Centers..... 3-2

3.4.2 Joint Intelligence Centers..... 3-3

3.4.3 Naval Counterintelligence..... 3-3

3.5 COMMAND RESPONSIBILITIES ..... 3-4

3.6 CONCLUSION..... 3-5

**CHAPTER 4 - ORGANIZATION AND RESPONSIBILITIES**

4.1 OVERVIEW ..... 4-1

4.2 SECRETARY OF HOMELAND SECURITY ..... 4-1

4.2.1 National Incident Management System ..... 4-1

4.2.2 Incident Command System ..... 4-2

4.3 SECRETARY OF STATE..... 4-2

4.4 SECRETARY OF THE NAVY AND CHIEF OF NAVAL OPERATIONS ..... 4-3

4.5 UNIFIED COMMANDER ..... 4-3

4.6 COMMANDER FLEET FORCES COMMAND..... 4-3

4.7 NAVNORTH..... 4-4

4.8 COMMANDER NAVY INSTALLATIONS..... 4-4

4.9 NAVY REGION COMMANDER AND NUMBERED FLEET COMMANDER ..... 4-4

4.10 INTERAGENCY COORDINATION ..... 4-5

**CHAPTER 5 - ANTITERRORISM / FORCE PROTECTION PLANNING**

5.1 OVERVIEW ..... 5-1

5.2 ASSESSMENT TOOLS ..... 5-1

5.2.1 Internal Assessment Tools ..... 5-1

5.2.2 External Assessment Tools ..... 5-2

5.3 PLANNING PROCESS ..... 5-3

5.3.1 Mission Analysis..... 5-3

5.3.2 Course of Action Development..... 5-3

5.3.3 Course of Action War Gaming ..... 5-3  
 5.3.4 Course of Action Comparison and Selection ..... 5-3  
 5.3.5 ATFP Plan Development ..... 5-3  
 5.3.6 Transition ..... 5-4  
 5.4 POST-INCIDENT RESPONSE PLANNING ..... 5-4  
 5.5 PLANNING PRODUCTS ..... 5-6

**CHAPTER 6 - ANTITERRORISM / FORCE PROTECTION EXECUTION**

6.1 OVERVIEW ..... 6-1  
 6.2 PRE-INCIDENT PREPARATIONS ..... 6-1  
 6.2.1 Threat Analysis ..... 6-1  
 6.2.2 Risk Assessments ..... 6-1  
 6.2.3 ATFP Plan ..... 6-2  
 6.2.4 Baseline Security Posture ..... 6-2  
 6.2.5 Random Antiterrorism Measures ..... 6-2  
 6.2.6 Post-Mission / Deployment Assessments ..... 6-2  
 6.3 INCIDENT RESPONSE ..... 6-2  
 6.4 POST-INCIDENT RESPONSE ..... 6-3  
 6.4.1 Phases of Post-Incident Response ..... 6-3  
 6.4.2 Post-Incident Command and Control ..... 6-4  
 6.5 CHEMICAL / BIOLOGICAL / RADIOLOGICAL / NUCLEAR / EXPLOSIVE  
 CRISIS AND CONSEQUENCE MANAGEMENT ..... 6-6

**CHAPTER 7 - LEGAL CONSIDERATIONS**

7.1 OVERVIEW ..... 7-1  
 7.2 DEFINITIONS ..... 7-1  
 7.3 SELF-DEFENSE ..... 7-2  
 7.3.1 Self-Defense within the United States and Its Territories ..... 7-3  
 7.3.2 Naval Vessel Protective Zone ..... 7-4  
 7.3.3 Self-Defense outside of the United States ..... 7-4

# LIST OF ILLUSTRATIONS

*Page  
No.*

## **CHAPTER 2 – TERRORIST THREAT**

Figure 2-1	Terrorist Threat Level Assessment Criteria.....	2-5
Figure 2-2	Force Protection Conditions .....	2-6

## **CHAPTER 3 – INTELLIGENCE**

Figure 3-1	Support for Unit-Specific Intelligence Needs.....	3-2
------------	---	-----

## **CHAPTER 6 – ANTITERRORISM / FORCE PROTECTION EXECUTION**

Figure 6-1	Post-Incident Command and Control .....	6-5
------------	---	-----

# BIBLIOGRAPHY

These publications were used as references during the production of this NWP and the associated NTTP 3-07.2.1 (Rev. A), Antiterrorism / Force Protection.

## DEPARTMENT OF DEFENSE PUBLICATIONS

DOD O-2000.12-H, Protection of DOD Personnel and Activities against Acts of Terrorism and Political Turbulence.

DODD 2000.12 (series), DOD Antiterrorism (AT) Program.

DODD 5200.8 (series), Security of Military Installations and Resources.

DODD 5210.56 (series), Use of Deadly Force and the Carrying of Firearms by DOD Personnel Engaged in Enforcement and Security Duties.

DODI 2000.16 (series), DOD Antiterrorism (AT) Standards.

DODI 5210.84 (series), Security of DOD Personnel at U.S. Missions Abroad.

## JOINT PUBLICATIONS

CJCSI 3121.01A, Standing Rules of Engagement for U.S. Forces.

CJCSI 5261.01 (series), Combating Terrorism Readiness Initiatives Fund.

Joint Chiefs of Staff Deputy Directorate of Operations for Combatting Terrorism (J-34) Installation Antiterrorism Program and Planning Tool, Volumes I and II.

JP 3-07 (series), Joint Doctrine for Military Operations Other than War.

JP 3-07.2 (series), Joint Tactics, Techniques, and Procedures (JTTP for Antiterrorism).

JP 3-10.1 (series), Joint Tactics, Techniques, and Procedures for Base Operations.

JP 3-26 (series), Joint Doctrine for Homeland Security.

## NAVY PUBLICATIONS

NTTP 3-07.3.2 (series), Navy Tactics, Techniques, and Procedures for Tactical Employment of Nonlethal Weapons.

NWP 1-14M (series), The Commander's Handbook on the Law of Naval Operations

NWP 5-01 (series), Naval Operational Planning.

OPNAVINST 3300.53 (series), Navy Combatting Terrorism Program.

## **NWP 3-07.2 (Rev. A)**

OPNAVINST 3300.54 (series), Protection of Naval Personnel and Activities against Acts of Terrorism and Political Turbulence.

OPNAVINST 3300.55 (series), Navy Combatting Terrorism Program Standards.

OPNAVINST 3500.39 (series), Operational Risk Management.

OPNAVINST 3591.1 (series), Small Arms Training and Qualification.

OPNAVINST 5530.13 (series), Department of the Navy Physical Security Instruction for Conventional Arms, Ammunition and Explosives.

OPNAVINST 5530.14 (series), Navy Physical Security.

SECNAVINST 3300.3 (series), Combating Terrorism Program Standards.

SECNAVINST 5500.29 (series), Use of Deadly Force and the Carrying of Firearms by Personnel of the Department of the Navy in Conjunction with Law Enforcement, Security Duties, and Personal Protection.

SECNAVINST 5510.36 (series), Department of the Navy Information Security Program Regulation.

SECNAVINST 5520.3 (series), Criminal and Security Investigations and Related Activities within the Department of the Navy.

# GLOSSARY

## A

**antiterrorism.** Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military forces. The antiterrorism program is one of several security-related programs that fall under the overreaching Force Protection and Combating Terrorism programs. An antiterrorism program is a collective effort that seeks to reduce the likelihood that Department of Defense personnel, their families, facilities and material will be subject to a terrorist attack, and to prepare a response to the consequences of such attacks if they occur.

**antiterrorism awareness.** Fundamental knowledge of the terrorist threat and measures to reduce personal vulnerability to terrorism.

**antiterrorism / force protection plan.** A plan that documents the specific measures taken to establish and maintain an antiterrorism / force protection program, ensuring readiness against terrorist attacks.

**antiterrorism officer.** The point of contact directly responsible to the Commanding Officer for all matters dealing with antiterrorism and force protection. Previously known as the Force Protection Officer.

**area of responsibility.** 1) The geographical area associated with a combatant command within which a combatant commander has authority to plan and conduct operations. 2) In naval usage, a predefined area of enemy terrain for which supporting ships are responsible for covering by fire on known targets or targets of opportunity and by observation.

## B

**blue dart message.** Time-sensitive terrorist incident notification message. Initiated by the Multiple Alert Threat Center to provide commands immediate indications and warning of the high potential for, and imminent threat of, a terrorist incident.

## C

**combatting terrorism.** Actions, including antiterrorism (defensive measures taken to reduce vulnerability to terrorist acts) and counterterrorism (offensive measures taken to prevent, deter and to respond to terrorism), terrorism consequence management (preparation for and response to the consequences of a terrorist incident / event) and intelligence support (collection and dissemination of terrorism related information) taken to oppose terrorism throughout the entire threat spectrum, to include terrorist use of chemical, biological, radiological, nuclear materials or high-yield explosive devices.

**consequence management.** Interagency services and emergency response force actions essential to mitigate and recover from damage, loss, hardship or suffering resulting from disasters or catastrophes, either manmade or natural.

## **NWP 3-07.2 (Rev. A)**

**counterintelligence.** Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, foreign persons or international terrorist activities.

**crisis management.** Measures taken to anticipate, prevent, resolve and / or contain a terrorist threat or incident; it may subsequently include a follow-on investigation and preparation of legal proceedings.

### **D**

**defense in depth.** The siting of mutually supporting defense positions designed to absorb and progressively weaken attack, prevent initial observations of the whole position by the enemy and to allow the commander to maneuver the reserve.

**deterrence.** The prevention from action by fear of the consequences. Deterrence is a state of mind brought about by the existence of a credible threat of unacceptable counteraction.

### **E**

**explosive ordnance disposal.** The detection, identification, on-site evaluation, rendering safe, recovery and final disposal of unexploded explosive ordnance. It may also include explosive ordnance that has become hazardous by damage or deterioration.

### **F**

**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, personal protective services and supported by intelligence, counterintelligence and other security programs.

**force protection conditions.** A Chairman of the Joint Chiefs of Staff-approved program standardizing the military services' identification of and recommended responses to terrorist threats and terrorist acts against U.S. personnel and facilities. This program facilitates interservice coordination and support for AT activities.

### **H**

**host nation.** A nation that receives the forces and / or supplies of allied nations and / or NATO organizations to be located on, to operate in or to transit through its territory.

**host nation support.** Civil and / or military assistance rendered by a nation to foreign forces within its territory during peacetime, crises or emergencies or war based on agreements mutually concluded between nations.

### **I**

**improvised explosive device.** A device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic or incendiary chemicals and designed to destroy, incapacitate, harass or distract. It may incorporate military stores but is normally devised from nonmilitary components.

**installation.** A grouping of facilities, located in the same vicinity, that support particular functions. Installations may be elements of a base.

**installation commander.** The individual responsible for all operations performed by an installation.

**intelligence.** 1) The product resulting from the collection, processing, integration, analysis, evaluation and interpretation of available information concerning foreign countries or areas. 2) Information and knowledge about an adversary obtained through observation, investigation, analysis or understanding.

## L

**law enforcement agency.** Any of a number of agencies including those within the Department of Defense and the Department of the Navy, chartered and empowered to enforce laws in the following jurisdictions: the United States, a state (or political subdivision) of the United States, a territory or possession (or political subdivision) of the United States or to enforce U.S. laws within the borders of a host nation.

**lead agency.** Designated among U.S. Government agencies to coordinate the interagency oversight of the day-to-day conduct of an ongoing operation. The lead agency is to chair the interagency working group established to coordinate policy related to a particular operation. The lead agency determines the agenda, ensures cohesion among the agencies and is responsible for implementing decisions.

**level I antiterrorism training.** Level I training is awareness training. It is provided to all DOD personnel accessions during initial training to include: military, DOD civilians, their family members 14 years old and greater (when family members are deploying or traveling on government orders) and DOD-employed contractors.

**level II antiterrorism training.** Level II training is designed to provide training for officers, non-commissioned officers and civilian staff personnel who are designated to serve as antiterrorism advisors to the commander.

## M

**memorandum of understanding.** A document that specifies actions and responsibilities to be performed by the provider and receiver but only in general terms. An MOU should be backed by an Interservice Support Agreement.

## N

**naval vessel protective zone.** A United States Coast Guard regulation that states: (a) all vessels within 500 yards of a U.S. Naval vessel shall operate at the minimum speed necessary to maintain a safe course and shall proceed as directed by the official patrol (senior naval or Coast Guard officer present), (b) no vessel is allowed within 100 yards of a U.S. naval vessel, (c) vessels requesting to pass within 100 yards of a US naval vessel shall contact official patrol on VHF Channel 16 and follow their direction, (d) commercial vessels at anchor may remain at anchor if a naval vessel passes them within 100 yards and (e) violations of the Naval Vessel Protection Zone are felonies, punishable by up to six years in prison and fines up to \$250,000.

**P**

**physical security.** That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material and documents; and to safeguard them against espionage, sabotage, damage and theft.

**port security.** The safeguarding of vessels, harbors, ports, waterfront facilities and cargo from internal threats such as destruction, loss, or injury from sabotage or other subversive acts, accidents, thefts or other causes of a similar nature.

**R**

**random antiterrorism measures.** Random, multiple security measures that when activated, serve to disguise the actual security procedures in effect; RAMs deny the terrorist surveillance team the opportunity to accurately predict security actions. RAMs strictly vary the time frame and / or location for a given measure.

**risk assessment.** The identification and assessments of hazards (first two steps of risk management process).

**risk management.** A process by which decision makers reduce or offset risk.

**S**

**status of forces agreement.** An agreement that defines the legal position of a visiting military force deployed in the territory of a friendly state. Agreements delineating the status of visiting military forces may be bilateral or multilateral. Provisions pertaining to the status of visiting forces may be set forth in a separate agreement, or they may form a part of a more comprehensive agreement. These provisions describe how the authorities of a visiting force may control members of that force and the amenability of the force or its members to the local law or to the authority of local officials. To the extent that agreements delineate matters affecting the relations between a military force and civilian authorities and population, they may be considered as civil affairs agreements.

**T**

**terrorist threat level.** An intelligence threat assessment of the level of terrorist threat faced by U.S. personnel and interests in a foreign country. The assessment is based on a continuous intelligence analysis of a minimum of five elements: terrorist group existence, capability, history, trends and targeting. There are four threat levels: Low, Moderate, Significant and High. Threat levels should not be confused with Force Protection Conditions. Threat level assessments are provided to senior leaders to assist them in determining the appropriate local force protection condition (Department of State also makes threat assessments that may differ from those determined by Department of Defense).

**threat assessment.** The continual process of compiling and examining all available information concerning potential terrorist activities by terrorist groups that could target a facility. A threat assessment will review the factors of a terrorist group's existence, capability, intentions, history and targeting, as well as the security environment within which friendly forces operate. Threat assessment is an essential step in identifying the probability of terrorist attack.

V

**vulnerability assessment.** A self-assessment tool. The installation, base, ship, unit or port uses the VA to evaluate its physical security plans, programs and structures relative to a terrorist attack. Examples include Joint Staff Integrated Vulnerability Assessment, Chief of Naval Operations Integrated Vulnerability Assessment, Port Integrated Vulnerability Assessment, Airfield Integrated Vulnerability Assessment, Naval Facilities Engineering Command's Risk and Vulnerability Analysis and higher headquarter assessments.

# ACRONYMS AND ABBREVIATIONS

## A

<b>AOR</b>	area of responsibility
<b>ASF</b>	auxiliary security force
<b>AT</b>	antiterrorism
<b>ATFP</b>	antiterrorism / force protection
<b>ATFPTS</b>	antiterrorism / force protection training supervisor
<b>ATO</b>	antiterrorism officer
<b>ATTO</b>	antiterrorism training officer
<b>ATTWO</b>	antiterrorism tactical watch officer

## C

<b>C2</b>	command and control
<b>C3</b>	command, control and communications
<b>C4I</b>	command, control, communications, computers and intelligence
<b>CBRNE</b>	chemical, biological, radiological, nuclear high-yield explosives
<b>CDO</b>	command duty officer
<b>CNI</b>	Commander Navy Installations
<b>CNOIVA</b>	Chief of Naval Operations integrated vulnerability assessment
<b>CO</b>	commanding officer
<b>COA</b>	course of action
<b>COCOM</b>	combatant commander
<b>COG</b>	chief of the guard
<b>CONOPS</b>	concept of operations
<b>CONUS</b>	continental United States
<b>C / V</b>	criticality and vulnerability

**D**

<b>DHS</b>	Department of Homeland Security
<b>DOD</b>	Department of Defense
<b>DOJ</b>	Department of Justice
<b>DON</b>	Department of the Navy
<b>DOS</b>	Department of State

**E**

<b>EOC</b>	emergency operations center
<b>ECP</b>	entry control point
<b>EOD</b>	explosive ordnance disposal
<b>EODMU</b>	explosive ordnance disposal mobile unit

**F**

<b>FAST</b>	fleet antiterrorism security team
<b>FBI</b>	Federal Bureau of Investigation
<b>FEMA</b>	Federal Emergency Management Agency
<b>FP</b>	force protection
<b>FPCON</b>	force protection condition
<b>FPTT</b>	force protection training team
<b>FRP</b>	Federal Response Plan

**H**

<b>HAZMAT</b>	hazardous material
<b>HN</b>	host nation
<b>HVA</b>	high value asset

**I**

<b>I&amp;W</b>	indications and warnings
<b>ICS</b>	incident command system

**NWP 3-07.2 (Rev. A)**

**IED** improvised explosive device

**IFE** individual protection equipment

**ISIC** immediate superior in command

**J**

**JSIVA** Joint Staff integrated vulnerability assessment

**L**

**LFA** lead Federal agency

**M**

**MANPAD** man-portable air defense system

**MTAC** multiple threat alert center

**MWD** military working dog

**N**

**NATO** North Atlantic Treaty Organization

**NCIS** Naval Criminal Investigative Service

**NIMS** National Incident Management System

**NLLS** Navy Lessons Learned System

**NRP** National Response Plan

**NSF** Navy security force

**NTTP** Navy tactics, techniques and procedures

**NVD** night vision device

**NVPZ** naval vessel protective zone

**NWDC** Navy Warfare Development Command

**NWP** Navy Warfare Publication

**O**

**OCONUS** outside the continental United States

**OOD** officer of the deck

**ORIGINAL**

<b>OPCON</b>	operational control
<b>OPLAN</b>	operation plan
<b>OPNAV</b>	Chief of Naval Operations
<b>OPNAVINST</b>	Chief of Naval Operations instruction
<b>OPSEC</b>	operations security
<b>ORM</b>	operational risk management
<b>OSC</b>	on-scene commander

**P**

<b>PIR</b>	priority intelligence requirement
<b>PIVA</b>	port integrated vulnerability assessment
<b>PPR</b>	preplanned response

**R**

<b>RAM</b>	random antiterrorism measure
<b>RFI</b>	request for information
<b>ROC</b>	region operations center
<b>ROE</b>	rules of engagement
<b>RPG</b>	rocket-propelled grenade
<b>RUF</b>	rules for use of force

**S**

<b>SCIO</b>	staff counterintelligence officer
<b>SECNAVINST</b>	Secretary of the Navy instruction
<b>SIPRNET</b>	Secret Internet Protocol Router Network
<b>SMEAC</b>	situation, mission, execution, administration, command and control
<b>SOFA</b>	status-of-forces agreement
<b>SOP</b>	standard operating procedure
<b>SORM</b>	standard organization regulations manual

**NWP 3-07.2 (Rev. A)**

**SROE** standing rules of engagement

**T**

**TA** threat assessment

**TTP** tactics, techniques and procedures

**TYCOM** type commander

**U**

**USCG** United States Coast Guard

**USDAO** United States Defense Attaché Office

**V**

**VAMP** vulnerability assessment management program

**W**

**WMD** weapons of mass destruction

# PREFACE

NWP 3-07.2 (Rev. A), Navy Doctrine for Antiterrorism / Force Protection, provides guidance to establish and maintain antiterrorism / force protection programs that deter, detect, defend against, mitigate and recover from the consequences of terrorist attacks against U.S. Navy forces. This publication should be used in conjunction with NTTP 3-07.2.1 (Rev. A), Antiterrorism / Force Protection.

Throughout this publication, references to other publications imply the effective edition.

Report any page shortage by letter to Commander, Navy Warfare Development Command.

## ORDERING DATA

Order a new publication or change, as appropriate, through the Navy supply system.

Changes to the distribution and allowances lists (to add or delete a command from the distribution list, or to modify the number of copies of a publication that is received) must be made in accordance with NTTP 1-01.

## RECOMMENDED CHANGES

Recommended changes to this publication may be submitted at any time using the accompanying format for routine changes.

Fleet units and stations submit recommendations through the chain of command to:

OFFICE OF THE CHIEF OF NAVAL OPERATIONS–N34  
2000 NAVY PENTAGON  
WASHINGTON, DC 20350-2000

In addition, forward two copies of all recommendations to:

COMMANDER  
NAVY WARFARE DEVELOPMENT COMMAND  
686 CUSHING ROAD  
NEWPORT, RI 02841-1207

## WEB-BASED CHANGE SUBMISSIONS

Recommended change submissions for this publication may be submitted to the Navy doctrine discussion group site. This discussion group may be accessed through the Navy Warfare Development Command SIPRNET website at <http://www.nwdc.navy.smil.mil/>.

(CLASSIFICATION)			
<b>RECOMMENDED CHANGE TO:</b> _____ <small>(PUBLICATION NUMBER / REVISION / CHANGE)</small>	<b>DATE:</b> _____		
<b>LOCATION:</b> _____ <small>(PAGE) (PARA) (LINE) (FIG. NO.)</small>			
<b>TYPE OF CHANGE:</b> <table border="1" style="width: 100%; border-collapse: collapse;"><tr><td style="width: 50%;">ADD ____ DELETE ____ MODIFY ____</td><td style="width: 50%;">TEXT ____ FIGURE ____</td></tr></table>		ADD ____ DELETE ____ MODIFY ____	TEXT ____ FIGURE ____
ADD ____ DELETE ____ MODIFY ____	TEXT ____ FIGURE ____		
<b>EXACT CHANGE RECOMMENDED:</b> USE ADDITIONAL SHEETS IF NEEDED. GIVE VERBATIM TEXT CHANGES IF FIGURE IS TO BE ADDED. SUPPLY ROUGH SKETCH OR IDENTIFY SOURCE. IF FIGURE IS TO BE CHANGED, INCLUDE A MARKED UP COPY OF EXISTING FIGURE.			
<b>RATIONALE:</b>			
<b>SUBMITTED BY:</b>			
_____ <small>(ORIGINATING COMMAND)</small>	_____ <small>(ORIGINATOR SEQUENCE NO.)</small>		
_____ <small>(POINT OF CONTACT)</small>	_____ <small>(PHONE - IDENTIFY DSN OR COMM)</small>		
<b>PRA ACTION:</b> ACCEPTED _____ MODIFIED _____ REJECTED _____			
<b>REMARKS:</b> (USE ADDITIONAL SHEETS IF NEEDED)			
_____ <small>(PRA POINT OF CONTACT)</small>	_____ <small>(PHONE - IDENTIFY DSN OR COMM)</small>		
<b>CONFERENCE DATE:</b> _____ <b>CONFERENCE AGENDA ITEM NO.:</b> _____			
PAGE _____ OF _____			
(CLASSIFICATION)			

FM ORIGINATOR

TO PRA COMMAND PLAD//JJJ//

INFO COMNAVWARDEVCOM NEWPORT RI//N5//

NAVWARCOL NEWPORT RI//213//

*Others as appropriate*

BT

CLASSIFICATION//NO3510//

MSGID/GENADMIN/(*Organization ID*)//

SUBJ/URGENT CHANGE RECOMMENDATION FOR NWP 3-07.2 (REV. A)//

REF/A/DOC/NWDC//

AMPN/REF A IS NTTP 1-01 (REV. B), THE NAVY WARFARE LIBRARY//

POC/(*Command Representative*)//

RMKS/1. IAW REF A URGENT CHANGE IS RECOMMENDED FOR NWP 3-07.2 (REV. A)

2. PAGE \_\_\_\_\_ ART/PARA NO \_\_\_\_\_ LINE NO \_\_\_\_\_ FIG NO \_\_\_\_\_

3. PROPOSED NEW TEXT (*Include classification*)

4. JUSTIFICATION.

BT

*Message provided for subject matter; ensure that actual message conforms to MTF requirements.*

## **URGENT CHANGE RECOMMENDATIONS**

When items for changes are considered to be urgent (as defined in NTTP 1-01, and including matters of safety), this information shall be sent by message (see accompanying sample message format) to the primary review authority, with information copies to Navy Warfare Development Command, and all other commands concerned, clearly explaining the proposed change. Information addresses should comment as appropriate. See NTTP 1-01 for additional guidance.

## **CHANGE SYMBOLS**

Revised text in changes is indicated by a black vertical line in the outside margin of the page, like the one printed next to this paragraph. The change symbol shows where there has been a change. The change might be added material or restated information. A change symbol in the outside margin by the chapter number and title indicates a new or completely revised chapter.

## **WARNINGS, CAUTIONS AND NOTES**

The following definitions apply to “WARNINGS,” “CAUTIONS” and “Notes” found throughout the manual.



### **WARNING**

An operating procedure, practice or condition that may result in injury or death if not carefully observed or followed.



### **CAUTION**

An operating procedure, practice or condition that may result in damage to equipment if not carefully observed or followed.

### **Note**

An operating procedure, practice or condition that is essential to emphasize.

## **WORDING**

The concept of word usage and intended meaning that has been adhered to in preparing this publication is as follows:

“Shall” has been used only when application of a procedure is mandatory.

“Should” has been used only when application of a procedure is recommended.

“May” and “need not” have been used only when application of a procedure is optional.

“Will” has been used only to indicate futurity, never to indicate any degree of requirement for application of a procedure.

# CHAPTER 1

## Introduction

### 1.1 PURPOSE

NWP 3-07.2 (Rev. A) provides guidance to:

1. Establish and maintain unit antiterrorism / force protection (ATFP) programs that deter, detect, defend, mitigate and recover from the consequences of terrorist attacks via the implementation of coherent baseline security measures.
2. Defeat an attack by the activation of preplanned responses.
3. Take required actions to manage a crisis and maintain / regain mission readiness.

### 1.2 SCOPE

This NWP is applicable to all U.S. Navy afloat, aviation and shore commands, within U.S. or foreign territory and in transit. It is also applicable to U.S. Coast Guard units while operating under Navy operational control and at any time the U.S. Coast Guard is operating as a specialized service within the Department of the Navy.

DOD Directive 2000.12 (series), Department of Defense (DOD) Antiterrorism (AT) Program, sets the requirement for Navy-wide ATFP programs. NWP 3-07.2 (Rev. A) complies with ATFP guidance and directives from the DOD, Joint Staff and Department of the Navy. Detailed topical ATFP guidance can be found in companion publications NTTP 3-07.2.1 (Rev. A), Navy Tactics, Techniques, and Procedures for Antiterrorism / Force Protection, NTRP 3-07.2.2, Navy Tactical Reference Publication for Force Protection Weapons Handling Standard Procedures and Guidelines and NTTP 3-07.3.2, Navy Tactics, Techniques, and Procedures for Tactical Employment of Non-Lethal Weapons.

### 1.3 DEFINITIONS

The following definitions are provided to assist in understanding the scope of antiterrorism and force protection:

**Terrorism:** The calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious or ideological. Joint Publication (JP) 1-02, DOD Dictionary of Military and Associated Terms

**Antiterrorism:** Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military forces. (JP 1-02)

**Force Protection:** 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. (JP 1-02)

## **1.4 OVERVIEW OF LESSONS LEARNED**

The following notable terrorist attacks against U.S. forces revealed weaknesses in force protection efforts and led to a renewed focus on preparing and implementing dynamic ATFP programs:

1. Attack on the Marine headquarters in Beirut, 23 October 1983. The Long Commission report stated: "Preattack security was found to be neither commensurate with the threat nor sufficient to preclude the disaster."
2. Attack on Khobar Towers, Dhahran, Saudi Arabia, 25 June 1996. The Downing Assessment Task Force made the following observation: "Certainly, our level of awareness of the terrorist threat has been heightened after this attack. However, much remains to be accomplished to ensure that our units stationed overseas make this heightened awareness part of their daily routine."
3. Attack on USS Cole (DDG 67) in the port of Aden, Yemen, 12 October 2000. The USS Cole Commission Report found: "The attack on the USS Cole (DDG 67) in the port of Aden, Yemen, on 12 October 2000 demonstrated a seam in the fabric of efforts to protect our forces, namely in-transit forces."

## **1.5 IMPACT ON COMMAND ACCOUNTABILITY**

Protection of personnel and assets are an implied task for every commander. ATFP considerations must be embedded in every facet of day-to-day operations.

Commanders at all levels must:

1. Establish and maintain a baseline security posture that affords their personnel and assets a level of security that is commensurate with their criticality and threat.
2. Develop preplanned responses for likely terrorist acts.
3. Be prepared to respond to terrorist acts and take appropriate action to maintain and / or regain mission readiness.

## **1.6 CONCLUSION**

As acts of terrorism increasingly become the preferred tactic used by groups unwilling or unable to directly challenge U.S. military strength, Navy forces must be aware of vulnerabilities, organize and deploy security forces and maintain constant situational awareness. The same degree of focus, intensity, preparation and training afforded traditional warfare areas is now required to ensure success in the fight against terrorism.

# CHAPTER 2

## Terrorist Threat

### 2.1 OVERVIEW

Since the bombing of the Marine barracks in Beirut, Lebanon, in 1983, the U.S. military has suffered more casualties from acts of terrorism than in combat operations. Although U.S. military strength is unmatched in the world, U.S. forces are committed to more unfamiliar environments than at any time in U.S. history because of widespread political instability around the world. Rogue states and other opponents of U.S. policy who cannot otherwise challenge U.S. military power can and do attack vulnerabilities of U.S. forces, seeking to erode military effectiveness and morale.

Acts of terrorism can significantly impact U.S. interests and policy. Terrorists have many advantages—they choose the battlefield, the target, the time and the level of the conflict. In many instances the target is not even aware of its status as a target. Military personnel, facilities and material, as identifiable symbols of the U.S. Government, are choice targets for terrorists seeking to change U.S. government policies at home or abroad.

The purpose of this chapter is to provide background information about terrorist groups, tactics and methodology that will assist commanders with creating and implementing effective antiterrorism / force protection (ATFP) programs and plans.

### 2.2 DEFINITION OF TERRORISM

Joint Publication 1-02, Department of Defense (DOD) Dictionary of Military and Associated Terms, defines terrorism as “the calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious or ideological.”

Terrorism’s “tools of the trade” are thus psychologically acute, meticulously planned well in advance and designed to induce unrest over a long period of time.

### 2.3 ELEMENTS OF TERRORIST GROUPS

All terrorist groups have ideologies, goals, particular characteristics and some form of structure or organization.

#### 2.3.1 Ideology

Ideology is a set of doctrines or beliefs that form the basis of a political, social, economic or other system that reflect the needs and aspirations of an individual, group, class or culture. Types of ideologies include:

1. Politics (i.e., Marxism-Leninism, fascism)
2. Nationalism (i.e., Irish Republican Army)
3. Religion (i.e., al Qaeda, Islamic Jihad)
4. Special interest (i.e., Earth Liberation Front, animal-rights groups).

### **2.3.2 Goals**

Terrorist groups set both immediate and long-range goals. Before a group or insurgent movement can make a viable bid for power or hope to seriously influence a government's long-term policy, it must achieve minor victories and accomplish some immediate goals. Each act of terrorism is designed to accomplish something specific as part of an overall strategy. Immediate or short-term goals usually include one or more of the following:

1. Recognition
2. Elimination of Western influence
3. Harassment, weakening or embarrassment of governments
4. Attainment of money or equipment
5. Destruction of facilities and disruption of communications
6. Discouraging foreign investors
7. Influence in government decisions
8. Freedom of prisoners
9. Satisfying vengeance.

### **2.3.3 Characteristics**

Although some terrorist groups have achieved a high level of military sophistication and are heavily armed, they typically choose to employ hit-and-run guerrilla tactics. Most terrorists will not choose to take up a static defensive posture against a stronger enemy unless they possess a "bargaining chip" such as hostages. Above all, terrorist group leaders do not want to risk losing organization members because of perceived weakness. Terrorist organizations are also typically:

1. **Urban-based.** An urban environment offers access to transportation, money-laundering mechanisms, communications systems and international contacts who can provide required travel documentation.
2. **Highly mobile.** Terrorists typically move frequently among cities and countries, not only to facilitate the planning and execution of operations, but also in search of safe havens and like-minded support.
3. **Well-trained.** In order to instill individual members with a strong desire for success, including a willingness to die for the cause, terrorist groups train and rehearse extensively. Emphasis is on physical conditioning, effective use of weapons and explosives, tactics and combat techniques, clandestine operations, psychological warfare and survival skills.
4. **Covert.** Although some groups (i.e., the Popular Front for the Liberation of Palestine) have overt political contingents, the operational cells of most terrorist groups can operate in covert postures for extended periods. While this clandestine nature contributes to their flexibility and effectiveness, it also requires terrorist groups to maintain and support intricate operational systems, complete with personnel and assets.

### 2.3.4 Organization

The basic operational unit of a terrorist group is the cell. The size of a cell is determined by its mission or function. For example, a cell organized to construct improvised explosive devices (IEDs) may consist of no more than one or two IED-trained members. Conversely, a cell tasked to organize the kidnapping of a dignitary will include a larger number of operatives because of the mission's complexity.

Cells normally found in well-organized terrorist groups include:

1. **Planning and Preparation Cell.** Once a target has been selected, the planning and preparation cell is tasked with formulating the operational plan.
2. **Administration and Logistics Cell.** This cell is often made up of professional people, such as lawyers, doctors, bankers and food handlers, who, while dedicated to the ideals of the group, are not willing to sacrifice their personal (or professional) status by taking direct action. This cell can, however, provide financial resources.
3. **Intelligence and Surveillance Cell.** This cell - the eyes and ears of the terrorist group - performs reconnaissance and surveillance of potential targets; the data gathered by the intelligence and surveillance team enhances operational planning.
4. **Operations Combat Cell.** The operations combat team is the action cell of the terrorist group, whose function is to conduct all combat operations for the group. Team members typically include bombers, shooters and assassins.

## 2.4 TERRORIST OPERATIONS

Once an intended target's weaknesses and vulnerabilities are known, terrorists select the best tactics to exploit them. Common terrorist methods include:

1. Assassination
2. Arson
3. Bombing
4. Hostage taking
5. Kidnapping
6. Hijacking or skyjacking
7. Seizure of important buildings or assets
8. Raids or attacks on facilities
9. Sabotage
10. Employment of weapons of mass destruction
11. Information warfare.

## **2.5 TERRORIST ATTACK PREPARATIONS**

Generally speaking, terrorist attacks do not just happen—they are well-planned events that seek to exploit perceived weaknesses in the target.

1. **Target options.** Choosing a target typically starts with a self-assessment of the terrorist group's capabilities, which will, in large part, define the methods of attack available to the group. After determining the objective (i.e., what they want to achieve), the terrorist group will develop a list of potential targets.
2. **Selection surveillance.** Data gathered from watching potential targets will help the terrorist group refine the list of choices. A potential target may be de-selected because surveillance data proves the choice to be too difficult to effectively attack.
3. **Target selection.** Once surveillance data results are assessed, terrorists are able to select their target or set of targets. The most likely targets are those that are vulnerable, undefended or with weak security.
4. **Detailed surveillance.** Terrorists often conduct further long-term, detailed surveillance of the chosen potential target(s), seeking to detect routines, procedures and site-specific security measures. An effective countersurveillance program is one that will detect such patterns of surveillance, alerting the target of an impending attack.
5. **Training and preparation.** Once the terrorists' plan of attack has been developed, the attack team will be chosen and trained. Attack teams are typically kept to the minimum effective number to ensure secrecy.
6. **Attack.** Terrorists wait for the right set of circumstances to attack, which can take months or even years. If, during this time, there is a change in the potential target's routine or level of security, the attack profile will also change, causing the terrorist mission to be delayed or scrapped.

## **2.6 TERRORIST THREAT LEVELS**

The DOD-developed methodology used to assess current terrorist threats to DOD personnel, material and interests is based on analysis of a combination of threat factors. The terrorist threat level for a particular area is determined by the presence or absence of threat factors. The Defense Intelligence Agency (DIA) and the unified commander may issue terrorism threat level assessments (see Figure 2-1).

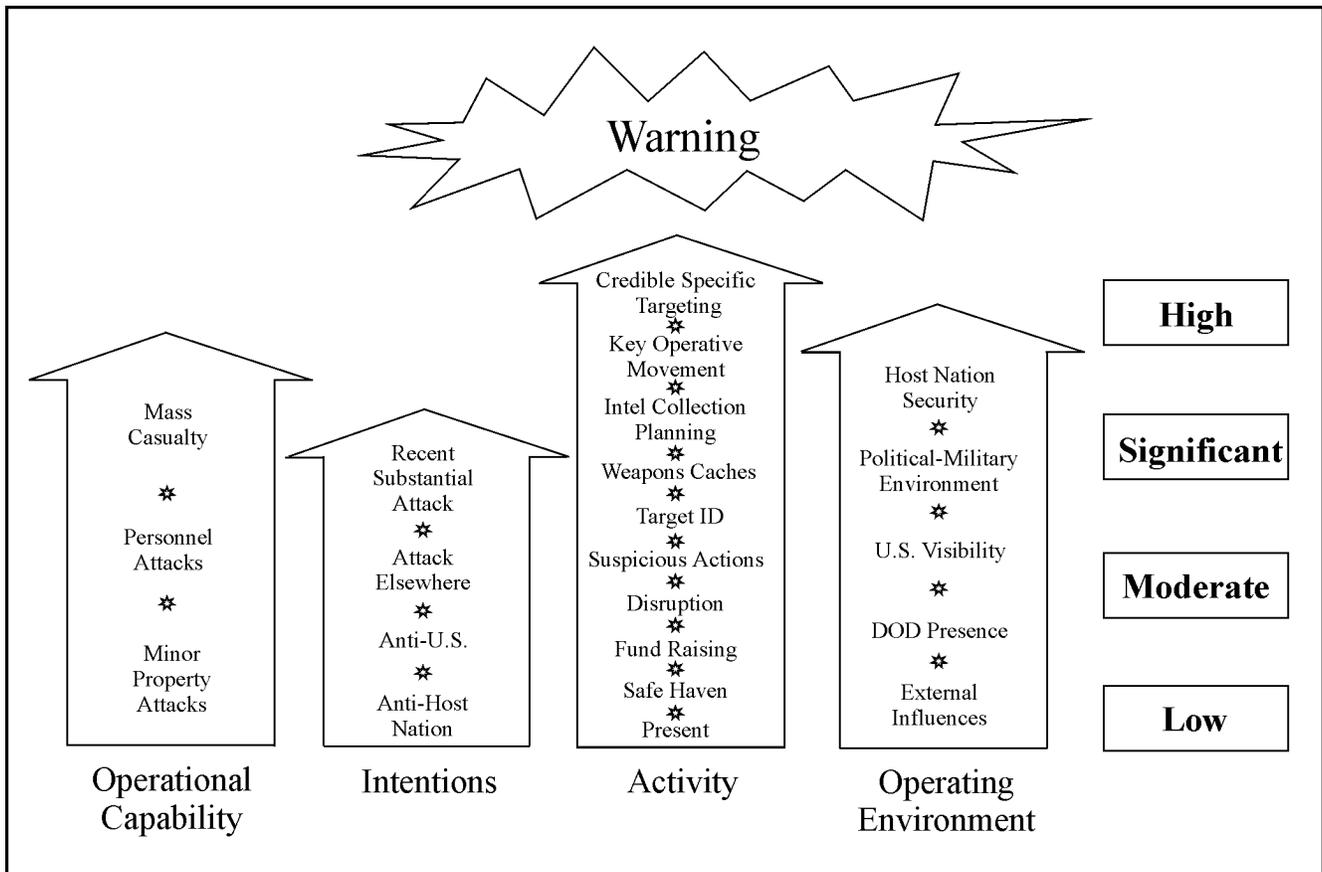


Figure 2-1. Terrorist Threat Level Assessment Criteria

Terrorist threat level assessments are not used to indicate when a terrorist attack will occur, nor are they used to specify a Force Protection Condition (FPCON). Naval Criminal Investigative Service Multiple Threat Alert Center, DIA and the unified commander issue separate warning notices in cases of imminent terrorist attack. In other words, the issuance of a terrorist threat level is not the same thing as the issuance of a warning notice. DOD threat level assessment factors are described in the following paragraphs:

1. **Operational Capability.** The acquired, assessed or demonstrated level of capability to conduct terrorist attacks.
2. **Intentions.** Actions indicative of preparations for specific terrorist operations.
3. **Activity.** Recently demonstrated anti-U.S. activity or stated or assessed intent to conduct such activity.
4. **Operating Environment.** The circumstances of the country under consideration.

Terrorist threat levels are set based on the analysis of a combination of the above threat assessment factors. The four levels, ranging from least to most are:

1. **Low.** No terrorist group is detected or the group activity is nonthreatening.
2. **Moderate.** Terrorist groups are present but there is no indication of anti-U.S. activity. The operating environment favors the host nation / United States.

**NWP 3-07.2 (Rev. A)**

- 3. **Significant.** An anti-U.S. terrorist group is operationally active and their preferred method of operation is to attack personnel; or the terrorist group’s preferred method of operation is to execute large casualty producing attacks but has limited operational activity. The operating environment is neutral.
- 4. **High.** An anti-U.S. terrorist group is operationally active and uses large casualty producing attacks as their preferred method of operation. There is a substantial DOD presence and the operating environment favors the terrorist.

**2.7 FORCE PROTECTION CONDITIONS**

Force protection conditions, shown in Figure 2-2, are a series of measures designed to increase the level of a unit’s defense against terrorist attacks. FPCONs are not aimed at specific threats, but are selected based on a combination of the following factors:

- 1. The terrorist threat level.
- 2. The capability to penetrate existing physical security systems.
- 3. The risk of terrorist attack to which personnel and assets are exposed.
- 4. The asset’s ability to execute its mission even if attacked.
- 5. The protected asset’s criticality to their missions.

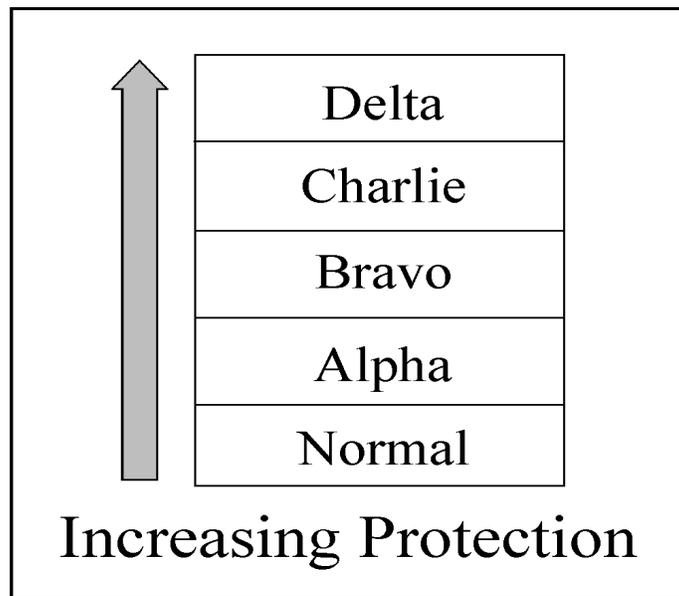


Figure 2-2. Force Protection Conditions

Commanders at any level can set the FPCON level; subordinate commanders can set a higher FPCON if the local situation warrants. FPCON measures are mandatory when declared, are implemented immediately and can be supplemented by additional measures. The declaration, reduction and cancellation of a FPCON remain the responsibility of the commander issuing the order. Each FPCON is briefly described below:

1. **FPCON NORMAL** applies when a general global threat of possible terrorist activity exists and warrants a routine security posture.
2. **FPCON ALPHA** applies when there is an increased general threat of possible terrorist activity against personnel or facilities, the nature and extent of which are unpredictable. Alpha measures must be capable of being maintained indefinitely.
3. **FPCON BRAVO** applies when an increased or more predictable threat of terrorist activity exists. Sustaining Bravo measures for a prolonged period may affect operational capability and relations with local authorities.
4. **FPCON CHARLIE** applies when an incident occurs or intelligence is received indicating some form of terrorist action or targeting against personnel or facilities is likely. Prolonged implementation of Charlie measures may create hardship and affect the activities of the unit and its personnel.
5. **FPCON DELTA** applies in the immediate area where a terrorist attack has occurred or when intelligence is received that terrorist action against a specific location or person is imminent. Normally, this FPCON is declared as a localized condition. FPCON Delta measures are not intended to be sustained for substantial periods.

Specific measures to be implemented at each FPCON are delineated in OPNAVINST 3300.54 (series), Protection of Naval Personnel and Activities against Acts of Terrorism and Political Turbulence, for ashore commands. For afloat commands, specific measures are described in the Antiterrorism Force Protection for Naval Operations Commanders Guide and in Chief of Naval Operations message traffic.

## **2.8 CONCLUSION**

The terrorist threat is not likely to diminish soon. On the contrary, events worldwide have shown the need for increased vigilance and preparation by U.S. Navy forces whether deployed or at home. Acts of terrorism are increasingly becoming the tactic of choice among those who wish to challenge the United States but do not have the capability or desire to directly confront U.S. forces using traditional military means.

Navy commanders who understand that terrorist threat scenarios are not static will design flexibility in their ATFP plans. Commanders who also maintain a workable balance among competing requirements - mission accomplishment, resource utilization and FPCON posture - will be positioned to execute the most successful ATFP operations.



# CHAPTER 3

## Intelligence

### 3.1 OVERVIEW

This chapter discusses the importance of intelligence in antiterrorism / force protection (ATFP) operations and defines the responsibilities of Department of Defense (DOD) intelligence organizations that support ATFP operations.

### 3.2 DEFINITIONS

“Information” and “intelligence” as used in this publication have different meanings:

**Information:** Data that has been gathered, but not fully correlated, analyzed or interpreted. Although information has not been fully analyzed or correlated, it may still be valuable to the tactical commander for threat warnings and target acquisition. Typical sources of information include the media, local authorities, local businesses and command personnel.

**Intelligence:** Product resulting from the collection, exploitation, processing, integration, analysis, evaluation and interpretation of available information. Reduced to its simplest terms, intelligence is knowledge and foreknowledge of the world—the prelude to decision and action by U.S. policymakers and intelligence consumers. Intelligence sources are described in detail below in paragraph 3.4.

In some cases, information may be disseminated immediately based upon operational necessity and potential impact on current operations. This type of raw intelligence is usually based on fragmentary information about fast-breaking events and may contain substantial inaccuracies or uncertainties that must be resolved through subsequent report and analysis. Finished intelligence products contain information that is compared, analyzed and weighted to facilitate the development of conclusions. The intelligence process includes steps that confirm information through a multiplicity of sources, reducing the chance of erroneous conclusions and susceptibility to deception.

### 3.3 INTELLIGENCE AND TERRORISM

Rigorous analysis of intelligence data in support of ATFP operations is critical. Post-analysis of terrorist incidents frequently reveals that indicators and information were on hand in raw data form prior to events, but few were able to comprehend the significance of those indicators.

Terrorists have the advantage of choosing the time, place and target for an attack. The intelligence community’s challenge is to identify threats, provide advance warning of terrorist attacks and disseminate critical intelligence in a usable form to commanders. This responsibility has become increasingly more difficult as terrorists target both U.S. military and civilian symbols at home and abroad.

### 3.4 ROLES AND RESPONSIBILITIES

It is important for ATFP planners to understand the roles and responsibilities of the intelligence community (what can and cannot be provided) as well as how to task appropriate organizations to provide information needed to

## NWP 3-07.2 (Rev. A)

complete the mission. It is equally important for intelligence organizations and analysts to understand the unique needs of ATRP forces, so intelligence support provided to deployed forces is mission-focused.

When developing mission-critical priority intelligence requirements (PIRs) (i.e., physical layout of a port, capability of host-nation security forces) and requests for information (RFIs) (i.e., capabilities of regional terrorists, local attitudes toward U.S. presence), commanding officers (CO) should think of the intelligence community as an inverted pyramid (see Figure 3-1). The CO need only be aware of the next intelligence organization in the chain of command, such as the strike group, air wing, amphibious ready group or numbered fleet intelligence officer (N2) when tasking national assets. The N2 will be connected to the next level of intelligence either through Navy or joint channels to push the requests to the next higher level. If information is requested from national assets such as the Central Intelligence Agency, National Security Agency or Defense Intelligence Agency, finished intelligence will follow the same route back to the requester via the staff N2. If the information requested can be satisfied at the theater or component level, answers will come directly to the requester.

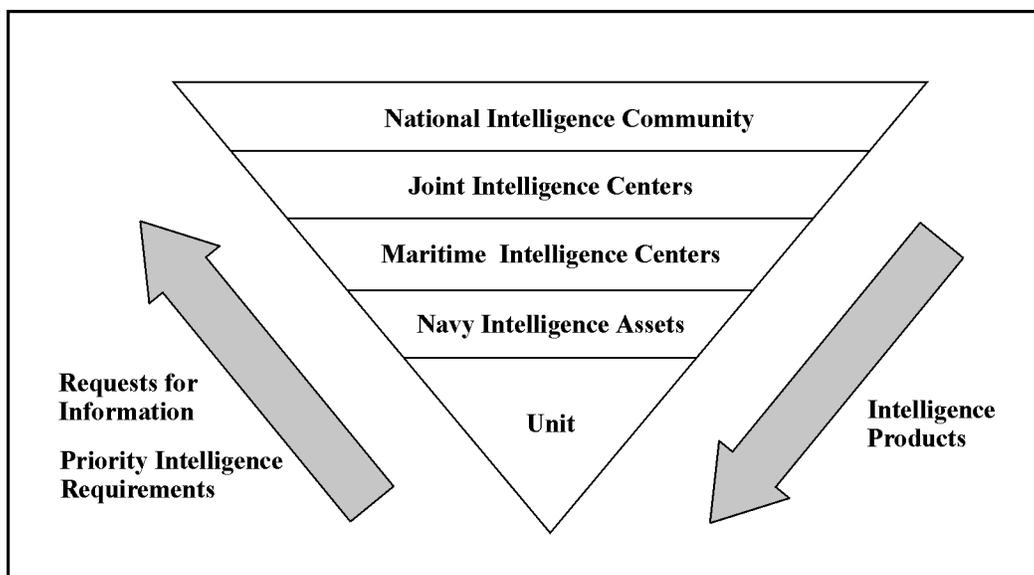


Figure 3-1. Support for Unit-Specific Intelligence Needs

The following sections describe intelligence centers and resources that can be called upon to support afloat and ashore commands.

### 3.4.1 Maritime Intelligence Centers

The Department of the Navy's intelligence organizations provide unique and continuous intelligence support to Navy operations. Navy assets receive their primary ATRP-related intelligence support from the Navy intelligence centers discussed below. As units deploy around the world, focused intelligence products are provided directly to the units from area of responsibility (AOR)-specific intelligence centers. The following organizations provide finished ATRP analytical products, indications and warning (I&W) reporting and watch centers to support fleet operations.

#### 3.4.1.1 National Maritime Intelligence Center

At the National Maritime Intelligence Center (NMIC) in Suitland, Maryland, the Office of Naval Intelligence (ONI) brings military and civilian employees into a single command to provide a single source for national-level

maritime intelligence. The NMIC also hosts the Marine Corps Intelligence Activity (MCIA), Coast Guard Intelligence Coordination Center (ICC) and Naval Information Warfare Activity (NIWA). These organizations provide national-level maritime intelligence to support joint warfighters, the Department of the Navy and national agencies and departments.

#### **3.4.1.2 Marine Corps Intelligence Activity**

MCIA focuses on crisis and predeployment support to expeditionary warfare units. MCIA complements and coordinates the efforts of the theater and other service and national intelligence organizations by providing unique threat, technical and terrain analysis products tailored to Marine Corps tactical units preparing to deploy. The activity functions as the Marine Corps' collection and production manager and as the primary coordination link with ONI expeditionary intelligence analysis and production assets.

#### **3.4.1.3 Coast Guard Intelligence Coordination Center**

ICC provides strategic intelligence support to Coast Guard law enforcement, military readiness, port security, marine safety and environmental protection personnel. The ICC serves as the Coast Guard's 24-hour I&W watch, maintaining a current picture of all maritime threats. The ICC is a critical source for assisting in domestic threat reporting and port vulnerability analyses.

#### **3.4.1.4 Naval Security Group**

As the Navy's executive agent for cryptology, information warfare and command-and-control warfare, Naval Security Group, located at Fort Meade, Maryland, is responsible for cryptologic planning and programming, system acquisition, training and administration of naval cryptologic field activities around the world.

### **3.4.2 Joint Intelligence Centers**

Each of the five unified combatant commanders (NORTHCOM, SOUTHCOM, EUCOM, CENTCOM, PACOM) has a joint intelligence center that analyzes and consolidates data to produce fused intelligence, long-range assessments and threat estimates for forces assigned to its AOR.

Joint Forces Intelligence Command in Norfolk, Virginia, is to assume responsibility for all joint intelligence transformation, experimentation and training.

### **3.4.3 Naval Counterintelligence**

Joint Publication 1-02, DOD Dictionary of Military and Associated Terms, defines counterintelligence as information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, foreign persons or international terrorist activities.

Naval Criminal Investigative Service (NCIS), headquartered at the Washington Navy Yard, has primary investigative and counterintelligence jurisdiction within the Department of the Navy. Additionally, NCIS is responsible for collecting, processing, storing and disseminating counterintelligence information regarding persons or organizations not affiliated with the Department of Defense. NCIS maintains a worldwide field structure to support the Navy both ashore and afloat.

### **3.4.3.1 ATFP Program**

NCIS collects and analyzes information about possible threats from various sources and advises commanders. This program includes investigations, threat briefings, intelligence collection and vulnerability assessments. NCIS personnel in this program are assigned to the staffs of the fleet and component commands as staff counterintelligence officers (SCIOs). SCIOs are the commanders' direct connection to all of the NCIS and Multiple Threat Alert Center (MTAC) ATFP program resources and services. NCIS also assigns agents to the unified commands as counterintelligence staff officers.

NCIS agents also support the Joint Staff Integrated Vulnerability Assessment (JSIVA) Program, the Chief of Naval Operations Integrated Vulnerability Assessment (CNOIVA) Program, as well as the Navy's Port Integrated Vulnerability Assessment (PIVA) Program.

### **3.4.3.2 Country Referent Program**

Through the NCIS Country Referent Program, agents conduct advance visits to expeditionary ports, airfields and exercise areas to prepare an ATFP threat assessment for transiting units. This ATFP collection effort is conducted within 30 days for moderate, significant and high threat countries, and within 90 days for low threat locales. NCIS threat assessments are issued 7-10 days prior to the arrival of the transiting unit. In many cases, NCIS agents are available to meet the transiting unit when it arrives.

### **3.4.3.3 Multiple Threat Alert Center**

Formerly known as the Antiterrorist Alert Center (ATAC), the MTAC in Washington, D.C., monitors all service, national and theater intelligence traffic and products to identify specific threats to Navy and Marine Corps personnel and resources. MTAC analysts track potential terrorist activities and trends, reporting them to the fleet via message traffic.

The MTAC spot message is the Navy's principal vehicle for disseminating terrorism warnings to Navy and Marine Corps commands. The MTAC issues spot messages to notify commanders when all-source analysis indicates that the near-term potential for a terrorist event has increased, but the situation does not necessarily warrant raising the overall threat level.

The MTAC disseminates Blue Dart messages when intelligence indicates that a specific, imminent and credible terrorist threat exists.

When a Navy Blue Dart, MTAC spot report or other terrorism threat warning message is received, commanders shall review on-scene terrorist force protection conditions as well as leave and liberty policies in the threatened area.

## **3.5 COMMAND RESPONSIBILITIES**

Commanders at all levels, as appropriate, must:

1. Review intelligence reports and disseminate warnings to subordinate commands.
2. Identify PIRs and RFIs, as required, to support mission accomplishment.

3. Establish procedures to develop local information and report all suspicious activity.
4. Establish procedures to fuse intelligence and local information to determine if the baseline security posture and Force Protection Condition need to be changed or elevated.
5. Ensure local security forces are continuously updated on likely threat activities.

### **3.6 CONCLUSION**

It is incumbent upon the commander to seek out intelligence resources at each port, airfield, naval station and air station to fully understand the local threat environment. By having access to fused intelligence from local, regional and national resources, commanders can accurately assess threats and employ ATFP resources to effectively prevent terrorism.



# CHAPTER 4

## Organization and Responsibilities

### 4.1 OVERVIEW

Following the terrorist attacks of 11 September 2001, Federal organizations tasked with antiterrorism / force protection (ATFP) responsibilities reorganized. By forming the Department of Homeland Security to coordinate efforts among sometimes competing agencies, Congress centralized many of the government's ATFP resources and intelligence assets in one department. Within the Department of Defense (DOD), a new unified commander, Northern Command (NORTHCOM), was established to assume responsibility for defense of the United States and to provide military assistance to civil authorities.

This chapter presents the ATFP operational and administrative chains of command for the U.S. Navy above the unit level. It discusses Navy ATFP responsibilities as well as how to coordinate interaction between the Navy and Federal and host nation (HN) agencies. (NTTP 3-07.2.1 (Rev. A), Antiterrorism / Force Protection, addresses the Navy's ATFP organization and responsibilities at the unit level.)

### 4.2 SECRETARY OF HOMELAND SECURITY

In an executive order signed in October 2001, President Bush set forth the mission of the Department of Homeland Security "to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks."

The Secretary of Homeland Security is the principal Federal official for domestic incident management. Pursuant to the Homeland Security Act of 2002, the Secretary is responsible to coordinate Federal operations within the United States to prepare for, respond to and recover from terrorist attacks, major disasters and other emergencies if and when any one of the following four conditions applies:

1. A Federal department or agency acting under its own authority requests the assistance of the Secretary.
2. The resources of state and local authorities are overwhelmed and Federal assistance has been requested by the appropriate state and local authorities.
3. More than one Federal department or agency has become substantially involved in responding to the incident.
4. The Secretary has been directed to assume responsibility for managing the domestic incident by the President.

Joint Publication 3-26, Joint Doctrine for Homeland Security, provides organizational responsibilities and command relationships.

#### 4.2.1 National Incident Management System

A Homeland Security Presidential Directive, February 2003, (HSPD 5 Management of Domestic Incidents), directs all Federal agencies to adopt and implement the National Incident Management System (NIMS) to work

## **NWP 3-07.2 (Rev. A)**

effectively and efficiently with state and local governments to prepare for, respond to and recover from domestic incidents, regardless of cause, size or complexity.

NIMS includes a core set of concepts, principles, terminology and technologies to provide interoperability and compatibility with:

1. Incident command system (ICS)
2. Multi-agency coordination systems
3. Unified commands
4. Systems that track training, qualifications and certification
5. Systems that identify and manage resources (including systems for classifying types of resources)
6. Systems that collect, track and report incident information and incident resources.

To implement NIMS, a new National Response Plan (NRP) is under development. The NRP will integrate Federal government domestic prevention, preparedness, response and recovery plans into one all-discipline, all-hazards plan. The NRP will consolidate and supercede current guidance in several plans, including:

1. Federal Response Plan (FRP)
2. FRP terrorism incident annex
3. National contingency plan
4. Federal radiological emergency response plan
5. Domestic terrorism interagency concept of operation plan.

### **4.2.2 Incident Command System**

Interagency coordination is achieved via the incident command system. ICS consists of multi-agency integration procedures to control personnel, facilities, equipment and communications. ICS is designed for use in both planned events and emergent incidents.

Commanding officers, antiterrorism officers and installation security officers shall become familiar with ICS concepts to be able to integrate into an ICS-format command structure. ICS training is available online through the Federal Emergency Management Agency (FEMA) at [www.training.fema.gov](http://www.training.fema.gov).

### **4.3 SECRETARY OF STATE**

The Secretary of State has the responsibility to coordinate international activities related to the prevention, preparation, response and recovery from a terrorist incident and for the protection of U.S. citizens and interests overseas. The Department of State negotiates with host nations to establish Status of Forces Agreements or HN support agreements.

#### **4.4 SECRETARY OF THE NAVY AND CHIEF OF NAVAL OPERATIONS**

The Secretary of the Navy, through the Chief of Naval Operations (CNO) and in support of unified commanders, is responsible for instituting Navy ATFP programs and supporting them with adequate planning, programming and budgeting. Other responsibilities include:

1. Ensuring adequate force protection of forces, installations and DOD personnel and dependents.
2. Incorporating ATFP policy and standards into Navy doctrine and ensuring ATFP doctrine is compatible with joint doctrine.
3. Instituting ATFP training programs.
4. Ensuring all Navy installations and activities conduct comprehensive ATFP program reviews and assessments.
5. Developing a Navy-oriented ATFP strategic plan that details the vision, mission, goals and performance measures in support of DOD's Antiterrorism Strategic Plan.

#### **4.5 UNIFIED COMMANDER**

The highest echelon of command for ATFP operations is the unified commander. Five Geographic Combatant Commanders (COCOMs) have overall ATFP responsibility within their areas of responsibility (AOR) and are specifically tasked with:

1. Establishing command ATFP policies and programs for the protection of all assigned forces, installations, DOD personnel and dependents in their AOR.
2. Assessing and reviewing ATFP programs of all assigned military forces and / or activities in the AOR.
3. Assessing the terrorist threat for the AOR.
4. Ensuring force protection conditions are uniformly implemented and disseminated as specified in DOD Directive 2000.12 (series), DOD O-2000.12-H (series) and DOD Instruction 2000.16 (series).
5. Developing a Geographic COCOM-oriented ATFP strategic plan that details the vision, mission, goals and performance measures in support of DOD's Antiterrorism Strategic Plan.

U.S. Northern Command, based at Peterson Air Force Base in Colorado, is the newest Geographic Combatant Command. NORTHCOM's areas of operations include the United States, Canada, Mexico, parts of the Caribbean and the contiguous waters in the Atlantic and Pacific Oceans up to 500 miles off the North American coastline.

#### **4.6 COMMANDER FLEET FORCES COMMAND**

Commander, Atlantic Fleet has assumed additional responsibilities as Commander, Fleet Forces Command (CFFC). In an initiative to standardize and increase efficiency of ATFP programs within the United States, the CNO designated CFFC as executive agent for ATFP operations for all CONUS Navy forces. CFFC is also the forwarding authority for Navy-wide ATFP requirements and is responsible for:

1. Developing fleet ATFP doctrine and tactics, techniques and procedures.

## **NWP 3-07.2 (Rev. A)**

2. Ensuring deployment training supports combatant commanders.
3. Recommending FPCON changes to Chief of Naval Operations.
4. Providing Navy forces in the NORTHCOM AOR (except Alaska and Hawaii, which are defended by Pacific Command).
5. Protecting forces, installations, personnel and dependents CONUS.
6. Consequence management of terrorist incidents while maintaining essential operations.

### **4.7 NAVNORTH**

Commander, Atlantic Fleet, designated Commander, U.S. Navy Forces North (NAVNORTH), serves as the maritime service component commander within the NORTHCOM AOR. Commander, Naval Forces North East and West serve as the fleet components to NAVNORTH. (Thus, numbered fleets are designated differently within the unified combatant commander's mission.)

Navy regions and numbered fleet commands report to Commander, Atlantic Fleet or Commander, Pacific Fleet. Each fleet command center performs operational planning and executes homeland defense missions, including requests for forces from NAVNORTH. Fleet commanders maintain situational awareness, allocate resources, measure and monitor readiness, analyze intelligence and disseminate threat analyses and FPCON changes to subordinates.

### **4.8 COMMANDER NAVY INSTALLATIONS**

Commander, Navy Installations (CNI) was established on 1 October 2003 under CNO as an Echelon II commander. CNI is the Navy's single installation management organization with the responsibility of providing uniform program, policy and funding for management and oversight of shore installation support to the fleet.

CFFC and OCONUS Naval forces exercise operational control over region commanders and subordinate shore activities, with CNI exercising administrative control for installation support funding and standardization of shore installation processes and policies.

Region commanders administratively report to CNI for purposes of funding and alignment of shore installation management policies and procedures. Administrative control includes the authority over subordinate shore organizations with respect to administration and support, including control of resources and equipment, personnel management, unit logistics, training and discipline.

CNI, region commanders and CFFC coordinate on policy, process and budget matters that overlap shore installation management and readiness of operational forces.

### **4.9 NAVY REGION COMMANDER AND NUMBERED FLEET COMMANDER**

Ashore commanding officers report to the Navy region commander in whose AOR they are physically located for all operational matters related to ATRP. Region commanders execute the ATRP mission through region operations centers (ROCs).

In the ROC, region commanders collaborate, communicate and control resources, issue orders and conduct crisis and consequence management. The ROC controls and brokers resources among subordinate commands and

coordinates requests for nonorganic resources (i.e., afloat assets, Marine Corps security forces and regional civil counterparts) and from the host nation if OCONUS. Navy region commanders report to the fleet commander.

The afloat commander's higher headquarters for ATFP is normally the numbered fleet. The numbered fleet maintains a battle watch to which an afloat commander reports in the event of a terrorist threat or incident. Numbered fleet commanders report to their respective fleet commanders.

#### **4.10 INTERAGENCY COORDINATION**

Navy activities must engage and plan with civilian agencies before a terrorist threat or incident occurs. Command and control activities with other agencies are better expressed as "communicate" and "coordinate." Navy activities must be active participants in civilian agency planning councils at a comparable level. Installations must also engage in local planning, while Navy regions should engage at state and regional planning levels.

Host nation support may be available to support ATFP operations; in such instances, it is important to make prior arrangements for that support, the details of which should be incorporated into ATFP plans.



## CHAPTER 5

# Antiterrorism / Force Protection Planning

### 5.1 OVERVIEW

Resourceful terrorists will continue to look for and choose guaranteed ways to inflict maximum damage upon American symbols and personnel. It is, therefore, important for commanders to understand the following basic antiterrorism fundamentals:

1. All military personnel and property are potential terrorist targets.
2. Ability to predict where, when and how terrorist attacks will occur is inexact.
3. Every asset cannot be protected sufficiently at all times to guarantee immunity from a terrorist attack.

The planning process is, first and foremost, a structured way of thinking that focuses on the mission and the threat. Employed at the outset of antiterrorism / force protection (ATFP) plan development, the six-step planning process guides ATFP planners to choose implementable solutions tailored to command requirements.

The planning process set forth in this chapter is applicable across the range of military operations, at any echelon of command, both afloat and ashore. Amplifying discussion of the planning process can be found in NTTP 3-07.2.1 (Rev. A), Antiterrorism / Force Protection.

### 5.2 ASSESSMENT TOOLS

Commanders must produce clear mission statements that enable ATFP planners to construct focused, effective ATFP plans. The following two sections describe both internal and external assessment tools commanders can use to assess risk, define threats and understand vulnerabilities prior to beginning the planning process.

#### 5.2.1 Internal Assessment Tools

Tools to formalize the commander's internal risk assessment process include:

1. **Operational Risk Management (ORM).** ORM is a Navy-wide process that identifies hazards, assesses risks and implements controls to reduce risks. ORM is described in OPNAVINST 3500.39 (series), Operational Risk Management.
2. **Criticality / Vulnerability (C / V) Assessments.** Commanders must decide which of their assets to protect and to what level. C / V assessments help planners determine which assets are most critical to a unit's mission and which are most vulnerable to attack.
3. **Planning and Response Element Assessments.** This assessment tool helps planners analyze the strengths and weaknesses of the major antiterrorism planning and response elements that contribute to a command's ability to deter and employ countermeasures, both pre-incident and post-incident.

## **NWP 3-07.2 (Rev. A)**

Detailed descriptions for each of the above assessment tools can be found in NTTP 3-07.2.1 (Rev. A), Antiterrorism / Force Protection.

### **5.2.2 External Assessment Tools**

External assessment tools are created by several organizations, including the Naval Criminal Investigative Service (NCIS), fleet commanders, unified commanders, Chief of Naval Operations and the Defense Threat Reduction Agency. Their products are described briefly below.

1. **Port Integrated Vulnerability Assessment (PIVA).** Addressing the force protection posture of ports, PIVAs provide useful data to craft inport security plans and draft force protection plans. A PIVA includes:
  - a. An evaluation of a port's security forces.
  - b. Weaknesses and vulnerabilities associated with the configuration of port facilities and surrounding terrain.
  - c. Host nation agreements.
  - d. U.S. security measures authorized by host nation, i.e., armed watchstanders on the pier.
  - e. Recommended security measures for all threat conditions.
  - f. Written and graphic guidance addressing how to employ ATFP measures while in port; also addresses where and how items such as barriers, fencing and lights can be obtained.
  - g. Shore and waterside security threats such as swimmers and fast boats.

Unified commanders typically task numbered fleet or component commanders to create PIVAs. NCIS provides useful resources for such tasking.
2. **Chief of Naval Operations Integrated Vulnerability Assessment (CNOIVA).** CNOIVA teams conduct periodic installation assessments to determine compliance with DOD and Navy force protection standards.
3. **Joint Staff Integrated Vulnerability Assessment (JSIVA).** The Defense Threat Reduction Agency conducts 80-100 JSIVAs annually at DOD installations worldwide. JSIVA teams determine vulnerabilities and propose ameliorating solutions. Team reports are sent to the installation commander, the Joint Staff and the appropriate combatant commander and military service chief.
4. **Vulnerability Assessment Management Program (VAMP).** VAMP is a Web-based tool, accessed through the SIPRNET, designed to track, prioritize and report vulnerabilities, which come from the results of JSIVAs, CNOIVAs and local assessments. NCIS serves as the VAMP program manager.
5. **Threat assessments.** An ATFP threat assessment is the end product of a specified area's threat analysis. It is coordinated by the Navy region commander in the United States and by the designated organization for the gaining theater commander. Commands receive theater and NCIS threat assessments per numbered fleet and theater procedures.

## **5.3 PLANNING PROCESS**

The planning process is the method by which commanders can create focused, realistic ATFP plans. The six steps in the planning process are: mission analysis, course of action (COA) development, course of action war gaming, course of action comparison and selection, ATFP plan development and transition. Each step is briefly described below and in more detail in NTTP 3-07.2.1 (Rev. A), Antiterrorism / Force Protection.

### **5.3.1 Mission Analysis**

The output of mission analysis is the development of a clear ATFP mission statement. The purpose of the mission statement is to clearly delineate what assets and areas are to be protected from specific threats and to prioritize each asset's criticality to the mission.

### **5.3.2 Course of Action Development**

Planners use the mission statement to develop several courses of action. A COA is a broadly stated potential solution to an assigned mission (i.e., defining entry control points to deny access to the ship). During COA development, planners consider those risk assessments that identify critical and vulnerable assets. Each prospective COA is examined to ensure that it is suitable, feasible, different, acceptable and complete with respect to both current and anticipated situations, the mission and commander's intent.

### **5.3.3 Course of Action War Gaming**

During COA war gaming, planners assess each potential COA against both the threat and the environment. By examining action-reaction-counteraction dynamics, planners can, for each potential COA, identify strengths and weaknesses, associated risks and asset shortfalls. The output of war gaming is the most reliable data, short of actual COA execution, by which commanders and planners can understand, calibrate and improve each COA.

### **5.3.4 Course of Action Comparison and Selection**

COA comparison and selection is a facilitated discussion (commander's war game) that results in COA selection. Unlike previous steps in the planning process, however, COA comparison and selection involves all participants, including the commander. The commander or chief of staff / executive officer serves as facilitator throughout the discussion.

From COA war game results, the commander first selects the COA deemed to have the highest probability of success, then briefs that decision to the group. At this point, the commander may also refine intent and concept of operations, identifying any parts of the chosen COA that need further planning attention. Each of the other war gamed COAs is then compared against the commander-selected COA.

### **5.3.5 ATFP Plan Development**

Building on the selected COA from the last step, planners codify commander's intent, other guidance and decisions into a formal ATFP plan. Depending on available time, complexity of operations and levels of command involved, the ATFP plan can be either written or issued as a verbal command. The written plan or order can be amplified with supporting appendices, i.e., estimates of supportability and other command-specific planning documents. The final section of this chapter lists topics that the ATFP plan should address.

Above all, the ATFP plan must be clear, concise, timely and useful.

### **5.3.6 Transition**

Once developed, the ATFP plan must be moved to the personnel who will execute it. In commands with large staffs, the transition occurs from the planning staff to the operations staff for execution. In smaller commands, those who write the plan may be the same personnel who supervise its execution.

## **5.4 POST-INCIDENT RESPONSE PLANNING**

The consequences resulting from a terrorist attack can be severe, as was demonstrated in the aftermath of the attack on the USS Cole. Hull damage from the initial explosion had to be immediately addressed by the damage control team so the ship would remain afloat. Immediate post-incident responses were also required from the Commanding Officer, the damage control party and the medical department, among others.

Post-incident responses are divided into two overlapping areas:

1. **Crisis management:** In ATFP operations, crisis management consists of those measures taken to identify, acquire and plan the use of needed resources to resolve the effects of a terrorist act.
2. **Consequence management:** In ATFP operations, consequence management consists of those measures taken to protect health and safety, restore essential services and provide emergency assistance to commands affected by the consequences of terrorism.

This section discusses issues that must be addressed to effectively develop ATFP post-incident responses that have a high probability of being successful.

1. **Communications.** Frequently, post-incident communications among responders at the scene, the operations center and higher authorities are hindered by a combination of system overload and incompatibility of communications equipment. The ATFP plan should address adequate secure and nonsecure communications.
2. **Evidence.** Because the sites of terrorist incidents are crime scenes, evidence at the scene must be protected. Witnesses' testimony and photographic and other evidence may be important to a successful prosecution. The ATFP plan should address the process by which a continuous chain of custody is maintained, from the time custody is established until it is presented in court.
3. **Logistics.** Adequate supplies (i.e., communications equipment, vehicles, security equipment and administrative support materials) must be available in the event of an incident. When post-incident response planning includes using outside response forces, additional strains will be placed on available messing, berthing and support needs.
4. **Apprehended personnel.** Apprehended military personnel must be handled according to Navy regulations and applicable installation standard operating procedures. In U.S. territory, civilian detainees must be released for disposition to the FBI or U.S. Marshals. Outside U.S. territory, civilian detainees will be processed according to the status-of-forces agreement with that particular country. The Staff Judge Advocate should be consulted prior to releasing any individual to host-nation authorities.
5. **Reports.** The ATFP plan should specify all required reporting requirements, with timelines, for notifying higher headquarters and others.

6. **Public affairs.** The primary duties of public affairs personnel are to ensure that the public (including news media) receives accurate information and to communicate a calm, measured and reasonable response to the ongoing event.
7. **Resources.** The following is a partial list of resources that may be required in the event of a terrorist attack:
  - a. Medical
    - (1) Medical care personnel
    - (2) Health / medical equipment and supplies
    - (3) Patient evacuation
    - (4) In-hospital care
    - (5) Food / drug / medical device safety
    - (6) Worker health / safety
    - (7) Radiological / chemical / biological hazards consultation
    - (8) Mental health care
    - (9) Public health information
    - (10) Vector control
    - (11) Potable water / wastewater and solid waste disposal
    - (12) Victim identification / mortuary services
    - (13) Veterinary services
  - b. Transportation
    - (1) Heavy equipment
    - (2) Ambulances
    - (3) Movement of incoming supplies / support
    - (4) Movement of incoming assistance personnel
  - c. Specialized resources
    - (1) Firefighting
    - (2) Hazardous material response teams
    - (3) Diving and salvage

## **NWP 3-07.2 (Rev. A)**

- (4) Urban search and rescue (collapsed building rescue)
  - (5) Weapons of mass destruction special response teams
  - (6) Explosive ordnance disposal
  - (7) Military Working Dog (MWD) teams
- d. Public Works
- (1) Potable water, power, temporary housing and other critical facilities
  - (2) Emergency repair to access routes, airfields, streets, bridges or other areas requiring emergency access to victims
  - (3) Emergency stabilization or destruction of damaged structures and facilities
  - (4) Damage and needs assessments
  - (5) Emergency clearance of debris.

## **5.5 PLANNING PRODUCTS**

The ATFP plan produced at the conclusion of the planning process should provide an integrated, comprehensive approach to deter, detect, defend against and mitigate terrorist threats. The classification of an ATFP plan is dependent upon its content, current policy and the specifics of a unit's situation. An effective ATFP plan will address:

1. Concept of operations
2. Preplanned responses
3. Tactics
4. Crisis management procedures
5. Consequence management procedures
6. Baseline security posture
7. Measures to increase security posture
8. Reporting procedures
9. Command and control procedures.

ATFP plan and inport security / force protection plan templates are included as appendices to NTPP 3-07.2.1 (Rev. A), Antiterrorism / Force Protection.

Every ATRP plan includes the identification of intelligence gaps in available threat holdings, factoring in time to develop requests for information from higher echelons to include the national agencies. Threat information is typically acquired from higher echelons, host-nation authorities, Naval Criminal Investigative Service, American embassies, civilian authorities and the advance party.



## CHAPTER 6

# Antiterrorism / Force Protection Execution

### 6.1 OVERVIEW

Successful antiterrorism / force protection (ATFP) programs have two things in common across the spectrum from pre-incident responses through post-incident management: deliberate preparations and deliberate actions. This chapter discusses the fundamental principles of ATFP that inform the plans, preplanned responses, tactics and crisis / consequence management strategies.

### 6.2 PRE-INCIDENT PREPARATIONS

ATFP operations are defensive operations: Terrorists choose the place, the method and the time to attack. Therefore, planners and the Antiterrorism Officer (ATO) at each command must:

1. Analyze the threat specific to a command's situation
2. Conduct risk assessments to determine the criticality and vulnerability of assets
3. Develop and execute an effective ATFP plan
4. Establish a baseline security posture
5. Implement random antiterrorism measures (RAM)
6. Conduct post-mission / deployment assessments to improve future performance.

#### 6.2.1 Threat Analysis

The ATO determines specific threats for each mission, chokepoint transit and port visit. The current threat analysis will focus how resources should be applied to counter viable threats while de-emphasizing unlikely threats. For example, small boat attacks might be likely during a transit of the Straits of Malacca, while the threat of an air attack is negligible. Antiair assets can then be diverted to counter surface attacks during the transit.

#### 6.2.2 Risk Assessments

ATFP planners define what needs to be protected and to what level. Assessment tools that assist with quantifying tasks include:

1. Operational risk management
2. Criticality assessment
3. Vulnerability assessment
4. Planning assessment

## **NWP 3-07.2 (Rev. A)**

5. Response element assessment
6. Vulnerability Assessment Management Program (VAMP).

NTTP 3-07.2.1 (Rev. A), Antiterrorism / Force Protection, provides detailed descriptions of each of these tools.

### **6.2.3 ATFP Plan**

Pre-incident preparations achieve deliberate focus when derived from a clear and unambiguous antiterrorism / force protection plan. The ATFP plan defines the spectrum of measures, qualifications, responses and tactics necessary to counter and manage terrorist incidents. ATFP plans are dynamic and one plan may not fit all situations; commanders adapt and implement plans to meet changing circumstances.

NTTP 3-07.2.1 (Rev. A), Antiterrorism / Force Protection, provides detailed instructions on ATFP plan development.

### **6.2.4 Baseline Security Posture**

The baseline security posture is defined as those security measures in place 24 hours a day, 7 days a week regardless of the threat level or force protection condition (FPCON). Examples include entry control points that always have serpentine barriers, small boats that patrol access points to aircraft carriers and watchstanders who check identification of all personnel entering a naval installation are each part of the baseline security posture.

Typically, when the threat level or FPCON increases, additional measures, in addition to the baseline security posture, are immediately implemented. The baseline security posture should not be so stringent that it restricts mission accomplishment.

### **6.2.5 Random Antiterrorism Measures**

Random antiterrorism measures are employed to deny terrorists target predictability. Implementing measures at varying times and places achieves two things: it changes the command defensive posture and it thwarts terrorists' planning. One example of a RAM is closing a base-access gate without warning for several hours one day, then closing another gate several days later.

### **6.2.6 Post-Mission / Deployment Assessments**

All lessons learned from ATFP-related actions are to be documented locally per theater requirements, as well as through the Navy Lessons Learned System (NLLS), administered by the Navy Warfare Development Command in Newport, Rhode Island. Information about NLLS is available at the Website [www.nwdc.navy.mil](http://www.nwdc.navy.mil) or at [www.nwdc.navy.smil.mil](http://www.nwdc.navy.smil.mil).

## **6.3 INCIDENT RESPONSE**

Incident responses are those actions taken by personnel, most likely watchstanders and reaction forces, to defend against a terrorist attack. When responding to an attack, or potential attack, personnel must first determine hostile intent, then decide whether to use force and to what level.

Commanders can position watchstanders for success by effectively preparing the battlespace, which includes:

1. **Proper mindset of watchstanders.** Alert, well-trained security forces will successfully detect and defend against terrorist attacks. Watchstanders must:
  - a. Be well-rested
  - b. Receive post-specific training and orders
  - c. Receive current intelligence
  - d. Know preplanned responses.
2. **Clear procedures.** ATFP operations are to be clearly delineated in succinct standard operating procedures, preplanned responses and tactics.
3. **Organized battlespace.** A layered physical defense ensures:
  - a. No single point of failure, thus forcing a threat to evade or penetrate several defenses before gaining access to a critical asset or area.
  - b. Conditions are set for the use of force, allowing watchstanders to detect, identify, classify and neutralize threats so that hostile intent can be determined as far from the protected asset or area as possible.
4. **Realistic training.** Watchstanders should receive repetitive, meaningful training to eliminate hesitation, confusion and ambiguity.

NTTP 3-07.2.1 (Rev. A), Antiterrorism / Force Protection, provides a detailed discussion on use of force and battlespace preparations.

## 6.4 POST-INCIDENT RESPONSE

Post-incident responses are those actions taken to mitigate effects and restore services after a successful terrorist attack. These actions are divided into two interrelated categories, crisis management and consequence management. Crisis management includes those actions taken to immediately mitigate and terminate the incident; consequence management involves both the immediate response to contain damage and the long-term recovery process.

The ability to respond during and immediately after a terrorist attack will depend upon the amount of planning, available security forces and ATFP measures in place at the time of the incident. For example, an installation at FPCON Alpha might have limited security forces to respond to an attack. If, however, an installation is at FPCON Bravo because of an increased threat of terrorist activity, more watchstanders will be posted, reaction forces will be at a higher level of readiness and additional physical barriers will be erected, thus being better prepared for an attack.

### 6.4.1 Phases of Post-Incident Response

Post-incident responses can be divided into three phases: commitment of local resources, arrival of additional resources and return to baseline / restoration of services.

## **NWP 3-07.2 (Rev. A)**

### **6.4.1.1 Commitment of Local Resources**

Local resources accomplish the following:

1. Control the scene of the incident:
  - a. Prevent access by nonessential personnel
  - b. Evacuate nonessential personnel from scene
  - c. Provide security in case of secondary attack
  - d. Contain spread of contamination if chemical, biological or radiological (CBR) attack
2. Identify an on-scene commander (OSC) and establish communications with higher authority
3. Confirm the type of incident (i.e., explosion, CBR attack)
4. Treat and evacuate casualties
5. Initiate damage control efforts (i.e., firefighting, flooding control).

These actions are accomplished concurrently and initially involve on-duty watchstanders. Subsequent personnel can include firefighters, emergency medical responders, security reaction forces and explosive ordnance disposal (EOD) teams.

### **6.4.1.2 Arrival of Additional Resources**

Additional law enforcement and security personnel and specially trained response forces, such as hostage rescue and hazardous material teams or host nation tactical units, augment initial response forces. Phase two begins when the affected installation, Navy region or host nation activates an operations center to coordinate crisis and consequence management efforts.

During this phase, a Federal agency such as the Federal Bureau of Investigation (FBI) or Department of Homeland Security (DHS) may assume jurisdiction, if in the United States, as lead Federal agency (LFA) over the incident. When another agency becomes the LFA, Department of Defense (DOD) forces assume a support role.

When outside the United States, the Department of State and U.S. Embassy will assume the key role in coordinating U.S. and host nation responses.

### **6.4.1.3 Return to Baseline / Restoration of Services**

In phase three, forces restore services (i.e., electrical power, traffic flow, base access) affected by the incident and establish a sustainable security posture. Efforts such as decontamination, medical surveillance, crime-scene investigation and damage control, as applicable, continue.

## **6.4.2 Post-Incident Command and Control**

As soon as possible after the start of a terrorist incident, the OSC establishes control and notifies higher authority. Initially, the OSC will likely be the senior watchstander closest to the incident, who might then be supplanted by

a senior officer arriving on the scene. Command and control should ultimately shift to an operations center (i.e., installation or regional operations center), where resources can be coordinated (see Figure 6-1). These resources include:

1. Public works
2. Security
3. Emergency medical
4. Public affairs
5. Logistics / supply
6. Explosive ordnance disposal
7. Local, state and Federal emergency management and law enforcement agencies
8. Department of Homeland Security
9. Naval Criminal Investigative Service
10. Other DOD commands
11. Host nation forces.

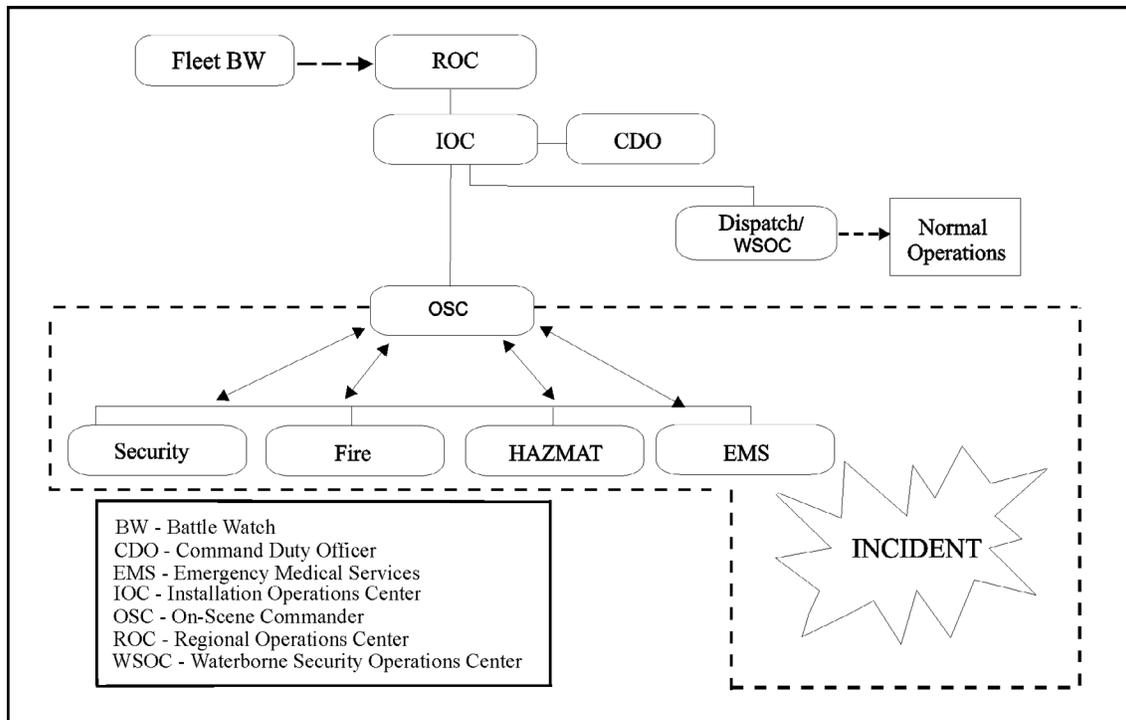


Figure 6-1. Post-Incident Command and Control

#### **6.4.2.1 Federal Response Plan**

The terrorism incident annex of the Federal Response Plan defines the antiterrorism responsibilities of Federal departments and agencies in the event of a terrorist incident. Commanders, antiterrorism officers and installation security officers should be familiar with the terrorism incident annex, which is available at [www.fema.gov/rrr/frp/](http://www.fema.gov/rrr/frp/).

#### **6.4.2.2 Department of Justice**

The Department of Justice (DOJ) is designated as the overall LFA for threats or acts of terrorism within the United States until the Attorney General transfers the overall LFA role to the Federal Emergency Management Agency. DOJ delegates the operational response to the FBI, who operates as the on-scene manager for the Federal government.

#### **6.4.2.3 Federal Bureau of Investigation**

The FBI supports the overall LFA by operating as the lead agency for crisis management. The FBI is responsible for appointing an FBI on-scene commander (or subordinate official) to manage and coordinate the crisis management response.

#### **6.4.2.4 Department of Homeland Security**

The Department of Homeland Security is designated as the lead agency for consequence management within the United States. To ensure there is one overall LFA, DHS is to support DOJ (as delegated to the FBI) until the Attorney General transfers the overall LFA role to DHS.

### **6.5 CHEMICAL / BIOLOGICAL / RADIOLOGICAL / NUCLEAR / EXPLOSIVE CRISIS AND CONSEQUENCE MANAGEMENT**

The potential for widespread effects from a weapon of mass destruction (WMD) event necessitates planning and coordination between Navy responders and local, state and Federal authorities.

Post-incident considerations in addition to those taken for non-WMD attacks include the following:

1. Procedures to quickly identify if an attack involved a chemical / biological / radiological / nuclear / explosive (CBRNE) weapon
2. Decontamination procedures
3. Casualty treatment procedures
4. CBRNE agent containment procedures
5. Personal protective equipment distribution procedures
6. Procedures to notify civilians and other military personnel of a CBRNE attack.

# CHAPTER 7

## Legal Considerations

### 7.1 OVERVIEW

When developing antiterrorism / force protection (ATFP) plans, operational commanders should ensure plans are in compliance with U.S. domestic, international and foreign laws.

Because terrorist incidents are criminal events under U.S. policy, various non-Department of Defense (DOD) government agencies are designated to assume lead response roles. Accordingly, it is important to understand how such interfaces with interagency, international and local agencies affect Navy commands. Each command must be cognizant of these issues and must incorporate the necessary legal guidance into operational ATFP planning. Interagency interfaces are described in more detail in Chapter 6, Antiterrorism / Force Protection Execution.

### 7.2 DEFINITIONS

Legal concepts that affect antiterrorism planning include:

1. **National waters:** Waters subject to the territorial sovereignty of coastal nations. Nations have two types of national waters:
  - a. **Internal waters:** Waters landward of the coastal baseline; normally the coastal low water line (i.e., lakes, rivers, harbors and lagoons). Internal waters have the same legal character as land.
  - b. **Territorial seas:** Measured seaward from the baseline of the coastal nation, subject to coastal nation sovereignty. The United States claims and recognizes, in accordance with the United Nations Convention on the Law of the Sea, territorial sea claims of other nations up to a maximum breadth from the baseline of 12 nautical miles.
2. **Innocent passage:** The right of all ships to engage in continuous and expeditious passage through the territorial sea and archipelagic waters of foreign coastal states in a manner not prejudicial to its peace, good order or security. Passage includes stopping and anchoring, but only if incidental to ordinary navigation or necessary by force majeure or distress, or for the purpose of rendering assistance to persons, ships or aircraft in danger or distress.

There is no right of innocent passage in internal waters and, unless in distress, ships and aircraft may not enter or overfly internal waters without permission of the coastal nation. Within the territorial seas, vessels, but not aircraft, have the right to engage in innocent passage.

3. **International waters:** Waters seaward of the territorial sea, where, for operational purposes, all nations enjoy the freedoms of navigation and overflight.
4. **Inherent right of self-defense:** Individual members of the Armed Forces of the United States, and commanders of units, always have a right to use force in self-defense regardless of where they are in the world. This authority includes the right and obligation to use all necessary means, and to take all appropriate actions, to defend individual members of the Armed Forces and military units from a hostile

## **NWP 3-07.2 (Rev. A)**

act or demonstrated hostile intent. The principles that comprise this right and obligation of U.S. military members and units to act in self-defense, while consistent, are set forth by DOD using different language depending on whether the unit is within U.S. territory and territorial waters or outside this legal boundary. DOD Directive 5210.56 (series), Use of Deadly Force and the Carrying of Firearms by DOD Personnel Engaged in Enforcement and Security Duties, provides guidance on self-defense within the United States and U.S. territorial seas. Outside U.S. territory, the Standing Rules of Engagement (SROE) provide the applicable direction on the use of force in self-defense.

5. **Universal principles of necessity and proportionality as applied to self-defense:** When exercising the use of force in self-defense, any unit or individual servicemember must act according to these principles of universal application:
  - a. **Necessity:** Exists when the use of force becomes necessary as a result of a hostile act or when a force or an individual demonstrates hostile intent.
  - b. **Proportionality:** Based on all facts known to the commander or individual at the time, the force used to counter a hostile act or demonstrated hostile intent must be reasonable in intensity, duration and magnitude.

### **7.3 SELF-DEFENSE**

A commander has the authority and obligation to use all necessary means available and to take all appropriate actions to defend U.S. personnel and units, including elements and personnel or other U.S. forces in the vicinity, against a hostile act or demonstrated hostile intent. In defending against a hostile act or demonstrated hostile intent, commanders will use only that degree of force necessary to decisively counter the hostile act or demonstrated hostile intent and to ensure the continued protection of U.S. forces.

All necessary means available and all appropriate actions may be used in self-defense. There is no checklist that must be followed when deciding whether or not to use force in self-defense. The following guidelines apply for the use of force in self-defense:

1. When time and circumstance permit, the hostile force should be warned, including in some circumstances through the use of warning shots, and given the opportunity to withdraw or cease threatening actions.
2. When use of force in self-defense is necessary, the nature, duration and scope of the engagement should not exceed that which is required to decisively counter the hostile act or demonstrated hostile intent and to ensure continued protection of U.S. forces. Use of deadly force is authorized when such action appears to be the only prudent means to counter the hostile act or hostile intent.

A critical objective of all ATRFP planning is to factor the requisite time and space for U.S. forces to make reasoned decisions regarding the use of force in self-defense. Measures that begin with routine inspection and identification, moving through increasing levels of non-lethal information gathering or non-lethal use of force to the point where deadly force becomes an option, will inform the decision-making process.

The conditions warranting the application of the right of self-defense cannot be precisely defined beforehand but must be left to the sound judgment of trained and responsible Navy personnel. The use of force must be exercised only as a last resort and then only to the extent that is reasonably necessary for self-defense. If there is no longer an imminent threat, force may not be used to inflict punishment for acts already committed. However, so long as the threat to U.S. personnel or forces continues to exist, actions in self-defense may persist.

NTTP 3-07.2.1 (Rev. A), Navy Tactics, Techniques and Procedures, Antiterrorism / Force Protection, provides more detailed discussion on use of deadly force. NWP 1-14M (series), The Commander's Handbook on the Law of Naval Operations, is also recommended for additional insight into these matters.

### **7.3.1 Self-Defense within the United States and Its Territories**

Commanders of Navy ships, aircraft, units and facilities within U.S. territory maintain the inherent right of self-defense, have the authority to enforce security measures and protect persons and property as detailed in DOD Directive 5210.56 (series); DOD Directive 5200.8 (series), Security of Military Installations and Resources; and OPNAVINST 5530.14 (series), Navy Physical Security. The inherent right of self-defense pertains to an unlawful hostile act or demonstrated hostile intent, which includes actual or suspected terrorist incidents. SECNAVINST 5500.29 (series), Use of Deadly Force and the Carrying of Firearms by Personnel of the Department of the Navy in Conjunction with Law Enforcement, Security Duties, and Personal Protection, adopts DOD Directive 5210.56 (series) in its entirety, and through that directive, outlines the use of deadly force and firearms policy and procedures for Navy and Marine Corps personnel regularly engaged in law enforcement and security duties.

DOD Directive 5210.56 (series) and SECNAVINST 5500.29 (series) provide guidance on the use of deadly force within the territory and territorial waters of the United States in Enclosure 2, stating that:

Deadly force is justified only under conditions of extreme necessity and when all three of the following circumstances are present:

1. Lesser means have been exhausted, are unavailable or cannot be reasonably employed;
2. The risk of death or serious bodily harm to innocent persons is not significantly increased by use; and
3. The purpose of the use of deadly force is one or more of the following:
  - a. Self-defense and defense of others when deadly force reasonably appears to be necessary against hostile person(s) to protect law enforcement or security personnel who reasonably believe themselves or others to be in imminent danger of death or serious bodily harm by the hostile person(s).
  - b. Assets involving national security when deadly force reasonably appears to be necessary to prevent the actual theft or sabotage of assets vital to national security. DOD assets shall be specifically designated as "vital to national security" only when their loss, damage or compromise would seriously jeopardize the fulfillment of a national defense mission. Examples of assets vital to national security include nuclear weapons; nuclear command, control and communications; and designated restricted areas containing strategic assets, sensitive codes or special access programs.
  - c. Assets not involving national security but inherently dangerous to others when deadly force reasonably appears to be necessary to prevent the actual theft or sabotage of resources, such as operable weapons or ammunition, that are inherently dangerous to others (i.e., assets that, in the hands of an unauthorized individual, present a substantial potential danger of death or serious bodily harm to others). Examples of assets inherently dangerous to others not related to national security include high-risk portable and lethal missiles, rockets, arms ammunition, explosives, chemical agents and special nuclear material.
  - d. Serious offenses against persons when deadly force reasonably appears necessary to prevent the commission of a serious crime that involves imminent danger of death or serious bodily harm,

## **NWP 3-07.2 (Rev. A)**

including the defense of other persons, where deadly force is directed against the person threatening to commit the crime. Examples of serious offenses against persons include murder, armed robbery and aggravated assault.

- e. Protect public health or safety when deadly force reasonably appears to be necessary to prevent the destruction of public utilities or similar critical infrastructure vital to public health or safety, the damage to which would create an imminent danger of death or serious bodily harm.

DOD Directive 5210.56 (series) also includes arrest, apprehension or escape within the listed situations permitting the use of deadly force under certain circumstances. All personnel engaged in AT / FP missions or law enforcement are recommended to carefully review this directive. Additionally, regarding DOD contract security forces, this directive specifically cautions that the use of deadly force criteria shall be established locally and shall be consistent with both DOD Directive 5210.56 (series) and local laws.

Except within certain designated restricted areas, Navy personnel do not have the authority to act in a law enforcement capacity outside the skin of the ship or outside the confines of an exclusive-use base facility but do have the right to protect military property, facilities and personnel.

Afloat commanders operating outside naval installations should coordinate with the applicable U.S. Coast Guard Captain of the Port and the Navy regional commander to establish security zones when necessary.

### **7.3.2 Naval Vessel Protective Zone**

A naval vessel protective zone (NVPZ) exists around U.S. naval vessels greater than 100 feet in length, including Military Sealift Command vessels, at all times in the navigable waters of the United States, whether the vessel is underway, anchored, moored or within a floating drydock, except when the vessel is moored or anchored within a restricted area or within a naval defensive sea area.

Nothing in the new regulations limits the inherent authority and obligation to use all necessary means available and to take all appropriate actions in self-defense. Entry into a NVPZ, including unauthorized entry into the 100-yard exclusion zone, does not, however, create a tripwire for the use of force. Deliberate disregard of a NVPZ should be viewed as one factor among others to be considered when determining whether DOD personnel are in imminent danger of death or serious bodily harm.

### **7.3.3 Self-Defense outside of the United States**

CJCSI 3121.01A of 15 January 2000, Chairman, Joint Chiefs of Staff Standing Rules of Engagement, implements the inherent right of self-defense and provides guidance for the application of force for mission accomplishment. The SROE are the fundamental policies and procedures governing the actions of U.S. force commanders in the event of a military attack against the United States and during all military operations, contingencies, terrorist attacks or prolonged conflicts outside the territorial jurisdiction of the United States.

The standing rules of engagement:

1. Implement the inherent right of self-defense, applicable worldwide to all echelons of command and personnel.
2. Provide guidance governing the use of force for mission accomplishment.
3. Are used in peacetime operations other than war, during transition from peacetime to armed conflict or war and during armed conflict in the absence of superseding guidance.

Theater-specific ROE may exist in each Combatant Commander's Area of Responsibility (AOR). Depending on the supplemental ROE desired, Combatant Commanders may have the authority to augment or request supplemental SROE. Presidential / Secretary of Defense approval may be required based on the type of supplemental ROE requested by the Combatant Commander.

U.S. Navy ships and forces on the high seas should use appropriate antiterrorism measures consistent with the known threat level in the AOR. Under customary international law, military ships and aircraft are sovereign platforms. Ships and aircraft require specific and advance entry permission (usually referred to as diplomatic clearance) for entry into internal waters or airspace of a foreign country, unless other bilateral or multilateral arrangements have been made. When U.S. forces are operating within internal waters or territory of a foreign nation, the foreign nation has primary responsibility for antiterrorism and law enforcement. Notwithstanding the foreign nation's primary responsibility, the U.S. commander remains ultimately responsible for unit self-defense. Moreover, U.S. Navy ships and aircraft have sovereign immunity from interference by local authorities. Police and port authorities may never legally board a U.S. Navy ship or aircraft to conduct an onboard search or inspection without the permission of the Commanding Officer. If such an inspection or search is desired, commanders should contact the Naval Criminal Investigative Service and the chain of command for guidance.

Commanders help ensure antiterrorism requirements are met by augmenting Host Nation (HN) measures with ship's company or contracted services within the context of local law and applicable international agreements. The defense attaché in each country serves as the official liaison between U.S. military forces and foreign governments. The appropriate naval component commander should provide the guidelines reflected in Status-of-Forces-Agreements (SOFAs) or memoranda of understanding to all commands visiting that nation. Every unit retains the right of self-defense from hostile acts or demonstrated hostile intent, but HN policies may inhibit U.S. forces' ATFP postures.

Civilian mariners (whether government or contractor employees) who operate Military Sealift Command ships (whether government-owned or contractor-owned) are not members of the Armed Forces or Federal law enforcement. In accordance with their civilian status, civilian mariners may not be protected by SOFAs. Consult the applicable SOFA and the AOR chain of command for guidance. Civilian mariners are not governed by military ROE or the Uniform Code of Military Justice.

When an incident occurs in a foreign country, the commander is to take all necessary measures to protect U.S. personnel and assets, and when time permits, notify the chain of command. The theater commander is responsible for notifying the Department of State.

The following unclassified terms and definitions are only applicable to self-defense under the Standing Rules of Engagement:

**Hostile act:** An attack or other use of force against the United States or U.S. forces, and in certain circumstances, U.S. nationals, their property, U.S. commercial assets and / or other designated non-U.S. forces, foreign nationals and their property is considered a hostile act. A hostile act is also force used directly to preclude or impede the mission and / or duties of U.S. forces, including the recovery of U.S. personnel and vital U.S. government property.

**Hostile force:** Any civilian, paramilitary or military force or terrorist, with or without national designation, that has committed a hostile act, exhibited hostile intent or has been declared hostile by appropriate U.S. authority is considered a hostile force.

**Hostile intent:** The threat of imminent use of force against the United States or U.S. forces, and in certain circumstances, U.S. nationals, their property, U.S. commercial assets and / or other designated non-U.S. forces, foreign nationals and their property is considered hostile intent. When hostile intent is present, the right exists to

## **NWP 3-07.2 (Rev. A)**

use proportional force, including armed force, in self-defense by all necessary means available to deter or neutralize the potential attacker or, if necessary, to destroy the threat. A determination that hostile intent exists and requires the use of proportional force in self-defense must be based on evidence that an attack is imminent. Evidence necessary to determine hostile intent will vary depending on the state of international or regional political tensions, military preparations, intelligence and Indications and Warnings information.

**Individual self-defense:** The individual's inherent right of self-defense is an element of unit self-defense. It is critical that individuals are aware and train to the principle that they have the authority to use all available means and to take all appropriate actions to defend themselves and other U.S. personnel in their vicinity. In the implementation of these SROE and other ROE, commanders have the obligation to ensure that the individuals within that commander's unit understand when and how they may use force in self-defense. When individuals assigned to a unit respond to a hostile act or demonstrated hostile intent in the exercise of self-defense, their use of force must remain consistent with the lawful orders of their superiors, the rules contained in this document and other applicable rules of engagement promulgated for the mission or AOR.

**U.S. forces:** All Armed Forces of the United States (including the Coast Guard), any person in the Armed Forces of the United States, and all equipment of any description that either belongs to the U.S. Armed Forces or is being used, escorted or conveyed by U.S. Armed Forces (including Type I and II MSC vessels) are considered U.S. forces.

# INDEX

*Page  
No.*

## A

Assessment Tools.....	5-1
ATFP Plan Development .....	5-3
ATFP Plan.....	6-2

## B

Baseline Security Posture.....	6-2
--------------------------------	-----

## C

Chemical / Biological / Radiological / Nuclear / Explosive Crisis and Consequence Management.....	6-6
Command Responsibilities.....	3-4
Commander Fleet Forces Command.....	4-3
Commander Navy Installations.....	4-4
Course of Action:	
Comparison and Selection .....	5-3
Development .....	5-3
War Gaming.....	5-3

## E

Elements of Terrorists Groups .....	2-1
External Assessment Tools .....	5-2

## F

Force Protection Conditions.....	2-6
----------------------------------	-----

## I

Impact on Command Accountability .....	1-2
Incident Command System .....	4-2
Incident Response .....	6-2
Intelligence and Terrorism .....	3-1
Interagency Coordination.....	4-5
Internal Assessment Tools .....	5-1

## J

Joint Intelligence Centers.....	3-3
---------------------------------	-----

**L**

Lessons Learned..... 1-2

**M**

Maritime Intelligence Centers ..... 3-2  
Mission Analysis ..... 5-3

**N**

National Incident Management System ..... 4-2  
Naval Counterintelligence ..... 3-3  
Naval Vessel Protective Zone ..... 7-3  
NAVNORTH.... 4-4  
Navy Region Commander and Numbered Fleet Commander..... 4-4

**O**

Organization ..... 2-3

**P**

Phases of Post-Incident Response ..... 6-3  
Planning Process ..... 5-3  
Planning Products..... 5-6  
Post-Incident:  
    Command and Control ..... 6-4  
    Response Planning ..... 5-4  
    Response ..... 6-3  
Post-Mission / Deployment Assessments..... 6-2  
Pre-Incident Preparations ..... 6-1

**R**

Random Antiterrorism Measures ..... 6-2  
Risk Assessments ..... 6-1  
Roles and Responsibilities ..... 3-1

**S**

Secretary of Homeland Security..... 4-1  
Secretary of State ..... 4-2  
Secretary of the Navy and Chief of Naval Operations ..... 4-3  
Self-Defense ..... 7-2  
    Outside of the United States ..... 7-3  
    Within the United States and Its Territories..... 7-3

**T**

Terrorist:

Attack Preparations .....	2-4
Operations .....	2-3
Threat Levels .....	2-4
Threat Analysis .....	6-1
Transition .....	5-4

**U**

Unified Commander .....	4-3
-------------------------	-----



LIST OF EFFECTIVE PAGES

Effective Pages	Page Numbers
Original	1 (Reverse Blank)
Original	3 (Reverse Blank)
Original	5 (Reverse Blank)
Original	7 thru 28
Original	1-1 thru 1-2
Original	2-1 thru 2-7 (Reverse Blank)
Original	3-1 thru 3-5 (Reverse Blank)
Original	4-1 thru 4-5 (Reverse Blank)
Original	5-1 thru 5-7 (Reverse Blank)
Original	6-1 thru 6-6
Original	7-1 thru 7-6
Original	Index-1 thru Index-3 (Reverse Blank)
Original	LEP-1 (Reverse Blank)





**NWP 3-07.2 (REV. A)**