

**NAVY WARFARE PUBLICATION**

**NAVY DOCTRINE FOR  
ANTITERRORISM/FORCE  
PROTECTION  
NWP 3-07.2**

DEPARTMENT OF THE NAVY  
OFFICE OF THE CHIEF OF NAVAL OPERATIONS

THIS PUBLICATION IS REQUIRED FOR OFFICIAL USE OR FOR ADMINISTRATIVE OR OPERATIONAL PURPOSES ONLY. DISTRIBUTION IS AUTHORIZED TO U.S. GOVERNMENT AGENCIES ONLY. OTHER REQUESTS FOR THE DOCUMENT MUST BE HANDLED IN ACCORDANCE WITH SECNAVINST 5510.31 SERIES.

PRIMARY REVIEW AUTHORITY:  
OPNAV N34 (V13)



0411LP1008888

*1 (Reverse Blank)*

ORIGINAL





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

September 2001

LETTER OF PROMULGATION

1. NWP 3-07.2, 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 is effective upon receipt.
3. SECNAVINST 5510.31 provides procedures for disclosing this publication or portions thereof to foreign governments or international organizations.



R. G. SPRIGG



September 2001

**PUBLICATION NOTICE**

**ROUTING**

1. NWP 3-07.2, NAVY DOCTRINE FOR ANTITERRORISM/FORCE PROTECTION, is available in the Navy Warfare Library and is effective upon receipt.
2. Summary: NWP 3-07.2, NAVY DOCTRINE FOR ANTITERRORISM/FORCE PROTECTION addresses the development and implementation of measures to deter and defeat terrorist attacks against U.S. Navy forces. It supports the Navy operational concept by providing general service guidance and identifying significant issues for Navy forces.

---



---



---



---



---



---



---



---



---



---



---

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

		<i>Page No.</i>
<b>CHAPTER 1 — INTRODUCTION</b>		
1.1	PURPOSE . . . . .	1-1
1.2	BACKGROUND . . . . .	1-1
1.3	SCOPE . . . . .	1-2
<b>CHAPTER 2 — TERRORIST THREAT</b>		
2.1	OVERVIEW . . . . .	2-1
2.2	TERRORIST GROUPS . . . . .	2-1
2.3	TERRORIST TACTICS . . . . .	2-1
2.4	TERRORIST ATTACK METHODOLOGY . . . . .	2-2
2.4.1	Phase One — Target Options . . . . .	2-3
2.4.2	Phase Two — Selection Surveillance . . . . .	2-3
2.4.3	Phase Three — Target Selection . . . . .	2-3
2.4.4	Phase Four — Detailed Surveillance . . . . .	2-3
2.4.5	Phase Five — Training and Preparation . . . . .	2-3
2.4.6	Phase Six — The Attack . . . . .	2-3
2.5	TERRORIST THREAT LEVELS . . . . .	2-3
2.6	TERRORIST FORCE PROTECTION CONDITIONS . . . . .	2-4
2.7	CONCLUSION . . . . .	2-5
<b>CHAPTER 3 — INTELLIGENCE, COUNTERINTELLIGENCE, AND THREAT ANALYSIS</b>		
3.1	OVERVIEW . . . . .	3-1
3.2	TERRORISM . . . . .	3-1
3.3	THE INTELLIGENCE PROCESS . . . . .	3-1
3.3.1	Defining Intelligence . . . . .	3-2
3.4	TASKING THE UNITED STATES INTELLIGENCE COMMUNITY . . . . .	3-2
3.4.1	Navy Intelligence . . . . .	3-2
3.4.2	Counterterrorism/Counterintelligence Centers . . . . .	3-4

3.5 NAVY ANTITERRORIST ALERT CENTER/BLUE DART  
MESSAGE PROCEDURES . . . . . 3-7

3.6 SUMMARY . . . . . 3-8

**CHAPTER 4 — LEGAL CONSIDERATIONS**

4.1 OVERVIEW . . . . . 4-1

4.2 GENERAL . . . . . 4-1

4.3 DEFINITIONS OF LEGAL TERMS . . . . . 4-2

4.4 AUTHORITY AND ACTIONS TO EXERCISE SELF-DEFENSE . . . . . 4-3

4.5 CONSIDERATIONS FOR CIVILIAN-CREWED SHIPS OPERATED  
BY OR FOR THE MILITARY SEALIFT COMMAND . . . . . 4-4

4.6 UNITED STATES TERRITORY ANTITERRORISM/FORCE  
PROTECTION LEGAL PLANNING . . . . . 4-4

4.7 FOREIGN OR NON-UNITED STATES TERRITORY ANTITERRORISM/FORCE  
PROTECTION LEGAL PLANNING . . . . . 4-4

4.8 ONGOING/IN-PROGRESS TERRORIST INCIDENT PLANNING. . . . . 4-5

**CHAPTER 5 — THE NAVY ANTITERRORISM/FORCE PROTECTION PROGRAM**

5.1 INTRODUCTION . . . . . 5-1

5.2 PROGRAM CONCEPT . . . . . 5-1

5.3 COMMANDER’S RESPONSIBILITY . . . . . 5-2

5.4 IMPLEMENTING THE NAVY ANTITERRORISM/FORCE  
PROTECTION PROGRAM . . . . . 5-2

5.4.1 Antiterrorism/Force Protection Plans . . . . . 5-2

5.4.2 Antiterrorism Officer Responsibilities . . . . . 5-4

5.4.3 Antiterrorism/Force Protection Board . . . . . 5-4

5.4.4 Security Forces . . . . . 5-4

5.5 ANTITERRORISM/FORCE PROTECTION ASSESSMENT PROCESS . . . . . 5-4

5.5.1 Threat Assessment . . . . . 5-5

5.5.2 Vulnerability Assessment . . . . . 5-5

5.5.3 Risk Assessment . . . . . 5-5

5.6 NAVY ANTITERRORISM/FORCE PROTECTION PROGRAM  
COORDINATION . . . . . 5-5

5.6.1 Operations Within United States Territory. . . . . 5-5

5.6.2 Operations Outside United States Territory . . . . . 5-6

5.7 HIGH SEAS ANTITERRORISM/FORCE PROTECTION PROGRAM. . . . . 5-6

	<i>Page No.</i>
5.8 POST MISSION/DEPLOYMENT ASSESSMENT . . . . .	5-6
<b>CHAPTER 6 — CONSEQUENCE MANAGEMENT</b>	
6.1 OVERVIEW . . . . .	6-1
6.2 GENERAL . . . . .	6-1
6.3 CONSEQUENCE MANAGEMENT PLANNING . . . . .	6-1
6.3.1 Phase One — Impacts and Consequences . . . . .	6-1
6.3.2 Phase Two — Resources Required . . . . .	6-2
6.3.3 Phase Three — Training and Exercising . . . . .	6-2
<b>INDEX . . . . .</b>	<b>Index-1</b>

# LIST OF ILLUSTRATIONS

*Page  
No.*

## **CHAPTER 2 — TERRORIST THREAT**

Figure 2-1. Terrorist Force Protection Conditions . . . . . 2-5

## **CHAPTER 3 — INTELLIGENCE, COUNTERINTELLIGENCE, AND THREAT ANALYSIS**

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

Figure 3-2. Counterterrorist and Counterintelligence Organizations . . . . . 3-5

## **CHAPTER 5 — THE NAVY ANTITERRORISM/FORCE PROTECTION PROGRAM**

Figure 5-1. DOD Antiterrorism Organization . . . . . 5-3

# REFERENCES

## DOD PUBLICATIONS

DODD 2000.12, DOD Combatting Terrorism Program.

DOD Handbook 2000.12-H, Protection of DOD Personnel and Activities Against Acts of Terrorism and Political Turbulence.

DODI 2000.14, DOD Combatting Terrorism Program Procedures.

DODI 2000.16, DOD Combatting Terrorism Program Standards.

DODD 5200.8, Security of Military Installations and Resources.

DOD 4500.54-G, Foreign Clearance Guide.

DODD 5200.8-R, Physical Security Program.

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

DODD 5225.5, DOD Cooperation With Civilian Law Enforcement Officials.

## JOINT PUBLICATIONS

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

Joint Staff Guide 5260, Service Member's Personal Protection Guide.

Joint Staff Pamphlet 5260, Coping With Violence.

CJCSI 5261.01, Combatting Terrorism Readiness Initiatives Fund.

JP 3-07, Joint Doctrine for Military Operations Other Than War.

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

## NAVY INSTRUCTIONS

SECNAVINST 5500.4G, Reporting of Missing, Lost, Stolen, or Recovered Government Property.

SECNAVINST 5500.29B, 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 5520.3B, Criminal and Security Investigations and Related Activities Within the Department of the Navy.

SECNAVINST 5530.4B, Naval Security Forces Ashore and Afloat.

OPNAVINST 3100.6, Special Incident Reporting.

## **NWP 3-07.2**

OPNAVINST 3300.53, Navy Combatting Terrorism Program.

OPNAVINST 3300.54, Protection of Naval Personnel and Activities Against Acts of Terrorism and Political Turbulence.

OPNAVINST 3300.55, Navy Combatting Terrorism Program Standards.

NAVFACINST 3440.17C, CBR-D.

OPNAVINST 3591.1C, Small Arms Training and Qualification.

OPNAVINST 5510.1H, Department of the Navy Information and Personal Security Program Regulation.

SECNAVINST 5510.36, Info Security Program.

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

OPNAVINST 5530.14B, Physical Security and Loss Prevention Manual.

OPNAVINST 5580.1, Department of the Navy Law Enforcement.

### **THEATER COMMANDER PUBLICATIONS**

USCINCPACINST 3850.2J, Antiterrorism Program.

USCINCCENT OPORD 97-01, Force Protection (used as background only).

### **FLEET COMMANDER PUBLICATIONS**

CNC/C5F OPORD 1000-96, Appendix 16, Annex C (replaced), Security and Antiterrorism.

CUSNC/C5F OPORD 98-01, Force Protection.

COMSEVENTHFLT OPORD 201, Appendix 27, Annex C, Anti-Terrorist Defense.

COMSEVENTHFLT OPORD 201, Appendix 28, Annex C, Anti-Piracy Defense.

C3F OPORD 201, Antiterrorism/Force Protection.

### **KEY MESSAGES**

CNO 310035Z OCT 00, SECNAV DEPARTMENT OF THE NAVY FORCE PROTECTION TASK FORCE (establishment & first principles).

CNO 222216Z NOV 00, SECNAV DEPARTMENT OF THE NAVY FORCE PROTECTION TASK FORCE (basic tenets).

CNO 050014Z DEC 00, SECNAV DEPARTMENT OF THE NAVY FORCE PROTECTION TASK FORCE (tasks).

CNO 030013Z FEB 01, FORCE PROTECTION SEA CHANGE.

SECSTATE 202316Z MAR 01, INTENSIFIED SECURITY FOR FORCE PROTECTION.

SECDEF 061702Z APR 01, DEPARTMENT OF DEFENSE DEPARTMENT OF STATE THREAT LEVEL METHODOLOGIES.

**TACMEMOS/TACNOTES**

COMTHIRDFLT TACMEMO 3-07-1-98, Maritime Antiterrorism Tactics.

SWDG TACMEMO 3-20.4-01, Surface Ship Force Protection/Antiterrorism in an Asymmetrical Threat Environment.

**LESSONS LEARNED**

Crouch, Gehman report, USS Cole Bombing report.

Downing Commission report, Khobar Towers Bombing report.

NLLS Website (SIPRNET) or NLLS CD-ROM, Various LL from operations and exercises.

**OTHER DOCUMENTS**

OPNAVINST 5530.xx (Draft), Force Protection Afloat.

C2F/C3F INST 3500.3 (Draft), Fifth Fleet AOR Deployer and Operations Training Guide.

Dept of State Publication 10433, Patterns of Global Terrorism 1996.

Joint Warfighting Center Handbook, Joint Task Force Commander's Handbook for Peace Operations, June 1997.

DOD Card, Antiterrorism Individual Protection Measures.

Dept of the Navy Booklet, Antiterrorism/Force Protection for Naval Operations, Commander's Guide.

NCIS Pamphlet, Antiterrorism Travel Security Measures.

USC 49 46501 (2), Special Aircraft Jurisdiction of the U.S.

USC 50 191, Magnuson Act.

USC 50 797, Internal Security Act.

USC 18 1385, Posse Comitatus Act.



# GLOSSARY

## A

**antiterrorism (AT).** 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 overarching Force Protection and Combatting Terrorism programs. An antiterrorism program is a collective effort that seeks to reduce the likelihood that DOD 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. (Joint Pub 1-02, OPNAVINST 3300.53A)

**antiterrorism awareness.** Fundamental knowledge of the terrorist threat and measures to reduce personal vulnerability to terrorism. (Joint Pub 1-02)

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

**antiterrorism officer (ATO).** 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 (FPO), changed to ATO by direction of DODINST 2000.16 revision of June, 2001.

**area of operations (AO).** An operational area defined by the Joint Force Commander for land and naval forces. Areas of operation do not typically encompass the entire operational area of the Joint Force Commander, but should be large enough for component commanders to accomplish their missions and protect their forces. (Joint Pub 1-02)

### area of responsibility (AOR)

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. (Joint Pub 1-02)

## B

**BLUE DART message.** Time sensitive terrorist incident notification message. Initiated by the Navy Antiterrorist Alert Center to provide commands immediate indications and warning of the high potential for, and imminent threat of, a terrorist incident.

## C

**captain of the port (COTP).** COTPs enforce within their jurisdictions, port safety, security, and marine environmental protection regulations including, without limitation, regulations for the protection and security of vessels, harbors, and waterfront facilities, anchorages, security zones, safety zones, regulated navigation areas, deep-water ports, water pollution, and ports and waterway safety. (33 CFR 1.01-30)

**combatting terrorism (CBT).** 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

## NWP 3-07.2

throughout the entire threat spectrum, to include terrorist use of chemical, biological, radiological, nuclear materials or high-yield explosive devices. (Joint Pub 1-02, OPNAVINST 3300.53A)

**consequence management (CM).** Interagency services and emergency response force actions essential to mitigate and recover from damage, loss, hardship or suffering resulting from disasters or catastrophes, either man-made or natural.

**counterintelligence (CI).** 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, or foreign persons, or international terrorist activities. (Joint Pub 1-02)

**counterintelligence support.** Conducting counterintelligence activities to protect against espionage and other foreign intelligence activities, sabotage, international terrorist activities, or assassinations conducted for, or on behalf of, foreign powers, organizations, or persons. (Joint Pub 1-02)

**counterterrorism (CT).** Offensive measures taken to prevent, deter, and respond to terrorism. (Joint Pub 1-02)

**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

**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. (Joint Pub 1-02)

### E

**explosive ordnance disposal (EOD).** 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. (Joint Pub 1-02)

### F

**force protection (FP).** 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 combatting terrorism, physical security, operations security, personal protective services, and supported by intelligence, counterintelligence, and other security programs. (Joint Pub 1-02)

### H

**hostage.** A person held as a pledge that certain terms or agreements will be kept. The taking of hostages is forbidden under the Geneva Conventions, 1949. (Joint Pub 1-02)

**host nation (HN).** 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. (Joint Pub 1-02)

**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. (Joint Pub 1-02)

### I

**improvised explosive device (IED).** 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. (Joint Pub 1-02)

**incident control point (ICP).** A designated point close to an incident where crisis management forces will rendezvous and establish control capability before initiating a tactical reaction. (Joint Pub 1-02)

**initial response force.** The first unit, usually military police, on the scene of a terrorist incident. (Joint Pub 1-02)

**installation.** A grouping of facilities, located in the same vicinity, that support particular functions. Installations may be elements of a base. (Joint Pub 1-02)

**installation commander.** The individual responsible for all operations performed by an installation. (Joint Pub 1-02)

**insurgent.** Member of a political party who rebels against established leadership. (Joint Pub 1-02)

## 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. (Joint Pub 1-02)

## L

**law enforcement agency (LEA).** Any of a number of agencies (outside the Department of Defense) chartered and empowered to enforce U.S. 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 within the borders of a host nation. (Joint Pub 1-02)

**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. (Joint Pub 1-02)

**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. (DOD Instruction 2000.16)

**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 and provide level I instruction for coded billets. (DOD Instruction 2000.16)

## M

**memorandum of understanding (MOU).** 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 Inter-Service support agreement. (NWP 4-08)

**military operations other than war (MOOTW).** Operations that encompass the use of military capabilities across the range of military operations short of war. These military actions can be applied to complement any combination of the other instruments of national power and occur before, during, and after war. (Joint Pub 1-02)

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. (Joint Pub 1-02)

**port security.** The safeguarding of vessels, harbors, ports, waterfront facilities, and cargo from internal threats such as destruction, loss, or injury from sabotage or other subversive acts; accidents; thefts; or other causes of similar nature. (Joint Pub 1-02)

R

**random antiterrorism measures (RAM).** 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. (MCO 3302.1B)

**risk assessment.** The identification and assessments of hazards (first two steps of risk management process). (Joint Pub 1-02)

**risk management.** A process by which decision makers reduce or offset risk. (Joint Pub 1-02)

S

**status-of-forces agreement (SOFA).** 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. (Joint Pub 1-02)

T

**terrorist force protection conditions.** The progressive level of protective measures implemented by all DOD components in response to terrorist threats in accordance with DOD Directive 0-2000.12. The terrorist force protection condition system complements the national level intelligence community assessment of terrorist intentions and capabilities. Note: Previously known as Threat Condition (THREATCON).

**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 terrorist 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 (TA).** 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 (VA).** 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. (Joint Pub 3-07.2)

# LIST OF ACRONYMS AND ABBREVIATIONS

## A

- ACIC.** Army Counterintelligence Center.
- AFOSI.** Air Force Office of Special Investigations.
- AO.** Area of operations.
- AOI.** Area of interest.
- AOR.** Area of responsibility.
- ARG.** Amphibious ready group.
- AT.** Antiterrorism.
- ATAC.** Navy Antiterrorist Alert Center.
- ATACSUM.** Antiterrorist Alert Center summary.
- AT/FP.** Antiterrorism/force protection.
- ATG.** Afloat training group.
- ATO.** Antiterrorism officer.

## B

- BAF.** Backup alert force.
- BG.** Battle group.

## C

- CDO.** Command duty officer.
- CI.** Counterintelligence.
- CIA.** Central Intelligence Agency.
- CINC.** Commander in chief.
- CIP.** Counterterrorism information portal.
- CISO.** Counterintelligence staff officers.
- CNOIVA.** CNO installation vulnerability assessment.
- CO.** Commanding officer.

**CT.** Counterterrorism.

**CTC.** Counterterrorist center.

**D**

**DATT.** Defense attaché.

**DESRON.** Destroyer squadron.

**DIA.** Defense Intelligence Agency.

**DOJ.** Department of Justice.

**DOS.** Department of State.

**E**

**EAP.** Emergency action plan.

**EOD.** Explosive ordnance disposal.

**F**

**FAA.** Federal Aviation Administration.

**FAST.** Fleet antiterrorism security team.

**FBI.** Federal Bureau of Investigation.

**FP.** Force protection.

**FTC.** Fleet training center.

**H**

**HN.** Host nation.

**HPU.** Harbor Patrol Unit (USN).

**HRB.** High risk billet.

**HRP.** High risk personnel.

**HUMINT.** Human intelligence.

**I**

**I&W.** Indications and warning.

**IC.** Intelligence community.

**ICC.** Intelligence Coordination Center (USCG).

**ICP.** Incident control point.

## **NWP 3-07.2**

**IDS.** Intrusion detection system.

**IED.** Improvised explosive device.

**IICT.** Interagency Intelligence Committee on Terrorism.

**INR.** Bureau of Intelligence and Research, Department of State.

**IO.** Information operations.

**ISIC.** Immediate superior in command.

**IW.** Information warfare.

### **J**

**JAC.** Joint Analysis Center.

**JCS.** Joint Chiefs of Staff.

**JFIC.** Joint Forces Intelligence Command.

**JICCEN.** Joint Intelligence Center, Central Command.

**JICPAC.** Joint Intelligence Center, Pacific Command.

**JSIVA.** Joint staff integrated vulnerability assessment.

**JTTP.** Joint tactics, techniques, and procedures.

**JULLS.** Joint universal lessons learned system.

### **L**

**LEA.** Law enforcement agency.

**LEDET.** Law Enforcement Detachment (USCG).

**LFA.** Lead federal agency.

### **M**

**MAA.** Master at arms.

**MCIA.** Marine Corps intelligence activity.

**MOOTW.** Military operations other than war.

**MOU.** Memorandum of understanding.

**MSC.** Military sealift command.

**MTT.** Mobile training team.

## N

**NCC.** Navy component commander.

**NCIS.** Naval Criminal Investigative Service.

**NLLS.** Navy lessons learned system.

**NMETL.** Navy mission essential task list.

**NMIC.** National Maritime Intelligence Center.

**NSA.** National Security Agency.

## O

**OIC.** Officer in charge.

**ONI.** Office of Naval Intelligence.

**OOD.** Officer of the deck.

**OPLAN.** Operation plan.

**OPSEC.** Operations security.

## P

**PAO.** Public affairs office.

**PCO.** Prospective commanding officer.

**PIR.** Priority intelligence requirements.

**PIVA.** Port integrated vulnerability assessment.

**PSP.** Physical security plan.

**PSU.** Port Security Unit (USCG).

**PXO.** Prospective executive officer.

## R

**RAM.** Random antiterrorism measures.

**RFI.** Request for information.

**ROE.** Rules of engagement.

## S

**SAC.** Special agent in charge.

**SAMI.** Small arms instructor course.

## **NWP 3-07.2**

**SAT.** Security alert team.

**SCI.** Sensitive compartmented information.

**SCIO.** Staff counterintelligence officer.

**SETL.** Security Environment Threat List.

**SIGINT.** Signals intelligence.

**SOFA.** Status-of-forces agreement.

**SOPA.** Senior officer present afloat.

**SROE.** Standing rules of engagement.

**SSDF.** Ship self defense force.

**STWO.** Staff tactical watch officer course.

**SWDG.** Surface warfare development group.

## **T**

**TA.** Threat assessment.

**TACON.** Tactical control.

**THREATCON.** Threat condition.

**TWC.** Threat Warning Center, DIA Office for Counterterrorism.

## **U**

**UCMJ.** Uniform code of military justice.

**USDAO.** United States Defense Attaché Office.

## **V**

**VA.** Vulnerability assessment.

## **W**

**WMD.** Weapon(s) of mass destruction.

# PREFACE

NWP 3-07.2, Navy Doctrine for Antiterrorism/Force Protection, addresses the development and implementation of measures to deter and defeat terrorist attacks against U.S. Navy forces. It supports the Navy operational concept and joint publications concerning antiterrorism/force protection. NWP 3-07.2 provides general guidance and identifies significant issues commanders should address in the realm of 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.

Make changes to the distribution and allowance lists (to add or delete your command from the distribution list, or to modify the number of copies of a publication that you receive) in accordance with NTTP 1-01.

## RECOMMENDED CHANGES

Submit recommended changes to this publication at any time using the accompanying format for routine changes. Fleet units and stations submit recommendations through their 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:

COMMANDER  
NAVWARDEVCOM  
686 CUSHING RD  
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 (NWDC) SIPRNET home page at <http://www.nwdc.navy.smil.mil>.

## 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 OPNAV N34, with information copies to NWDC, and all other concerned commands, clearly explaining, with appropriate justification, the proposed change. Information addressees should comment as appropriate. See NTTP 1-01.

	(CLASSIFICATION)				
<b>RECOMMENDED CHANGE TO:</b> _____	(PUBLICATION NUMBER / REVISION / CHANGE)	<b>DATE:</b> _____			
<b>LOCATION:</b> _____	(PAGE)	(PARA)	(LINE)	(FIG. NO.)	
<b>TYPE OF CHANGE:</b>	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>					
_____		_____		_____	
(ORIGINATING COMMAND)		(ORIGINATOR SEQUENCE NO.)			
_____		_____		_____	
(POINT OF CONTACT)		(PHONE - IDENTIFY DSN OR COMM)			
<b>PRA ACTION:</b>	ACCEPTED _____	MODIFIED _____	REJECTED _____		
<b>REMARKS:</b> (USE ADDITIONAL SHEETS IF NEEDED)					
_____		_____		_____	
(PRA POINT OF CONTACT)		(PHONE - IDENTIFY DSN OR COMM)			
<b>CONFERENCE DATE:</b> _____			<b>CONFERENCE AGENDA ITEM NO.:</b> _____		
			PAGE _____ OF _____		
			(CLASSIFICATION)		

FM ORIGINATOR  
 TO CNO WASHINGTON DC//N34//  
 INFO CINCLANTFLT NORFOLK VA//N3/N5/N46//  
 CINCPACFLT PEARL HARBOR HI//N3/N5/N46//  
 COMNAVWARDEVCOM NEWPORT RI//N5//  
 NAVWARDEVCOM DIVISION WASHINGTON DC//TT40//  
 (Others as appropriate)

BT  
 CLASSIFICATION//N03510//  
 MSGID/GENADMIN/(Organization ID)//  
 SUBJ/URGENT CHANGE RECOMMENDATION FOR NWP 3-07.2//  
 REF/A/DOC/NWDC/01FEB2001//  
 AMPN/REF A IS NTPP 1-01 WHICH DELINEATES PROCEDURES FOR  
 MANAGEMENT OF THE NWP SYSTEM.//  
 POC/(Command Representative)//  
 RMKS/ 1. IAW REF A URGENT CHANGE IS RECOMMENDED FOR NWP 3-07.2  
 2. PAGE \_\_\_\_\_ 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.*

**CHANGE SYMBOLS**

Revised text in changes is indicated by a black vertical line in either 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 material added or information restated. A change symbol in the margin by the chapter number and title indicates a new or completely revised chapter.

# CHAPTER 1

## Introduction

### 1.1 PURPOSE

This NWP is intended to be a single source reference for antiterrorism/force protection (AT/FP) doctrine applicable to Navy shore, aviation, and afloat units. It reflects doctrine and guidance produced by the Joint Chiefs of Staff (JCS), the Secretary of the Navy, Chief of Naval Operations, and the Department of Defense (DOD). This publication covers antiterrorism concepts, terrorism threat issues, antiterrorism guidance and direction.

This NWP should be used in conjunction with NTTP 3-07.2.1, Navy Tactics, Techniques, and Procedures for Antiterrorism/Force Protection. NTTP 3-07.2.1 provides detailed examples and instructions for commanders to use in developing and implementing effective AT/FP programs.

### 1.2 BACKGROUND

The term “terrorism” is defined in Joint Pub 1-02, the Department of Defense Dictionary of Military and Associated Terms, 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.” This definition is the foundation throughout this publication for the guidance to commanders at all levels. Specific policy and directive guidance for the DOD Combatting Terrorism Program is contained in DOD Directive 2000.12.2.

Terrorism can be waged by small groups and, if successful, can have significant impact on U.S. interests and policy. Initially it appears the terrorist has all of the advantages — he chooses 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 are often large, identifiable symbols of the U.S. Government and ideal targets for terrorists seeking to change U.S. government policies at home or abroad.

As acts of terrorism increasingly become the preferred tactic used by groups unwilling or unable to directly challenge U.S. military strength, it becomes imperative for Navy forces to recognize that success in the fight against terrorism requires the same degree of focus, intensity, preparation, and training afforded more traditional warfare areas. Combatting terrorism involves actions, including *antiterrorism* (defensive measures used to reduce the vulnerability to terrorist acts) and *counterterrorism* (offensive measures taken to prevent, deter, and respond to terrorism), taken to oppose terrorism throughout the entire threat spectrum. This publication focuses on antiterrorism. The following definitions are provided to assist in understanding the difference between antiterrorism and counterterrorism.

1. Antiterrorism (AT) includes defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military forces. (Joint Pub 1-02)
2. Counterterrorism (CT) involves those offensive measures taken to prevent, deter, and respond to terrorism. Sensitive and compartmented counterterrorism programs are addressed in relevant National Security Decision Directives, National Security Directives, contingency plans, and other relevant classified documents. (Joint Pub 1-02)

Antiterrorism, as discussed throughout this publication, is an element of a broader concept called force protection. The term “force protection” (FP) is defined as a security program designed to protect service members, civilian employees, family members, facilities, and equipment in all locations and situations, accomplished through planned and

## **NWP 3-07.2**

integrated application of combatting terrorism, physical security, operations security (OPSEC), personal protective services, and supported by intelligence, counterintelligence (CI), and other security programs. (Joint Pub 1-02)

AT/FP should be considered a Navy core competency and therefore a critical part of every mission area. Planning for all operations should include considerations for AT/FP in order to maintain the readiness and effectiveness of Navy forces. It must be understood that AT/FP efforts complement unit mission areas rather than preclude them. Through balanced programs that include awareness, training, and specialized equipment, integrated with the effective policies and doctrine, the Navy establishes and maintains a posture to deter and defeat all threats, including terrorism.

FP is an overarching program designed to protect U.S. armed forces assets (personnel, material, and equipment) from those personnel or organizations that intend political advance against United States interests, policies, and goals by damaging equipment or intimidating, injuring, maiming, kidnapping, or killing United States military personnel and their dependents. It encompasses a number of programs including, but not limited to, antiterrorism, physical security, OPSEC, information security, and intelligence gathering. This effort is based on the 31 performance standards delineated in Department of Defense Instruction 2000.16, Combatting Terrorism Program Standards.

The Navy AT/FP program focuses on preventing terrorist attacks on Navy assets and personnel through education and training. Beginning at the initial entry level training and continuing through an entire career, the program seeks to build an awareness and warrior mindset toward AT/FP in every sailor and give them the skills necessary to identify and respond to terrorist acts. This warrior mindset is vital to empowering our personnel to meet the terrorist threats they face both in U.S. territory and abroad. Navy personnel must incorporate the same warrior spirit into AT/FP that they have developed to support traditional warfare areas.

The goal of the Navy's AT/FP program is to deter, deny, and defeat terrorism. Deterrence involves projecting a visible ability to defeat a terrorist attack. Although terrorists may be willing to give their lives for an attack, they are generally less willing to die in a failed effort. Skilled and trained Navy personnel actively defending their unit or facility are an effective deterrent to terrorists. The purpose of denial is to prevent terrorists from finding a seam they can exploit. This encompasses everything from providing accurate intelligence to ensuring adequate standoff distances around units and installations. The last principle of the Navy's program is to defeat the terrorist using active measures up to, and including the use of force.

Combatting terrorism is the responsibility of every individual in the Navy. Each individual must recognize his/her responsibility and be capable of identifying and reacting to a potential threat. One of the critical goals of the AT/FP program is to make every set of eyes and ears in the Navy into a detector focused on identifying potential terrorist threats.

### **1.3 SCOPE**

This NWP is applicable to all Navy units and commands to include ships, aircraft squadrons, shore installations, and other types of units, within U.S. or foreign territory, and in transit. It is intended to provide doctrine and policy to assist Navy forces in designing, developing, implementing, and evaluating effective programs to reduce the risk of a terrorist attack and mitigate its effects should one occur. This NWP 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.

# CHAPTER 2

## Terrorist Threat

### 2.1 OVERVIEW

This chapter provides commanders with background information concerning the terrorist threat to enable better review and implementation of AT/FP procedures for their units.

### 2.2 TERRORIST GROUPS

A terrorist group's selection of targets and tactics is often a function of the group's affiliation, level of training, organization, sophistication, and opportunity. There is a considerable body of research attempting to categorize terrorist groups by government affiliation and motivation. It is important to understand a potential adversary's goals, philosophies, and strategies in order to effectively plan for a defense against that adversary's tactics. For this reason, commanders and all individuals actively involved in developing AT/FP defenses must seek out available sources of information concerning terrorists. A list of AT/FP references used in the production of this publication should be used as an example of materials that should be held by the command and/or reviewed. The majority of the cited documents may be obtained electronically via DOD, Joint Staff, and OPNAV AT/FP websites.

The U.S. Department of State (DOS) publishes an annual report entitled, "Patterns of Global Terrorism," summarizing trends in terrorism. The current and past years' reports can be found on the U.S. State Department website at [www.state.gov/s/ct/rls/pgrtrpt/](http://www.state.gov/s/ct/rls/pgrtrpt/) along with other counterterrorism documents. One of the report's appendices describes designated foreign terrorist organizations and includes a description of the group, its strength, activities, area(s) of operation (AO), and sources of external aid.

### 2.3 TERRORIST TACTICS

Terrorist tactics vary in sophistication according to the level of training the individual or group has received. The objectives and sophistication of the terrorist group will dictate, to some degree, the tactics used. Terrorist objectives may include attracting publicity for a group's cause, demonstrating the group's power or the existing government's lack of power, exacting revenge, or causing government overreaction. Regardless of the tactics or objectives, terrorists seek to identify and exploit vulnerabilities or seams in security.

A critical factor in understanding terrorism is the emotional impact of the terrorist act on an audience other than the victim. The terrorist of today will exploit information operations (IO) against the United States as much as the media will allow. News media coverage is important to terrorists who are attempting to incite public fear or gain attention for their cause. Another determinant of tactics and target selection is the role the terrorist group perceives itself as playing. Terrorism can be used as either an overt or a covert aspect of a political movement engaged in a power struggle within an existing political system. Terrorists frequently claim affiliation with causes or political organizations to give their actions a claim to respectability. Terrorist tactics are criminal violations that require expert criminal investigation with a goal toward prosecution. Common terrorist tactics include:

1. Assassination. A term generally applied to the killing of prominent persons and symbolic enemies as well as traitors who defect from the group.
2. Arson. Arson is the crime of maliciously setting fire to a building or the property of another person. Less dramatic than most tactics, arson has the advantage of low risk to the perpetrator and requires only a low level of technical knowledge.

3. **Bombing.** The bomb, or improvised explosive device (IED), is the terrorist's weapon of choice. Bombings have accounted for over one-half of all recorded international terrorist attacks since 1983. IEDs are inexpensive to produce and can range from very basic to highly sophisticated devices. They are generally of low risk to the perpetrator but suicide bombings are becoming increasingly prevalent. A devoted terrorist willing to sacrifice his/her life can cause tremendous damage as demonstrated by the 1983 vehicle bombing of the U.S. Marine barracks in Beirut, or the 2000 small boat bombing of the USS Cole in Yemen.
4. **Hostage Taking.** This usually is an overt seizure of one or more individuals with the intent of gaining publicity or other concessions in return for release of the hostages. While dramatic, hostage and hostage barricade situations are risky for the perpetrator.
5. **Kidnapping.** While similar to hostage taking, kidnapping has significant differences. Kidnapping is usually a covert seizure of one or more specific persons in order to exact specific demands. The perpetrators of the action may not be known for a long time. News media attention is initially intense but decreases over time. Because of the time involved, successful kidnapping requires elaborate planning and logistics. The risk to the terrorist is less than in the hostage situation.
6. **Hijacking or Skyjacking.** Sometimes employed as a means for escape, hijacking is normally carried out to produce a spectacular hostage situation. Although trains, buses, and ships have been hijacked, aircraft are the preferred target because of their greater mobility and vulnerability.
7. **Seizure.** Seizure usually involves a building or object that has value in the eyes of the audience. There is some risk to the terrorist because security forces have time to react and may opt to use force to resolve the incident, especially if few or no innocent lives are involved.
8. **Raids or Attacks on Facilities.** Armed attacks on facilities are usually undertaken for one of three purposes: to gain access to radio or television broadcast capabilities in order to make a statement; to demonstrate the government's inability to secure critical facilities or national symbols; or to acquire resources (e.g., robbery of a bank or armory).
9. **Sabotage.** Sabotage is the destruction of property or obstruction of normal operations, or treacherous action to defeat or hinder a cause or endeavor. The objective in most sabotage incidents is to demonstrate how vulnerable society is to terrorist actions.
10. **Weapons of Mass Destruction (WMD).** There is an increasing threat of terrorist use of high explosives, chemical, biological, nuclear, or radiological weapons.
11. **Information Warfare (IW).** Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while leveraging and defending one's own information, information systems, and computer-based networks. The maturation of global connectivity via the Internet allows computer hackers anywhere in the world to attack computer systems with viruses.

## **2.4 TERRORIST ATTACK METHODOLOGY**

Generally speaking, terrorist attacks don't just happen — they often take months of preparation and planning. Even though terrorists may be willing to sacrifice their lives in an attack, they are less willing to sacrifice their lives, or the reputation of their organization, in an unsuccessful attack. Many terrorist attacks are preceded by a degree of planning, training, and preparation that rivals an organized military operation.

A six-step process encompassing target selection, training, and preparation before the actual attack is initiated often precedes terrorist attacks. It is important to understand the basics of this process to avoid becoming the chosen target.

### **2.4.1 Phase One — Target Options**

Once a terrorist or terrorist group decides to conduct an attack they begin the process of target selection. Potential targets selected will depend on group capabilities, type of attack they want to make, and what they want to achieve by successfully making the attack. At the end of this phase they will have developed a list of potential targets.

### **2.4.2 Phase Two — Selection Surveillance**

During this phase each of the potential targets will receive some degree of light surveillance to determine its acceptability for further consideration. This surveillance may reveal a successful attack on a particular target is beyond the group's capability or does not meet intended objectives. A person or facility initially considered as a potential target may be discounted at this point because it is perceived to be too difficult a target to successfully attack.

### **2.4.3 Phase Three — Target Selection**

Based on the phase two surveillance, the terrorist selects a target, or set of targets.

### **2.4.4 Phase Four — Detailed Surveillance**

Detailed, and often long term, surveillance is then conducted against the chosen potential target(s). Surveillance will reveal routines, procedures, and security measures so that vulnerabilities can be identified and planned against. This phase presents a weakness in the terrorist's preparation. An effective counter-surveillance program may be able to detect surveillance and alert the target of impending attack potential. Implementing random or changing patterns in the security profile, collectively referred to as random antiterrorism measures (RAM), may make further targeting too difficult to ensure a successful attack.

### **2.4.5 Phase Five — Training and Preparation**

The attack plan will be developed, the attack team assembled and trained, and logistics preparations made.

### **2.4.6 Phase Six — The Attack**

Once phase five is accomplished the terrorists wait for the right set of circumstances to make their attack. It may be months before the planned-for circumstances occur and the attack takes place. Changes in procedures or routine on the part of the potential target can complicate the intended attack profile and delay the attack until the expected conditions present themselves.

## **2.5 TERRORIST THREAT LEVELS**

Terrorist threat levels are the intelligence community's (IC's) system for articulating and categorizing the terrorist threat worldwide. They represent a DOD-developed methodology for assessing the terrorist threat to DOD personnel, material, and interests based on a combination of threat analysis factors. The terrorist threat level determined for a particular area is a reflection of the presence or absence of these factors. General FP condition supporting measures, and unit and facility resources are helpful in developing threat responses. The Defense Intelligence Agency (DIA) and the combatant commander may issue terrorism threat level assessments. The DOS also issues a terrorism threat level assessment, based on different factors, that is completely separate from the DOD and Commander in Chief (CINC) threat assessment (TA). It is titled Security Environment Threat List (SETL) and applies to State Department assets.

Terrorist threat levels do not address when a terrorist attack will occur and do not specify a FP condition status. The issuance of a terrorist threat level is not a warning notice. The Navy Antiterrorist Alert Center (ATAC), DIA, and/or the combatant commander issue separate warning notices regarding imminent terrorist attacks. The following DOD threat level assessment methodology addresses the threat to DOD posed by terrorists:

## **NWP 3-07.2**

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 forged from a combination of the above TA factors. Recent changes in DOD Instructions have changed the previous five-level system to one that has four steps. The four steps from lowest to highest are: low, moderate, significant, and high.

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 (HN)/U.S.
3. Significant — An anti-U.S. terrorist group is operationally active and attacks personnel as their preferred method of operation, or a group uses large casualty producing attacks as their preferred method and 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.

## **2.6 TERRORIST FORCE PROTECTION CONDITIONS**

Terrorist FP conditions, formerly known as Threat Condition (THREATCON), are selected based on the terrorist threat level, the capability to penetrate existing physical security systems, the risk of terrorist attack to which personnel and assets are exposed, the asset's ability to execute its mission even if attacked, and the protected asset's criticality to their missions.

The terrorist threat levels represent the IC's assessment of the likelihood of terrorist attacks on DOD personnel and assets. However, the FP conditions are the principal means that a commander has to apply operational decisions on how to guard against the threat. The commander must weigh the intelligence data, modify security measures based on the threat, and balance these measures against the loss of mission effectiveness during prolonged security operations and the deleterious effect on personnel morale and welfare.

Commanders at any level can establish FP conditions and subordinate commanders can establish higher FP conditions if the local situation warrants it. FP condition measures are mandatory when declared, are implemented immediately, and can be supplemented by additional measures. The declaration, reduction, and cancellation of FP conditions remains the responsibility of the commanders issuing the order. The following is a brief description of each FP condition listed in Figure 2-1.

1. FP Condition NORMAL — Applies when a general threat of possible terrorist activity exists but warrants only a routine security posture.
2. FP Condition ALPHA — Declared when a general threat of possible terrorist activity is directed toward installations, vessels, or personnel, the nature and extent of which are unpredictable and where circumstances do not justify full implementation of FP condition BRAVO measures. However, it may be necessary to implement certain selected measures from FP condition BRAVO as a result of intelligence received or as a deterrent. The measures in this threat condition must be capable of being maintained indefinitely.

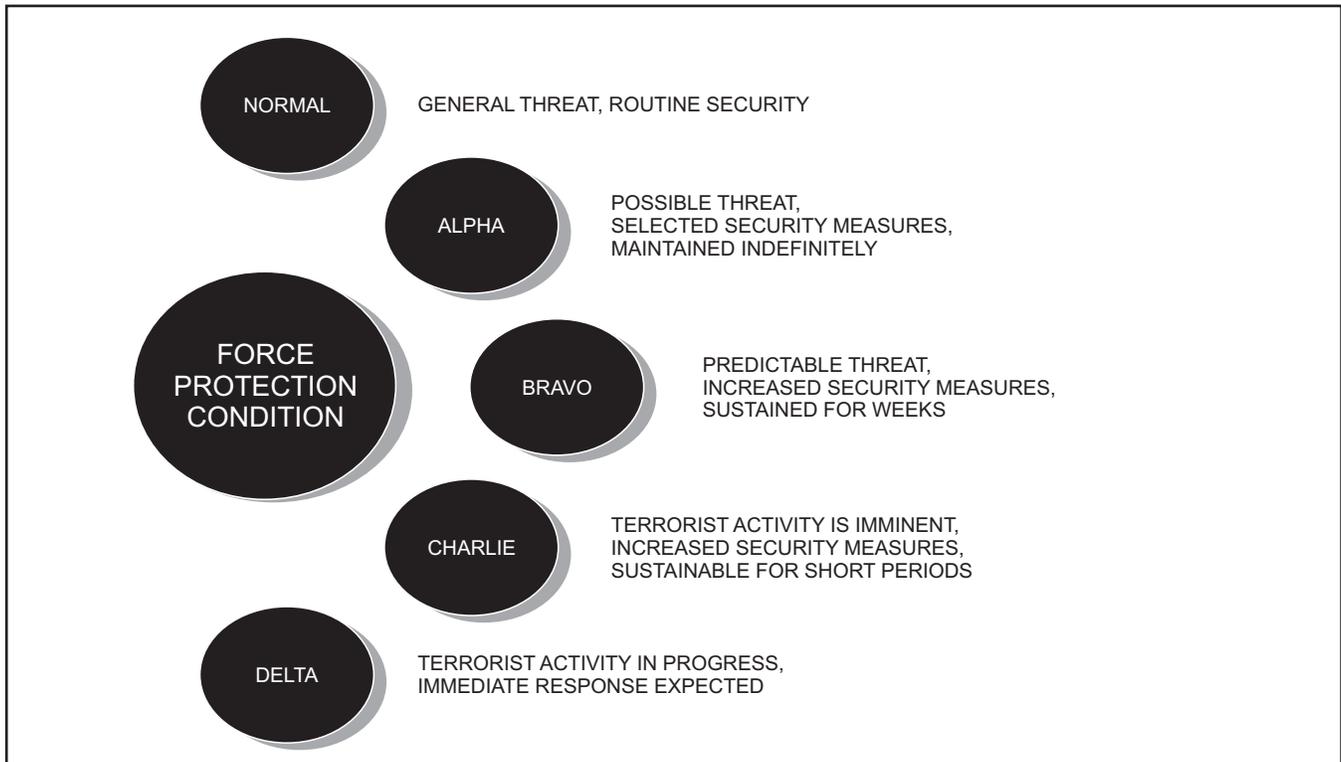


Figure 2-1. Terrorist Force Protection Conditions

3. FP Condition BRAVO — Declared when an increased and more predictable threat of terrorist activity exists. The measures of this FP condition must be capable of being sustained for weeks without causing undue hardships, affecting operational capability, and aggravating relations with local authorities.
4. FP Condition CHARLIE — Declared when an incident occurs or intelligence is received indicating that some form of terrorist action against installations, vessels, or personnel is imminent. Implementation of this FP condition for more than a short period will probably create hardship and affect the peacetime activities of the unit and its personnel.
5. FP Condition DELTA — Declared when a terrorist attack has occurred in the immediate area or intelligence indicates a terrorist action against a specific location or person is likely. Normally, this FP condition is declared only as a localized warning.

## 2.7 CONCLUSION

The terrorist threat is not likely to diminish soon. On the contrary, recent events worldwide have shown the need for increased vigilance and preparation by 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. U.S. military forces are highly visible symbols of power and they embody our national principles abroad. To support the engagement elements of the U.S. national security and military strategies, the Navy must maintain a worldwide presence putting Navy forces and personnel at risk of being terrorist targets. U.S. military forces and personnel have frequently been the target of terrorist attacks in the past and that trend is certain to continue for many years to come. Therefore, the baseline posture for AT/FP preparedness must be greater for military forces and personnel than it has been in the past.



## CHAPTER 3

# Intelligence, Counterintelligence, and Threat Analysis

### 3.1 OVERVIEW

This chapter explains the fundamentals of intelligence, the intelligence cycle, producers of intelligence and the United States IC as they apply to AT/FP. Intelligence and counterintelligence are the first lines of defense in an AT/FP program and this chapter emphasizes tailored and focused intelligence that does not overwhelm and is useful to commanders. The role of the IC is to identify the threat, provide advance warning, and disseminate critical intelligence in a usable form to commanders.

### 3.2 TERRORISM

In remarks made in January 2001, upon the release of the findings of the USS Cole Commission, Secretary of Defense William Cohen and Admiral Harold Gehman stated that:

“There was not specific intelligence communicated to the captain of the ship; . . . the warnings that were received were general in nature and not directed against this ship; and . . . they preceded this tragedy at least a month prior to that time. So one of the recommendations would be to get much greater focus on intelligence that is focused for the ships and for all the commanders. . . . We recommend that . . . the theater intelligence centers focus some resources on tracking, dedicating intelligence products, overwatching and advising these transiting units as to the risks into the areas in which they are going.”

Terrorism is the most significant asymmetric threat to our interests at home and abroad. The characteristics of the most effective terrorist organizations — highly compartmented operations planning, good cover and security, extreme suspicion of outsiders, and ruthlessness — make them very difficult intelligence targets.

### 3.3 THE INTELLIGENCE PROCESS

Rigorous analysis of intelligence data in support of AT/FP operations is critical. The dramatic increase in terrorist incidents in the past several years, especially those directed against U.S. military and diplomatic personnel, has resulted in a heightened awareness toward terrorism. This situation has created an increased demand on information collection, and in many cases, resulted in the inundation of our intelligence system with raw data. Post-analysis of terrorist incidents reveals that indicators and information were on hand in raw data form, but very few people were able to comprehend it and much of the data went unanalyzed. It is important for AT/FP planners to understand the IC, what it can and cannot provide, and how to task the appropriate organizations to provide the information needed to complete the mission. Equally important, intelligence organizations and analysts must understand the unique needs of the consumer and must provide focused intelligence support to deployed forces. While Executive Order 12333 states, “Maximum emphasis should be given to fostering analytical competition among appropriate elements of the intelligence community,” it goes on to say that, “To the greatest extent possible . . . all agencies and departments should seek to ensure full and free exchange of information in order to derive maximum benefit from the United States intelligence effort.”

### **3.3.1 Defining Intelligence**

The difference between *information* and *intelligence* is significant within the IC and this concept drives how commanders use intelligence.

1. Information is the assimilation of data that has been gathered, but not fully correlated, analyzed, or interpreted. Although the information has not been fully analyzed or correlated, it may still be valuable to the tactical commander for threat warning and target acquisition.
2. Intelligence, on the other hand, is the 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 around us — the prelude to decision and action by U.S. policymakers and intelligence consumers.

Development of an intelligence product involves collecting information from a number of different sources. In some cases, information may be disseminated immediately based upon operational necessity and potential impact on current operations (for instance a BLUE DART message from the Navy ATAC). 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 allow the development of conclusions. The intelligence process confirms information through a multiplicity of sources to reduce the chance of erroneous conclusions and susceptibility to deception.

## **3.4 TASKING THE UNITED STATES INTELLIGENCE COMMUNITY**

When developing mission critical priority intelligence requirements (PIRs) and requests for information (RFIs), the Commanding Officer (CO) should think of the IC as an inverted pyramid (see Figure 3-1). The CO need only be aware of the intelligence organization nearest his or her organization such as the battle group (BG), air wing, Amphibious ready group/Marine expeditionary unit (ARG/MEU), destroyer squadron (DESRON), or numbered fleet 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 (CIA), National Security Agency (NSA), or DIA, finished intelligence will follow the same route back to the requester via the staff N2. If the information requested could be satisfied at the theater or component level, answers will come directly to the requester.

Predeployment briefs provided by analysts from Navy intelligence, Naval Criminal Investigative Service (NCIS), and DIA provide the unit commander, N2 and the antiterrorism officer (ATO) with the current threat CT/CI environment of the mission area. During a brief, further requests for focused, tailored information or intelligence products for CI concerns in the area of responsibility (AOR) can be raised.

The following section discusses the many intelligence centers found within DOD that can be called upon to support afloat and ashore assets.

### **3.4.1 Navy Intelligence**

The Department of the Navy has intelligence organizations that provide unique and continuous intelligence support to Navy operations. Navy intelligence is part of the “corporate enterprise” of military intelligence agencies working within the IC. Navy intelligence products and services support the operating forces, the Department of the Navy, and the maritime intelligence requirements of national level agencies. Navy assets receive their primary AT/FP-related intelligence support from the Navy intelligence centers discussed below. These Navy centers are the primary intelligence brokers for information provided by the rest of the national IC. As units deploy to support CINCs around the world, focused intelligence products are provided directly to the units from AOR-specific intelligence centers. The following organizations provide finished AT/FP analytical products, indications and warning (I&W) reporting, and 24 hour/365 days a year watch centers to support fleet operations. Commanders and their N2s should make themselves aware of these intelligence products and services before deployment.

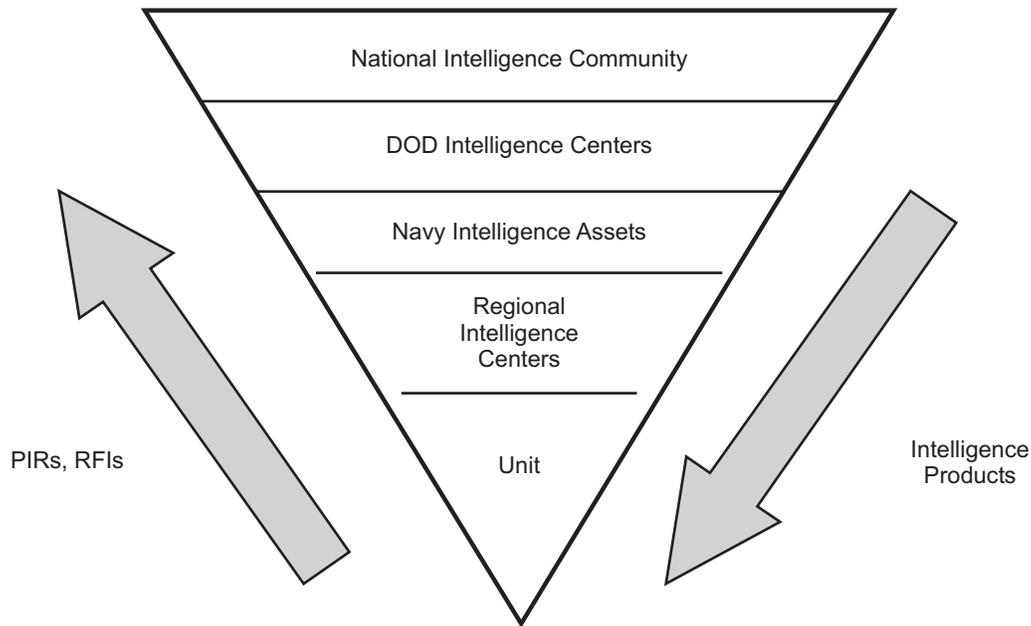


Figure 3-1. Support for Unit Specific Intelligence Needs

1. National Maritime Intelligence Center (NMIC) — The NMIC incorporates the Office of Naval Intelligence, the Marine Corps Intelligence Activity and the Coast Guard Intelligence Coordination Center and is the national resource for all maritime and expeditionary operations.
2. The Office of Naval Intelligence (ONI) — Located primarily within the NMIC, ONI is the national production center for global maritime intelligence. ONI is the principal source for maritime intelligence as it applies to antiterrorism, FP, counter proliferation, naval operations other than war, special warfare, and intelligence in support of Naval Coastal Warfare operations.
3. Commander, Naval Security Group — The Naval Security Group is the Navy’s executive agent for cryptology and IW, and command and control warfare. It is responsible for cryptologic planning and programming, system acquisition, training and administration of naval cryptologic field activities around the world. The Marine support battalion collocates companies at selected naval cryptologic field activities and provides Marine Corps participation with the Naval Security Group. Marine support battalions also provide support to naval expeditionary operations through augmentation of Fleet Marine Force Radio Reconnaissance Battalions.
4. Marine Corps Intelligence Activity (MCIA) — MCIA focuses on crisis and predeployment support to expeditionary warfare units. It 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.
5. Coast Guard Intelligence Coordination Center (ICC) — The ICC, collocated at NMIC, provides strategic intelligence support to Coast Guard law enforcement, military readiness, port security, marine safety and environmental protection missions. 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 analysis.

### **3.4.2 Counterterrorism/Counterintelligence Centers**

CT/CI centers provide intelligence products that should be used in the command's AT/FP plan. CT/CI analysis serves as the baseline for determining the degree and type of FP required. It is the basis for devising and implementing an effective AT/FP program. CT/CI analysis:

1. Identifies foreign intelligence threats and the collection capabilities and intentions of terrorist groups, state-sponsored terrorist organizations, and potentially hostile foreign intelligence services.
2. Aids in allocating strategic and tactical resources to neutralize threats.
3. Identifies vulnerabilities or gaps in U.S. security programs.
4. Assists in implementing more cost-effective security procedures and countermeasures.

Various agencies, working groups, and task forces within the U.S. Government perform terrorism assessments, with the scope and direction of their respective efforts dictated by their area of interest (AOI) and specific needs unique to their requirements. At the national level, the CIA performs primary terrorism analysis on foreign terrorist groups and the FBI is responsible for monitoring and reporting on the activities of domestic terrorist groups, as well as foreign groups operating in the U.S. The CIA has an extensive capability to monitor, gather information, and produce in-depth analysis on a broad cross-section of matters relating to terrorism in foreign countries.

Within the IC, various agencies have organized CT and CI centers to address the growing domestic and international terrorist threat. Analysis centers discussed in this section provide products in support of AT/FP efforts fleetwide. Figure 3-2 represents the multiple centers within the intelligence community. Within DOD, there are many CT/CI centers at the command, regional, and service level.

1. Director of Central Intelligence, Counterterrorist Center (CTC) — The lead center in the U.S. Government's fight against terrorism. The CTC brings together representatives from all of CIA's directorates and numerous government agencies that support the counterterrorist mission and produces all-source analysis of groups and states involved in international terrorism.
2. Interagency Intelligence Committee on Terrorism (IICT) — The interagency forum for coordination and cooperation on counterterrorist-related intelligence activities, including areas such as collection requirements, the exchange of information and technology, and the production of coordinated intelligence community terrorist analysis.
3. Bureau of Intelligence and Research (INR) — The primary mission of INR is to gather intelligence to serve the U.S. diplomatic corps. The Bureau has a key role in ensuring that intelligence activities are consistent with U.S. foreign policy.
4. Federal Bureau of Investigation (FBI) — The FBI is responsible for detecting and counteracting foreign intelligence activities gathering information that adversely affects U.S. national security interests. The FBI conducts foreign CI investigations under the authority of Executive Order 12333 and acts of Congress. The FBI's CT mission is to identify and neutralize the threat in the U.S. posed by terrorists and their supporters, whether they are nations, groups, or individuals.

#### **3.4.2.1 Department of Defense Counterterrorism and Counterintelligence Centers**

Within DOD, the DIA and the intelligence branches of the armed services have, as a part of their mission, a requirement to produce assessments of the actual or potential terrorist threat targeted against U.S. military interests throughout the world. These assessments are used by decision makers at the highest levels within DOD, and in each of the branches of the armed forces, for a variety of purposes including attempts to deter terrorist initiatives against sensitive military targets, other military facilities, and U.S. military personnel overseas. Assessments produced at the national level, while based on the best information available from all sources within the national intelligence

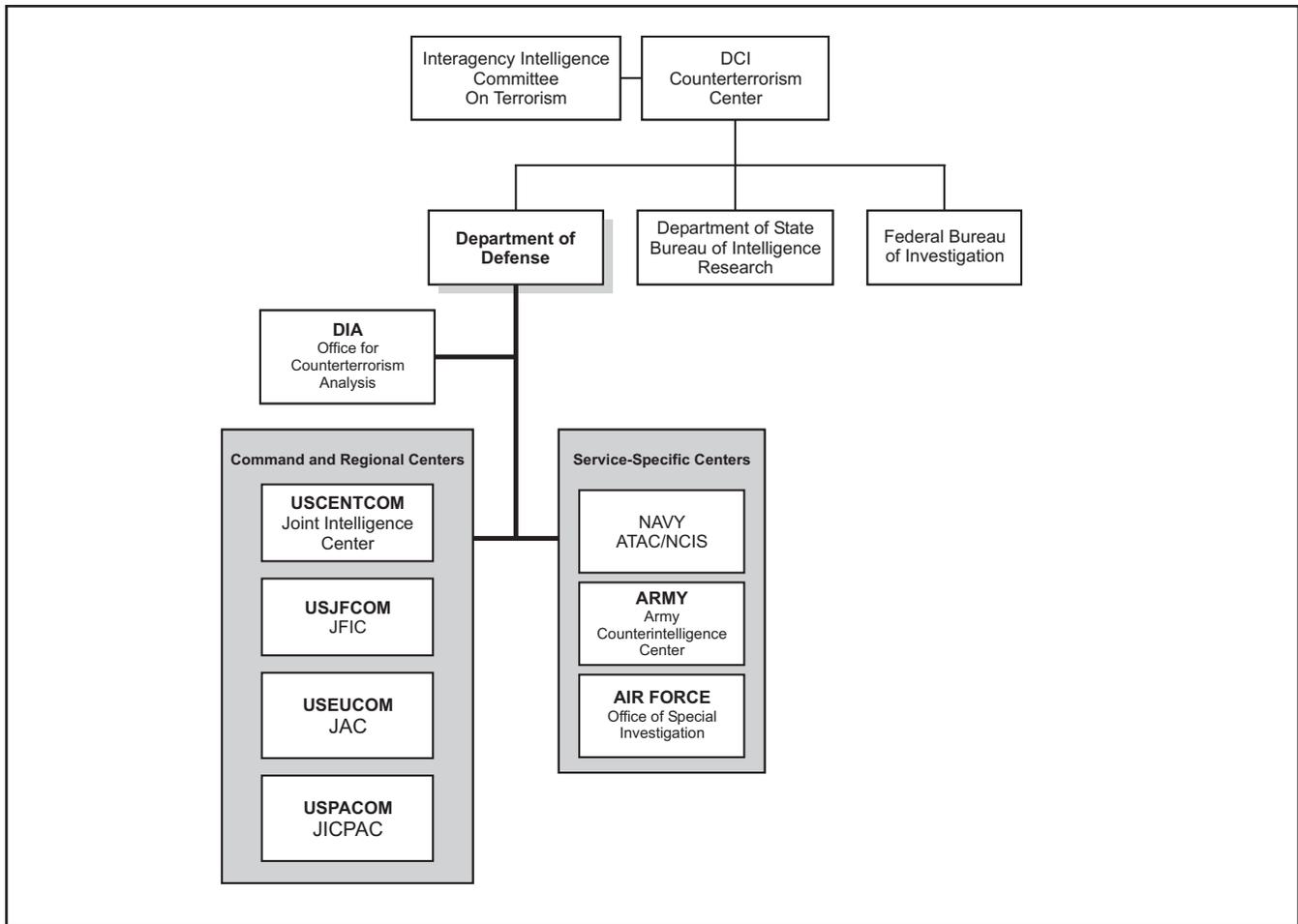


Figure 3-2. Counterterrorist and Counterintelligence Organizations

community, are often general in nature. The purpose of these assessments is to provide consumers, military commanders, and security personnel with the intelligence necessary for local threat assessments.

1. DIA Office for Counterterrorism, Threat Warning Center (TWC) — The TWC is the coordinating office for DIA on terrorism. The TWC is in the process of moving all of its products to new homepages available on INTELINK. These pages will eventually serve as a portal to all TWC's products and terrorism database. Through the incorporation of community products, TWC's homepage will eventually expand to become a community-wide counterterrorism information portal (CIP). Versions of CIP will be released at the Secret level on SIPRNET, TS/SCI level on JWICS, and Secure COI.

#### 3.4.2.2 Command and Regional Counterterrorism and Counterintelligence Centers

Focused daily intelligence products are available to unit commanders while transiting and once they arrive on station. The following regional intelligence centers provide threat reports and messages to deployed units as well as reports from the ATAC.

1. Joint Forces Intelligence Command (JFIC) — JFIC in Norfolk, Virginia, provides tailored intelligence support to all units in USJFCOM AOR/AOI.
2. Joint Analysis Center USEUCOM (JAC Molesworth) — Located in Molesworth, United Kingdom, the JAC provides analysis of the terrorism and foreign intelligence service threat throughout USEUCOM's AOR/AOI in support of their FP mission. There is also an I&W watch, which maintains theater-wide threat levels.

3. Joint Intelligence Center USCENTCOM (JICCENT) — The primary Joint Intelligence Center for USCENTCOM in Tampa, Florida, provides intelligence support to U.S. forces in the Middle East AOR. An additional JIC in Riyadh, Saudi Arabia, provides support for operation SOUTHERN WATCH and monitors terrorist related activities in the region.
4. Joint Intelligence Center Pacific (JICPAC) — JICPAC in Pearl Harbor, Hawaii, operates a fusion center that conducts current situation analysis, collection management and long-range assessments and threat estimates.

For specific information and procedures regarding the distribution and use of intelligence products from these centers, consult NTP 3-07.2.1, Navy Tactics, Techniques, and Procedures for Antiterrorism.

### **3.4.2.3 Service Sponsored Counterterrorism and Counterintelligence Centers**

Since no one source of information is the authoritative voice on CT/CI issues, it is incumbent on the CO and ATO to review all-source theater and NCIS intelligence assessments coordinated by the Fleet level intelligence staffs. Most of the CT/CI information needed to support a unit's deployment will already have been created within DOD channels and will be easily obtained. The service sponsored CT/CI centers monitor all national, service, and theater intelligence traffic and products to identify specific threats to their personnel. These sources provide unique CT/CI products that should be tracked by the command before and during deployments to understand the threat environment. The Navy intelligence CT/CI assets of this effort are centered with the NCIS. A description of the NCIS role in AT/FP is discussed below, followed by a description of Army and Air Force efforts.

1. NCIS — NCIS has primary investigative and counterintelligence jurisdiction within the Department of the Navy. This jurisdiction is grounded and documented in Presidential Executive Order, DOD instructions, and Secretary of the Navy instructions. NCIS maintains a worldwide field structure that provides criminal and counterintelligence support to the Navy both ashore and afloat. In addition to this charter, the Director, NCIS, is the CNO Special Assistant for Naval Investigative Matters and Security (N09N), and is the Assistant for Foreign Counterintelligence (N2E). Within the Department of the Navy, NCIS has exclusive investigative jurisdiction in noncombat matters involving actual, potential, or suspected terrorism, sabotage, espionage, and subversive activities. NCIS also has the primary responsibility for collecting, processing, storing, and disseminating counterintelligence information regarding persons or organizations not affiliated with DOD. Additionally, NCIS is the element exclusively assigned to maintain liaison on all criminal investigative, CI, and security matters with federal law enforcement, security, and intelligence agencies; and is the primary agency for liaison in these matters with state, local, and foreign law enforcement, security, and intelligence agencies, including those of foreign and U.S. military departments (SECNAVINST 5520.3B). Through the Navy ATAC, NCIS monitors all national, service, and theater intelligence traffic and products to identify specific threats to Navy personnel and resources. These sources provide unique CT/CI products that are tracked by the ATAC and can be provided to the command before and during deployments to understand the threat environment.
2. The NCIS AT/FP Program — NCIS has developed an AT/FP program that collects and analyzes information about possible threats from various sources, and advises commanders on how best to defend against them. This program includes investigations, threat briefings, intelligence collection, and vulnerability assessments. NCIS agents are assigned to the staffs of the fleet and component commands as staff counterintelligence officers (SCIOs). These SCIOs are the commanders' direct connection to all of the NCIS and Navy ATAC AT/FP program resources and services. The SCIOs work closely with the N2s, N3s, and ATOs of the operational forces they support. NCIS also assigns agents to the unified commands as counterintelligence staff officers (CISOs). NCIS agents, analysts, and physical security specialists are forward deployed, both domestically and overseas, acting as the Navy's "eyes on target" for installation commanders, and transiting ships and units. NCIS analysts are also assigned to the three major joint intelligence centers. Additionally, special agents afloat are assigned to deploying carrier BGs and ARGs to provide AT/FP support to those deploying forces.

Through the NCIS Country Referent Program, agents conduct advance visits to expeditionary ports, airfields, and exercise areas to prepare an AT/FP TA for transiting units. This "on the ground" AT/FP collection effort is conducted

within 30 days for moderate, significant, and high threat countries; and within 90 days for low threat locales. NCIS TAs are issued 7-10 days prior to the transiting unit arriving. In many cases, these agents are made available to meet the transiting unit when it arrives. NCIS agents also support the Joint Staff Integrated Vulnerability Assessment Program (JSIVA), the CNO Installation Vulnerability Assessment Program (CNOIVA), as well as the Navy's Port Integrated Vulnerability Assessment Program (PIVA). NCIS has developed the counterintelligence FP program, which collects and analyzes information about possible threats from various sources and advises military commanders on how best to defend against them. This program includes investigations, threat briefings, counterespionage operations, and intelligence collection. Some NCIS personnel work closely with the planning staffs of the operational forces they support, while others are forward deployed, acting as the eyes and ears for the approaching forces. Special agents also conduct operations designed to identify and counter efforts by foreign intelligence services to obtain classified information about U.S. warfighting capabilities. NCIS assigns trained counterintelligence professionals to the staffs of unified, naval component, and fleet commanders, and to the three major joint intelligence centers. Personnel assigned to these positions identify the military commander's counterintelligence information needs and determine the best way to satisfy those needs.

1. Navy Antiterrorist Alert Center (ATAC) — NCIS analysts, along with active duty and reserve intelligence personnel, staff the ATAC situated in Washington, DC. The ATAC is the centerpiece of the Navy's efforts to counter the terrorist threat to Department of the Navy personnel as well as other service and U.S. Government organizations. Initiated as a CNO project in December 1983, the ATAC maintains a constant watch to analyze various information and intelligence for possible terrorist threats against Navy and Marine Corps commands. ATAC analysts track these activities and trends and report them to the fleet via their messaging system. These reports, in conjunction with theater intelligence reports, provide forward-deployed units with the most current information and intelligence on potential threats.
2. Army Counterintelligence Center (ACIC) — The ACIC's mission is to provide timely, accurate, and effective multidiscipline counterintelligence and terrorism analysis in support of the U.S. Army, sustaining base commanders, and CONUS-based deploying forces (in coordination with component commands). ACIC also provides intelligence expertise concerning ground system technologies and counterintelligence investigations and operations. In support of FP, ACIC produces a monthly terrorism summary as well as a daily input to the Anti-Terrorism Operations and Intelligence Center's Force Protection Memorandum. The ACIC also provides specific travel TAs for VIP travelers from the Army and DOD.
3. Air Force Office of Special Investigations (AFOSI) — AFOSI's mission is to counter the threat to Air Force security posed by hostile intelligence services and terrorist groups, and identify and assess the threat for Air Force commanders. AFOSI manages offensive and defensive activities to detect, counter and destroy the effectiveness of hostile intelligence services and terrorist groups that target the Air Force for espionage. This includes investigating the crimes of espionage, terrorism, technology transfer, and computer infiltration. The counterintelligence mission also includes providing personal protection to senior Air Force officers and other officials as well as supervising an extensive antiterrorism program in geographic areas of heightened terrorist activity.

There are many other CT/CI and AT/FP analytical and response cells within DOD that were not identified here. It is incumbent upon the commander, the ATO, and intelligence officer to seek out these resources at each port facility, naval station, and air station to fully appreciate the local threat environment. Access to intelligence gathered at the local (including HN) level along with regional and national intelligence, will aid the commander in developing an accurate threat picture and thereby optimize the employment of AT/FP assets. The products and services available through these cells can be provided through the regional intelligence centers or tasked through the ATAC.

### **3.5 NAVY ANTITERRORIST ALERT CENTER/BLUE DART MESSAGE PROCEDURES**

Threat warning information will be afforded the maximum protection possible consistent with the need to inform threatened units in a timely fashion. The ATAC spot message is the Navy's principal vehicle for disseminating terrorism warnings to Navy and Marine Corps commands. The ATAC 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

## **NWP 3-07.2**

does not necessarily warrant raising the overall threat level. Navy ATAC spot reports do not require receipt notification.

The ATAC disseminates BLUE DART messages when intelligence indicates that a specific, imminent, and credible terrorist threat exists. These messages are identified by the code words “BLUE DART” and require acknowledgment by immediate message from all action addressees. The message will be acknowledged by immediate precedence. Navy BLUE DART reporting procedures do not replace existing CINC reporting requirements.

When a Navy BLUE DART, ATAC spot report, or other terrorism threat warning message is received, commanders will review on-scene terrorist FP conditions and leave and liberty policies in the threatened area. For specific information and procedures regarding the distribution and use of intelligence products from the ATAC, consult NTPP 3-07.2.1, Navy Tactics, Techniques, and Procedures for Antiterrorism.

### **3.6 SUMMARY**

The correct use of intelligence, counterintelligence, and threat analysis is the foundation for an effective antiterrorism posture. Commanders at all levels must understand and seek out information in preparation for any port/airfield visit to ensure a clear picture of the local threat environment is gained.

# CHAPTER 4

## Legal Considerations

### 4.1 OVERVIEW

This chapter highlights legal considerations for operational commanders when developing and implementing AT/FP plans. Legal advisors should be consulted from the very beginning of the planning process to ensure compliance with U.S. domestic, international, and foreign law.

### 4.2 GENERAL

It is critical to pursue AT/FP planning and implementation with the same zeal and sense of purpose afforded other warfighting skills. The results of a terrorist incident are just as deadly and destructive as a surprise enemy attack; however, the preparation necessary to prevent or respond to a terrorist incident is considerably different. U.S. policy views terrorist incidents as criminal events and has assigned various non-DOD government agencies lead roles in responding to them. Operational commanders must understand the various interagency, international, and local interfaces and incorporate legal concerns in AT/FP planning.

Commanders are ultimately responsible for protecting their units, ships, aircraft, and installations from terrorist attack regardless of territorial jurisdiction. CJCSI 3121.01A of 15 January 2000, the CJCS Standing Rules of Engagement (SROE), implement the inherent right of self-defense and provide guidance for the application of force for mission accomplishment. The SROE provide the fundamental policies and procedures governing the actions to be taken by 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 SROE are intended to:

1. Implement the inherent right of self-defense, which is applicable worldwide to all echelons of command and personnel.
2. Provide guidance governing the use of force for mission accomplishment.
3. Be 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.

CINCs may augment the SROE, as necessary; however, the National Command Authority must approve modifications to the SROE.

The Internal Security Act (50 U.S.C. §797) provides authority for installation commanders to take appropriate steps to safeguard property and personnel under their cognizance. Peacetime operations conducted within U.S. territory (shoreward of the outer edge of the 12 nm territorial sea), are governed by employment of force rules contained in DOD Directive 5210.56 and SECNAVINST 5500.29B. The Magnuson Act (50 USC §191, as implemented at 33 CFR part 6), provides broad authority for taking measures to protect ports, harbors, waters, vessels, and waterfront facilities of the United States.

These rules do not limit a commander's inherent authority and obligation to use all necessary means available and to take all appropriate actions in self-defense of their unit and other U.S. forces in the vicinity. During overseas port visits, HN sovereignty concerns will vary. In some cases, HNs may limit the active participation by U.S. military in implementing security measures. Notwithstanding this fact, nothing limits or curtails a commanding officer's

obligation and duty to defend his/her unit and personnel. Maximum coordination with local commands, defense attachés, and higher authority is critical to shaping the best possible FP posture under the circumstances.

### **4.3 DEFINITIONS OF LEGAL TERMS**

The following are important legal concepts and a short definition of each as they relate to antiterrorism:

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 this baseline is the coastal low water line. Lakes, rivers, harbors, and lagoons are examples of internal waters. Internal waters have the same legal character as land itself. 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.
  - b. Territorial seas — The territorial sea is measured seaward from the baseline of the coastal nation and is subject to coastal nation sovereignty. The U.S. claims and recognizes territorial sea claims of other nations up to a maximum breadth of 12 nm.
2. International waters — Waters seaward of the territorial sea, where, for operational purposes, all nations enjoy the freedoms of navigation and overflight.
3. Inherent right of self-defense — A commander has the inherent authority and obligation to use all necessary means available and to take all appropriate actions to defend his/her unit and other U.S. forces in the vicinity from a hostile act or demonstration of hostile intent. Neither the SROE, nor any supplemental measures activated to augment the SROE, limit this inherent right and obligation. At all times, the requirements of necessity and proportionality, as amplified in the SROE, will guide the on-scene commander's or an individual's choice of appropriate response to a particular hostile act or demonstration of hostile intent.
4. Unit self-defense — The act of defending a particular U.S. force element, including individual personnel, and other U.S. forces in the vicinity, against a hostile act or demonstrated hostile intent.
5. Individual self-defense — The inherent right to use all necessary means available and to take all appropriate actions to defend oneself and U.S. forces in one's vicinity from a hostile act or demonstrated hostile intent. Commanders have an obligation to ensure that individuals within their respective units understand and are trained on when and how to use force in self-defense.
6. Elements of self-defense — Application of force in self-defense requires the following two elements:
  - a. Necessity — Exists when a hostile act occurs or when a hostile force or individual(s) 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. Hostile Act — An attack or other use of force against the United States or U.S. forces, which includes force used directly to preclude or impede the mission and/or duties of U.S. forces and the recovery of U.S. personnel and vital U.S. government property. In certain circumstances, the use of force against U.S. nationals, their property, U.S. commercial assets, and/or other designated non-U.S. forces, foreign nationals, and their property is also a hostile act.
8. Hostile Intent — The threat of imminent use of force against the United States or U.S. forces, which includes the threat of imminent use of force that would preclude or impede the mission and/or duties of U.S. forces, including the recovery of U.S. personnel or vital U.S. government property. In certain circumstances, hostile

intent is the threat of imminent use of force against U.S. nationals, their property, U.S. commercial assets, and/or designated non-U.S. forces, foreign nationals, and their property.

9. Hostile force — Any civilian, paramilitary, or military force or terrorist(s), with or without national designation, that has committed a hostile act, exhibited hostile intent, or has been declared hostile by appropriate U.S. authority.
10. U.S. forces — All Armed Forces (including the Coast Guard) of the United States, 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 the U.S. Armed Forces.

#### 4.4 AUTHORITY AND ACTIONS TO EXERCISE SELF-DEFENSE

A unit commander has the authority and obligation to use all necessary means available and to take all appropriate actions to defend the unit, 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, unit 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 individual and unit self-defense:

1. When time and circumstance permit, the hostile force should be warned 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.

When determining whether it is necessary to use force in self-defense, U.S. forces must have the maximum time and space possible to make that determination. Providing U.S. forces with the requisite time and space to make reasoned decisions should be viewed as a critical objective underlying all FP planning. Measures beginning with routine inspection and identification and moving through increasing levels of nonlethal information gathering, or nonlethal use of force, to a point where deadly force may become an option, will aid in the commander's or individual's decision making process. In order to warrant the use of deadly force, a potential threat must possess:

1. The apparent means to commit a hostile act
2. The imminent ability to commit a hostile act
3. The apparent intent to commit a hostile act.

The conditions calling for the application of the right of self-defense cannot be precisely defined beforehand, but must be left to the sound judgment of 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 or mission accomplishment. If the individual no longer poses an imminent threat, force may not be used to inflict punishment for acts already committed. Each component commander should promulgate specific AT/FP guidance for their AOs, to assist commanders and their sailors to enact FP measures that will maximize their opportunity to recognize hostile intent that would trigger their obligation to act in self-defense.

#### **4.5 CONSIDERATIONS FOR CIVILIAN-CREWED SHIPS OPERATED BY OR FOR THE MILITARY SEALIFT COMMAND**

Military Sealift Command (MSC) ships are civilian-manned and therefore have some unique legal considerations that differ from Navy vessels that have military crews. MSC ships are unarmed with the exception of a modest complement of small arms for a minimum of five qualified crewmembers. The civilian mariners (whether government or contractor employees) that operate MSC 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 status-of-forces agreements (SOFAs) and are not governed by military ROE or the Uniform code of military justice (UCMJ). The small crew size of MSC ships generally precludes the tasking of crewmembers for full-time security duties without impacting their primary missions (cargo operations, etc.).

Thus, MSC ships have very limited self-defense capabilities. In all cases, FP activities would be limited to actions within the lifelines of the ship (for example, due to their civilian status, it is inappropriate to employ a civilian mariner as a pier sentry or picket boat operator). Accordingly, operational commanders must be prepared to augment MSC ships when, in their judgment, an armed or dedicated security force is required.

#### **4.6 UNITED STATES TERRITORY ANTITERRORISM/FORCE PROTECTION LEGAL PLANNING**

Commanders of Navy ships, aircraft, units, and facilities within U.S. territory maintain the inherent right of self-defense and have the authority to enforce security measures and to protect persons and property as detailed in DOD Directive 5200.8 and the Navy Physical Security Manual (OPNAVINST 5530.14C). This includes the inherent right of self-defense, either unit or individual, against an unlawful hostile act or demonstrated hostile intent, which would include actual or suspected terrorist incidents and the establishment of security programs. SECNAVINST 5500.29B 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. This instruction states that military and civilian officials of the Navy and Marine Corps not regularly involved in full-time law enforcement, security, or counterintelligence duties shall not carry firearms for personal protection within the continental United States, unless specifically authorized by CNO, VCNO, or the Commandant of the Marine Corps.

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 the confines of an exclusive use base facility, but do have the right to protect military property, facilities, and personnel. The legal and policy prohibition on the use of active duty DOD military personnel, DOD civilian employees, and contractors such as DOD security police for direct enforcement of civil laws in the United States or its possessions is contained in the Posse Comitatus Act (18 USC 1385), DODD 5525.5, DOD Cooperation with Civilian Law Enforcement Officials, and SECNAVINST 5820.7 series.

The authority to enforce civil law often does exist in the immediate waters around a naval installation pursuant to regulations promulgated in the Code of Federal Regulations by the Army Corps of Engineers or the Coast Guard. Appropriate legal authority should be consulted prior to taking any action on criminal law enforcement matters in these areas.

Pursuant to the Internal Security Act (50 U.S.C. §797), Navy Regulations, and DOD Directive 5200.8, installation commanders possess the authority and responsibility to maintain law and order on naval installations. Installation commanders must provide the initial and immediate response to any incident in order to isolate and contain the incident. Afloat commanders operating outside of naval installations can coordinate with the applicable U.S. Coast Guard Captain of the Port and/or the Navy regional commander for establishing security zones when necessary.

#### **4.7 FOREIGN OR NON-UNITED STATES TERRITORY ANTITERRORISM/FORCE PROTECTION LEGAL PLANNING**

U.S. Navy ships and forces on the high seas shall use appropriate antiterrorism measures consistent with the known threat level. Under customary international law, military ships and aircraft are sovereign platforms.

For entry into the internal waters or airspace of a foreign country, ships and aircraft require specific and advance entry permission (usually referred to as diplomatic clearance), unless other bilateral or multilateral arrangements have been made. When U.S. forces are operating in the territorial sea, or within the internal waters or the 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. naval ships and aircraft enjoy 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.

In some countries, the U.S. Government negotiates SOFAs, or Memoranda of Understanding (MOU). Commanders shall ensure their own antiterrorism needs are met by coordinating augmentation of HN measures by ship's company or contracted services. 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 these agreements. Regardless of HN policy, however, every unit retains the right of self-defense from hostile acts or demonstrated hostile intent.

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

#### **4.8 ONGOING/IN-PROGRESS TERRORIST INCIDENT PLANNING**

When AT/FP measures fail and a terrorist incident results, a lead federal agency (LFA) is designated for coordinating U.S. Government consequence management following the incident. Specifically, those LFAs are:

1. The DOS for terrorist incidents occurring outside U.S. territory, with the exception of the Arabian Gulf where DOD and DOS have an MOU transferring responsibility for security of forces on the Arabian Peninsula to the DOD.
2. The Department of Justice (DOJ) for terrorist incidents occurring within U.S. territory. Unless otherwise specified by the Attorney General, the FBI shall be the lead agency within the DOJ for operational response to such incidents.
3. The Federal Aviation Administration (FAA) for aircraft piracy within the special aircraft jurisdiction of the United States. (49 U.S.C. 46501 (2))

Although the DOJ is the LFA designated for coordinating U.S. Government actions to resolve terrorist incidents within the U.S., installation commanders have inherent authority to take necessary and lawful measures to maintain security on installations to protect military personnel, facilities, and property. Installation commanders are responsible for providing the initial and immediate response to any incident occurring on the installation and for containing the damage, protecting property and personnel, and restoring order on the installation. Unless a service member is a suspect in the incident, the FBI will eventually assume lead investigative responsibility for the incident. Unless directed by competent authority, a commander may never delegate or abrogate ultimate responsibility for protecting federal property, facilities, and personnel. Commanders must, however, allow the FBI to perform its lead role in reacting to terrorist incidents when these military interests are not prejudiced.

Military personnel will always remain under the command and control of the military chain of command. If military forces are employed during a tactical response to a terrorist incident, the military commander retains operational responsibility. FBI personnel may be employed by the military commander, but may not participate in the assault phase without the permission of the FBI special agent in charge (SAC).

Outside U.S. territory, the DOS is the lead agency in countering terrorism directed against U.S. personnel and assets other than facilities, installations, or personnel under the command of a U.S. area military commander. The United States Coast Guard has certain authorities that may be appropriate to use in reducing the risk of a terrorist incident within U.S. territorial waters. The FBI is the lead agency for responding to terrorist actions occurring in maritime areas subject to U.S. jurisdiction.



## CHAPTER 5

# The Navy Antiterrorism/Force Protection Program

### 5.1 INTRODUCTION

The commanding officer has the ultimate responsibility for developing and implementing a command AT/FP program. With the assistance of the ATO and the AT/FP Board, the responsible commander will have a dynamic AT/FP program capable of addressing and countering an equally dynamic terrorist threat.

The purpose of the Navy's AT/FP program is to ensure that Navy forces remain mission capable at all times. AT/FP efforts are an important aspect of all military operations; these efforts must be integrated with mission accomplishment using operational risk management techniques. Terrorists are effective if they deter or prevent U.S. forces from carrying out their missions, whether through direct action or the mere threat of an attack. Effective implementation of the Navy AT/FP program will deter the terrorist and allow Navy units, ships, squadrons, and activities to carry out their assigned missions.

### 5.2 PROGRAM CONCEPT

The Navy AT/FP program concept builds on a foundation of terrorist threat analysis and the preparation of an integrated threat estimate. The integrated threat estimate examines the interactions among the following elements:

1. Terrorist threat
2. Risk of terrorist attack
3. Vulnerability of DOD components to terrorist
4. Assessment of asset criticality to DOD missions and functions.

On the basis of the integrated terrorist threat estimate, military commanders and civilian managers as appropriate develop and implement an AT/FP plan to reduce the likelihood of terrorist attack and mitigate its effects should one occur. Preventive measures include terrorism awareness, education and training, physical security enhancements, the training and deployment of security forces, implementation of AT/FP measures, personal protective measures, and even classroom or residential instruction for Navy-affiliated personnel and their families. Two important components of any AT/FP program are the ATO and the AT/FP Board. The ATO assists the commander in developing and implementing the AT/FP plan and the AT/FP Board helps facilitate coordination of antiterrorism efforts throughout the command.

Notwithstanding efforts to prevent terrorist incidents at Navy facilities or involving Navy personnel, military commanders and civilian managers must also include the development of a terrorism crisis management plan to cover such contingencies when preventative efforts do not succeed. Chapter 6, Consequence Management, describes principles to follow when planning and responding to a terrorist incident.

### **5.3 COMMANDER'S RESPONSIBILITY**

Every commander is responsible for ensuring that an effective AT/FP program exists in his or her unit. This starts with the assignment of an ATO. The ATO supports the commander in establishing the required training program and implementing security measures, from Level I training for all hands to the measures prescribed under specific FP conditions. The commander's responsibility for the safety of the unit includes military and civilian personnel (as well as dependents where/when applicable).

Once the CO and ATO develop the AT/FP plan, the commander must provide full support to the ATO and the AT/FP Board. Commanders must constantly evaluate security against the terrorist threat in order to effectively evaluate security requirements. The same AT/FP procedures practiced during deployments also apply to security concerns while in U.S. ports, airfields, and installations. Commanders of Navy units, installations, ships, and squadrons have two major antiterrorism responsibilities:

1. Provide security for personnel under their authority and control (to include family members and civilians when applicable) consistent with threat, risk, vulnerability, criticality, assigned roles, missions, and resources.
2. Provide awareness information and educational materials to help service members, DOD civilians, and contractor personnel prepare themselves and their dependents to reduce their individual risk and vulnerability to terrorism.

### **5.4 IMPLEMENTING THE NAVY ANTITERRORISM/FORCE PROTECTION PROGRAM**

Implementation of effective antiterrorism measures for the protection of Navy personnel and their families must be part of a comprehensive AT/FP program, interwoven with physical security measures, crime prevention, crisis management planning, and wartime mobilization training (see Figure 5-1). The assigned ATO is the commander's primary resource for implementing AT/FP programs. The ATO may coordinate all other antiterrorism resources, oversee AT/FP planning, and implement antiterrorism measures and training.

The ATO must work closely with intelligence personnel to analyze intelligence information and create threat analyses for each mission or deployment. The ATO must assist the CO in developing and refining the AT/FP plan based on current threat analyses, vulnerability assessments, and the commander's guidance, and then execute training to support the plan.

The key to effectively deterring terrorists is to convince them that Navy assets are too difficult to strike. The AT/FP program accomplishes this through the projection of a formidable defensive ability. Implementing RAMs from higher FP conditions is an effective way to confuse any potential terrorist observing a unit. RAMs are merely normal or exceptional measures implemented at a different or unpredictable time. It is this unpredictability in defensive measures that could prevent would-be attackers from executing their planned tactics. For this reason, it is essential that RAMs are kept classified and safeguarded to prevent potential adversaries from gaining access to them and thereby countering their deterrence benefit.

#### **5.4.1 Antiterrorism/Force Protection Plans**

AT/FP plans should identify and reduce the risk of loss or damage to people, equipment, and facilities and develop procedures to detect and deter planned terrorist actions before they take place, thereby reducing the probability of a terrorist event. The plan may also encompass the reactive or tactical stage of a terrorist incident, including direct contact with terrorists to end the incident with minimum loss of life and property.

The prevention portion of any AT/FP plan should include the following minimum elements that work in concert to reduce the vulnerability of a ship, unit, aircraft, or installation to terrorist attack:

1. Terrorism TA
2. Vulnerability assessment

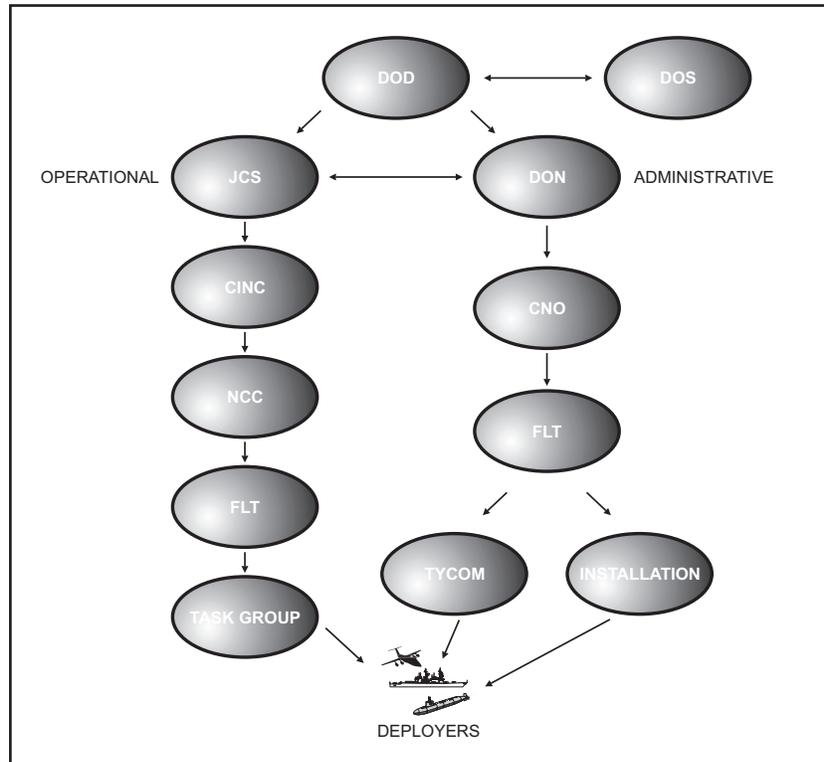


Figure 5-1. DOD Antiterrorism Organization

3. Risk assessment
4. AT physical security measures
5. Terrorist incident response measures
6. Terrorist consequence management measures.

The AT/FP plan should provide an integrated, comprehensive approach to counter terrorist threats. This approach requires a continuous state of awareness, training, planning, and preparedness based on the terrorist threat levels/FP conditions and the ship, aircraft, or installation's vulnerabilities. The plan has two phases, proactive and reactive.

1. Proactive Phase. The proactive phase encompasses the planning, resourcing, preventive measures, preparation, awareness education, and training that takes place before a terrorist incident. Emphasis is placed on:
  - a. Intelligence gathering
  - b. Coordination with local and host country security forces
  - c. Development and implementation of preventive measures and in-depth planning
  - d. Integration of physical assets.
2. Reactive Phase. The reactive phase includes the tactics, techniques, and procedures to be utilized by a unit to defeat a terrorist attack, as well as crisis and consequence management actions taken to resolve a terrorist incident. Chapter 6 covers the reactive phase in more detail.

## **NWP 3-07.2**

For specific information and procedures regarding the development of the AT/FP plan, consult NTTP 3-07.2.1, Navy Tactics, Techniques, and Procedures for Antiterrorism.

### **5.4.2 Antiterrorism Officer Responsibilities**

Previously known as the Force Protection Officer (FPO), the ATO is the point of contact directly responsible to the CO for all matters dealing with AT/FP and oversees the implementation of the antiterrorism program. Included in the ATO's responsibilities are: creating and executing AT/FP programs; preparing AT/FP plans; managing AT/FP resources; and conducting antiterrorism training for the command. Depending on the size of the ship, unit, or installation, the ATO may be filled as a dedicated billet or as an additional duty. Generally, when the ATO position is an additional duty, at least one senior petty officer with Level II training serves as an assistant to the ATO. Refer to DODI 2000.16 of June 14, 2001, for further specific guidance concerning the assignment and responsibilities of the ATO.

### **5.4.3 Antiterrorism/Force Protection Board**

Units will find significant benefits in establishing an AT/FP Board composed of key personnel, under the guidance of the CO. The purpose of the AT/FP Board is to coordinate implementation of the AT/FP plan. Candidates for the board should include:

1. Unit executive officer/officer in charge
2. ATO
3. Department heads
4. Intelligence personnel
5. NCIS personnel
6. Medical personnel
7. Damage control assistant
8. Masters at arms
9. Physical security officer
10. Legal officer.

Board members are the AT/FP points of contact for their respective activities. The command's ATO should also be a member of the installation or higher echelon AT/FP Boards.

### **5.4.4 Security Forces**

Security forces form one of the most important AT/FP assets available to the installation, ship, unit, or squadron. Navy security forces provide the personnel to carry out the AT/FP plan and must be properly trained to fulfill these duties. Security forces may consist solely of personnel who are trained and dedicated to providing security, or additional personnel, lacking formal security training, may augment these forces. Anyone performing security duties must have a current qualification for their assigned weapons and responsibilities.

## **5.5 ANTITERRORISM/FORCE PROTECTION ASSESSMENT PROCESS**

The AT/FP assessment process begins with the conduct of a risk-based assessment. The process consists of identifying the potential threats and analyzing the vulnerabilities to determine the risks. AT/FP working groups may manage

this process for commanders or the ATO may lead the effort. The assessment includes a thorough review of the Navy Combatting Terrorism Standards, the current threat level and FP condition, and the actions required for each condition.

### **5.5.1 Threat Assessment**

An AT/FP TA is the product of a threat analysis for a particular area and will be coordinated by the regional commander in the United States and by the designated organization for the gaining theater CINC. Commands shall receive theater and NCIS TAs per numbered fleet and theater procedures. For specific information and procedures regarding the distribution and use of the various TA products, consult NTTP 3-07.2.1, Navy Tactics, Techniques, and Procedures for Antiterrorism.

### **5.5.2 Vulnerability Assessment**

Vulnerability assessments are available from several different sources. These include the JSIVA, CNOIVA, and the PIVA, intended mainly for installations. In-transit units should conduct their own assessment using the format in NTTP 3-07.2.1, Navy Tactics, Techniques, and Procedures for Antiterrorism. The assessment will address the broad range of terrorist threats to the security of personnel and assets and it should be conducted periodically. The assessment should consider the range of identified and projected threats against a specific location or installation. Assistance should be requested from NCIS, numbered fleet, and OPNAV N34 to ensure a complete assessment is conducted.

### **5.5.3 Risk Assessment**

Commanders should utilize threat and vulnerability assessments to make decisions about what level of risk, as part of the risk management process, they are willing to accept. Risks to the most critical Navy assets should be eliminated whenever possible, but it is ultimately the commander's decision about what level of risk to accept.

## **5.6 NAVY ANTITERRORISM/FORCE PROTECTION PROGRAM COORDINATION**

Navy units must coordinate their AT/FP programs with support organizations regardless of their location. In the United States, state and local authorities and other federal agencies provide valuable support resources that assist commanders in meeting their AT/FP needs. It is even more important for units in foreign territories to develop clear relationships with HN officials and organizations due to their relative isolation from robust U.S. services.

### **5.6.1 Operations Within United States Territory**

An important aspect of a successful AT/FP program in the United States is communication and coordination among the host and tenant commands at any installation. This refers to permanent tenant commands as well as transient units en route to another location. The installation commander has primary responsibility for security on the installation; however, each tenant is required to have a security officer or ATO. This individual must closely coordinate command actions with the installation security forces and ATO.

Nothing removes the commanding officer's responsibility for his or her command, yet there is a shared responsibility for security at each port and installation. There will normally be installation security forces on patrol and a clear understanding of the AOR of the ship and installation security forces must be established immediately. It is also important that there is rapid, clear communication between the unit's watch/security element and the installation security force to minimize any confusion as a situation may develop. Tenant commands should have a clear understanding of the host's responsibilities and exercise those security relationships regularly.

All security operations must be oriented around a defense in depth or layered approach to security and address threats from the air, surface, and subsurface. Although visible perimeters cannot be established in the air, antiterrorism procedures must consider this potential threat. Increased observation and detection capabilities may be used to compensate for the inability to implement physical barriers in the air and subsurface areas. Providing standoff distances to installations, ships, and units is one of the primary purposes of defense in depth. Standoff protects Navy forces from

improvised explosive devices (IEDs), small arms, rockets, mortars, and other weapons that have limited ranges by placing the target out of range of the threat. In addition, standoff distances give Navy forces the opportunity to identify and react to approaching personnel and vehicles.

## **5.6.2 Operations Outside United States Territory**

Commanders face unique challenges when addressing AT/FP issues outside of sovereign U.S. territory. The Navy, as a representative of the U.S. Government, must cooperate with HNs while effectively integrating AT/FP planning with the support offered and complying with stipulations of the HN. The following paragraphs highlight considerations for operating outside U.S. territory.

### **5.6.2.1 Responsibilities of Host Nation/Port Authority**

For operations conducted outside of the United States, the DOS negotiates with the HN to establish SOFA or HN support agreements. These agreements between the HN, sponsor, and contributors establish the detailed legal status of the operation. HN laws apply to official activities of U.S. forces located in the HN to the extent provided by international agreement or the SOFA. HN laws apply to U.S. forces engaged in other than official activities, unless specifically modified or made not applicable to U.S. forces by the terms of an international agreement.

### **5.6.2.2 Local and Host Nation Security Support**

A HN bears primary responsibility for maintaining security for visitors to its ports and airfields. In addition to normal security efforts by the port/airfield authority, HNs may be able to aid U.S. antiterrorism efforts through enforcement of restricted access perimeters and monitoring and escort of all vessels and personnel transiting the area. HNs may also have extensive resources to aid in the consequence management of a terrorist incident. Such a commitment from the HN must be negotiated by the DOS in conjunction with the Theater Combatant Commander or the NCC. Individual Navy units transiting a foreign port or airfield should receive specific guidance from the NCC on what to expect from the HN and the unit should liaison with the United States Defense Attaché Office (USDAO), numbered fleet, and NCIS staffs regarding additional arrangements required from HN authorities.

Contracted foreign nationals may also serve to augment a unit security element providing several benefits. Most importantly, foreign nationals may be able to take certain actions or perform functions not granted to U.S. military personnel under the DOS agreement with the HN. HN contracted security personnel may be able to use weapons and force, interdict and arrest potential terrorists, patrol restricted access areas, and provide important intelligence not available to U.S. personnel.

## **5.7 HIGH SEAS ANTITERRORISM/FORCE PROTECTION PROGRAM**

During transit in international waters the CO has full authority to protect the ship from any and all threats. Under these circumstances defense in depth is effected using the ship's combat systems in the same manner they would be used for any other mission. The CO must establish communication with the Naval component commander to update the AOR threat awareness picture and conduct appropriate training to ensure that the correct AT/FP posture is maintained. Commanders at all levels can raise FP conditions in response to increased threats and to implement antiterrorism measures outlined in those levels.

## **5.8 POST MISSION/DEPLOYMENT ASSESSMENT**

Insights gained from a mission or deployment need to be shared with the NCC, CINC, and the entire Navy. All lessons learned from AT/FP related actions should be documented locally per CINC and NCC requirements, as well as through the Navy Lessons Learned System (NLLS). This will ensure worldwide data access for all users via the SIPRNET or the NLLS CD-ROM sets that are distributed in either an unclassified or classified version. For information about the NLLS, contact the Navy Warfare Development Command (NWDC) or visit the NWDC unclassified web site at [www.nwdc.navy.mil](http://www.nwdc.navy.mil) or the classified site at [www.nwdc.navy.smil.mil](http://www.nwdc.navy.smil.mil).

# CHAPTER 6

## Consequence Management

### 6.1 OVERVIEW

This chapter highlights the planning and coordination issues that must be considered to deal with the potential consequences resulting from a terrorist attack on Navy ships, aircraft, or facilities both within the United States and in overseas locations.

### 6.2 GENERAL

The goal of the Navy's AT/FP program is to deter, detect, and deny any terrorist attack. In the event a terrorist is successful, however, the consequences of the incident must be dealt with rapidly and effectively. The same degree of planning, training, and exercising that is essential to successful completion of other mission areas is equally applicable to consequence management.

Management of terrorist incidents is divided into two interrelated phases known as crisis management and consequence management. Crisis management describes the measures taken to resolve a hostile situation to include law enforcement efforts aimed at prevention, interdiction, and threat management, as well as efforts to support investigation and prosecution. Consequence management describes the efforts to respond to and mitigate the impact of a terrorist incident on people, facilities, and infrastructure. It involves measures to treat the injured, protect health and safety, restore essential services, and provide emergency relief.

The consequences of a terrorist incident are similar to those associated with natural disasters or accidents. In both cases injuries to personnel, destruction of property, and loss of essential services are possible. The primary differences are that a terrorist incident is a man-made event. In the initial stage of response it may not even be realized a terrorist attack has occurred. Responders to an incident must remember that it could be terrorist initiated and they could be the ultimate targets. Responders must be aware of the potential for secondary devices or unexpected consequences that could include the use of biological, chemical, or nuclear agents. They must also remember the incident site is a crime scene and reasonable attempts must be made to preserve potential evidence while rescuing victims, putting out fires, and conducting other emergency response functions.

The key to effective consequence management of terrorist incidents is pre-event planning. The below described process is equally applicable to all levels, facilities, and units.

### 6.3 CONSEQUENCE MANAGEMENT PLANNING

Consequence management planning is effectively a three-step process. These phases should be familiar to most shore facilities because they are similar to disaster preparedness planning already conducted for natural and accidentally occurring events. Transiting units should be cognizant of consequence management support in place at the home port/airfield as well as in each of the locations to be visited.

#### 6.3.1 Phase One — Impacts and Consequences

The first phase identifies the potential impacts and associated consequences of a particular type of incident focusing on worst case scenarios for a particular facility or unit. For example, if a multilevel building with several hundred occupants is a potential target for a large vehicle bomb, the primary effect of such an attack is blast damage. Potential blast damage could include severe building damage or collapse. One of the consequences of building collapse is

trapped personnel, both dead and injured. In this example shore facilities should have already established the primary and backup command and control elements linking security, medical, fire, and public utility assets for responding to other types of disasters or accidents.

### **6.3.2 Phase Two — Resources Required**

In phase two the resources required to respond to the consequences and impacts of phase one are identified. In following the above example, resources would be required to rescue personnel in a collapsed structure. Additionally, a minimum number of ambulances, hospital beds, and mortuary assets would be necessary. These requirements would be compared with resources available. Where demand exceeds available resources, mitigation actions can be taken by identifying non-DOD assets and executing support or mutual aid agreements, or identifying where the required DOD assets could be obtained. Planners must realize that when bringing assets into an area they must also plan for the messing, berthing, security, and support of those assets.

### **6.3.3 Phase Three — Training and Exercising**

Once a consequence management plan has been developed, the appropriate personnel must be trained and the plan must be exercised to ensure it will function as designed. This is a continuous process and is instrumental for the effective response to a terrorist incident when confusion and uncertainty are highest. This training must include the military and civilian organizations that are a part of the consequence management team.

For specific information and procedures regarding consequence management, consult NTTP 3-07.2.1, Navy Tactics, Techniques, and Procedures for Antiterrorism.

# INDEX

*Page  
No.*

## A

Antiterrorism	
Officer responsibilities . . . . .	5-4
Antiterrorism/force protection	
Assessment process . . . . .	5-4
Board . . . . .	5-4
Foreign or United States territory legal planning . . . . .	4-4
High seas program. . . . .	5-6
Plans . . . . .	5-2
Assessment	
Risk . . . . .	5-5
Threat . . . . .	5-5
Vulnerability . . . . .	5-5
Authority and actions to exercise self-defense . . . . .	4-3

## C

Commander’s responsibility . . . . .	5-2
Consequence management . . . . .	Chapter 6
Planning. . . . .	6-1
Phase one— impacts and consequences . . . . .	6-1
Phase two— resources required . . . . .	6-2
Phase three— training and exercising . . . . .	6-2
Considerations for civilian-crewed ships operated by or for the military sealift command . . . . .	4-4
Counterterrorism/counterintelligence centers . . . . .	3-4

## D

Defining intelligence. . . . .	3-2
Definitions of legal terms. . . . .	4-2

## F

Foreign or non-United States territory antiterrorism/force protection legal planning. . . . .	4-4
---	-----

## H

High seas antiterrorism/force protection program . . . . .	5-6
--	-----

## I

Implementing the Navy antiterrorism/force protection program . . . . .	5-2
Intelligence, counterintelligence, and threat analysis . . . . .	Chapter 3
Intelligence process . . . . .	3-1

**L**

Legal considerations . . . . . Chapter 4

**N**

Navy antiterrorism/force protection program . . . . . Chapter 5  
 Navy Antiterrorist Alert Center/Blue Dart message procedures . . . . . 3-7  
 Navy intelligence . . . . . 3-2

**O**

Ongoing/in-progress terrorist incident planning . . . . . 4-5  
 Operations  
     Outside United States territory . . . . . 5-6  
     Within United States territory . . . . . 5-5

**P**

Post mission/deployment assessment . . . . . 5-6  
 Program concept . . . . . 5-1

**R**

Risk Assessment . . . . . 5-5

**S**

Security Forces . . . . . 5-4

**T**

Tasking the United States intelligence community . . . . . 3-2  
 Terrorism . . . . . 3-1  
 Terrorist  
     Attack methodology . . . . . 2-2  
         Phase one— target options . . . . . 2-3  
         Phase two— selection surveillance . . . . . 2-3  
         Phase three— target selection . . . . . 2-3  
         Phase four— detailed surveillance . . . . . 2-3  
         Phase five— training and preparation . . . . . 2-3  
         Phase six — the attack . . . . . 2-3  
     Force protection conditions . . . . . 2-4  
     Groups . . . . . 2-1  
     Tactics . . . . . 2-1  
     Threat levels . . . . . 2-3  
 Threat assessment . . . . . 5-5

**U**

United States territory antiterrorism/force protection legal planning . . . . . 4-4

**V**

Vulnerability Assessment . . . . . 5-5



## LIST OF EFFECTIVE PAGES

Effective Pages	Page Numbers
Original	1 (Reverse Blank)
Original	3 (Reverse Blank)
Original	5 (Reverse Blank)
Original	7 thru 15 (Reverse Blank)
Original	17 thru 30
Original	1-1, 1-2
Original	2-1 thru 2-5 (Reverse Blank)
Original	3-1 thru 3-8
Original	4-1 thru 4-5 (Reverse Blank)
Original	5-1 thru 5-6
Original	6-1, 6-2
Original	Index-1 thru Index-3 (Reverse Blank)
Original	LEP-1 (Reverse Blank)





**NWP 3-07.2**