Navy Antiterrorism/Force Protection (AT/FP) Program

CAPT Dan J. Morgiewicz, USN
11 February 2004
Prologue

- **Navy AT/FP Evolved in response to:**
  - Beirut Barracks ’83 (Long Commission)
    - ATAC
    - NIS Code 24 / OP 09N
  - Khobar Tower ’96 (Downing Task Force)
    - OPNAV N34
    - IVA Program Stood Up
    - Training Continuum begun for all hands
  - USS Cole ’00 (Gehman/Crouch Commission)
    - AT/FP Task Force
    - PIVA begun for expeditionary ports
    - NWP / NTTP / NMETLS
  - 9/11
    - AT/FP Task Force, Round 2
    - Formal Melding of N34/Code 24
## History of Terrorist Attacks

<table>
<thead>
<tr>
<th>Perceived Threat</th>
<th>Beirut</th>
<th>Khobar Towers</th>
<th>African Embassy</th>
<th>Cole</th>
<th>11 Sep</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sniper</td>
<td>Small bomb (interior)</td>
<td>Small bomb (interior)</td>
<td>Pier Side Attack</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Destructive Mechanism</th>
<th>Beirut</th>
<th>Khobar Towers</th>
<th>African Embassy</th>
<th>Cole</th>
<th>11 Sep</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bomb</td>
<td>Bomb</td>
<td>Bomb</td>
<td>Bomb</td>
<td>Bomb</td>
<td>Hijacked Airplane</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Delivery Method</th>
<th>Beirut</th>
<th>Khobar Towers</th>
<th>African Embassy</th>
<th>Cole</th>
<th>11 Sep</th>
</tr>
</thead>
<tbody>
<tr>
<td>Truck</td>
<td>Truck</td>
<td>Truck</td>
<td>Truck</td>
<td>Boat</td>
<td>Hijacked Airplane</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Geographic Region</th>
<th>Beirut</th>
<th>Khobar Towers</th>
<th>African Embassy</th>
<th>Cole</th>
<th>11 Sep</th>
</tr>
</thead>
<tbody>
<tr>
<td>ME</td>
<td>ME</td>
<td>Africa</td>
<td>ME</td>
<td>US</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Intel</th>
<th>Beirut</th>
<th>Khobar Towers</th>
<th>African Embassy</th>
<th>Cole</th>
<th>11 Sep</th>
</tr>
</thead>
<tbody>
<tr>
<td>General threat</td>
<td>General threat</td>
<td>General threat</td>
<td>General threat</td>
<td>General threat</td>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Lesson</th>
<th>Beirut</th>
<th>Khobar Towers</th>
<th>African Embassy</th>
<th>Cole</th>
<th>11 Sep</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application of rules of engagement</td>
<td>Greater stand-off distance</td>
<td>Recognize world-wide threat</td>
<td>Anticipate new methods</td>
<td>US at Risk, innovation</td>
<td></td>
</tr>
</tbody>
</table>
New Assumptions/Mindset

• We Face:
  - Strategic “Anti-Access” Terror Campaign
  - Well Resourced/Trained/Motivated Operatives
  - Multi-Theater Operations
  - Large Vehicle Bombs Remain a Likely Method
  - Targets May Include Ships, Aircraft, Bases
  - Not Necessarily (Not Primarily) Military Targets
  - World-Wide Threat, Including (Especially) US
  - Suicide Bombers
  - Possible Rogue Actors

• So ....
  - “Really” Need Competent Deterrent Posture, Scalable According to Threat/I&W
Be Prepared to ....

- **Deter**
  - "Hard Look"
    - Weapons
    - Uniforms
    - Body Armor
    - Dogs
  - Randomness
    - Roving/Mobile Forces
    - Measures

- **Detect**
  - Open Eyes and Ears
  - Technology
  - Intel/Law Enforcement Liaison
  - Counter-Surveillance

- **Defend**
  - Reaction

- **Mitigate Consequences**
  - Pre-Planned Responses
N34/NCIS

• N3/N5 responsible for AT/FP - Operational mindset/structure to report to CNO
• NCIS(NO9N) responsible for LE/Phys Security
• Merger left basic functions of N34 & NCIS intact
  - Advocated by Navy leadership (VCNO) since 1997
  - Parallel with Joint Staff and other Services
  - Builds on combined expertise of the two organizations
  - Single “belly button”/SMEs
• Synergy of effort
  - AT/FP, law enforcement, physical security, CbT and Counterintelligence functions are intrinsically linked
  - Cannot divide current N34/NCIS organization without incurring duplication of effort
• Enhances speed and agility, force multiplier
• Assessment sponsor is honest broker
  - Independent and unencumbered by constituencies
• Co-locates all aspects of AT/FP with N34 in charge:
  - Policy, Doctrine, Training
  - Vulnerability Assessments, CBRNE
  - RDT&E, Leverage Technology, Security Systems
  - PPBS and Budget Execution
  - Law Enforcement/NSF, Reserves/Personnel
  - Personal Security Operations, Regional Inv. Coord.
  - Nuclear Weapons Security, USMC MSF Bn (FAST)
N34/NCIS

- Seamless ID of threats (terrorist, CBRNE, criminal and foreign intel) and response
- N34/NCIS focus is AT/FP only
- Interacts with Congress, GAO, Naval Audit Service, others w/one voice
- Closer Navy working relationships with Interagency and DOD technology working groups
  - Minimizes duplication of effort
  - Quicker solutions
Threat Levels

- Threat Level Measures Degree of Risk to personnel, facilities, assets or interests
- DIA Declares Threat Level based on threat factors

**Factor**
- Existence
- Capability
- History
- Intentions
- Targeting

**Levels**
- High
- Significant
- Moderate
- Low
Force Protection Conditions

• Force Protection Condition (FPCON):
  – Decision by Responsible Commander to guard against the threat

• Selected based on assessment of the threat

• Subordinates May set Higher Condition/Measures
  • FPCON Delta
  • FPCON Charlie
  • FPCON Bravo
  • FPCON Alpha
  • FPCON Normal- General Global Threat of Terrorist Activity
    – Baseline security posture (no specific measures identified)
Security Continuum

• Good Order and Discipline
• Law Enforcement
  – Anti-Theft/Vandalism, Traffic/Crowd Control, Missing Persons, Drugs, etc
• Security
  – Anti-Espionage, Physical Security, Surveillance, High Value Compounds
• High-Risk Billets/Personal Security Details
• Force Protection
  – Anti-Terrorist
  – Scalable Deterrent Posture (Threat Driven)
• Nuclear Weapons Security
  – Constant, “Zero Defect” Posture - Consequence Driven (Not Threat)
• War-Fighting
  – Lock Down, Defeat “SPETZNAZ-Level” Threat, “Fight for Life”
Training Continuum

- Level I
  - All hands basic situational awareness and program standards
- Level II
  - ATO for ship or commands
- Level III
  - PXO/PCO training
- Level IV
  - Senior command, flag level training done by JCS
- Fleet level training
  - Conducted by fleet commands at the individual, unit and battle group levels
Initiatives (Training)

• CATNSF: Center for Antiterrorism/Naval Security Forces
  • Single center of Navy ATFP training
  • Armed Sentry
  • “Chief of the Guard”
  • Commanders Course – Level III add on options

• NSF 21 training review
  • NCIS/N34 level review of MA training program

• Web Based Level I Training
  • Broadening distribution
  • Enhanced Server to accommodate high usage level
  • Updated guidance regarding hijacking
# Naval Security Forces

<table>
<thead>
<tr>
<th>Year</th>
<th>End-strength</th>
<th>9545</th>
<th>MA</th>
</tr>
</thead>
<tbody>
<tr>
<td>FY01</td>
<td>1911</td>
<td>698</td>
<td>2273</td>
</tr>
<tr>
<td>FY02</td>
<td>2723</td>
<td>4641</td>
<td>250</td>
</tr>
<tr>
<td>FY03</td>
<td>7327</td>
<td>3040</td>
<td>2723</td>
</tr>
<tr>
<td>FY04</td>
<td>8167</td>
<td>2200</td>
<td>8167</td>
</tr>
<tr>
<td>FY05</td>
<td>8867</td>
<td>1500</td>
<td>8867</td>
</tr>
<tr>
<td>FY06</td>
<td>8867</td>
<td>1500</td>
<td>8867</td>
</tr>
<tr>
<td>FY07</td>
<td>8867</td>
<td>1500</td>
<td>8867</td>
</tr>
</tbody>
</table>

*Conversion rates:
- FY01: 459
- FY02: 1115
- FY03: 692
- FY04: 450
- FY05: 250
- FY06: 250
- FY07: 1179
Ongoing Initiatives

- MA Evolving to NSF
- NCIS Transformation
- Policy and Doctrine
  - NWP, NTTP
- Comprehensive Retooling of Training
  - Simulators, Distance Learning
- Nuclear Weapons Security
- Military Sealift Command Force Protection
- HN/Local Cooperation/Support
  - 2 Way Street
- Mobile Security Force
- Technology .....
Acquisition Roles and Responsibilities

- Strategy
- Policy
- Vulnerability Assessments
- Manpower
- Capability Assessments
- Technology
- Capability Assessments
- Resourcing
- Capabilities to the Fleet

N6/7 (Sea)
N70 (coordinate)

N34

N4 (Shore)
N46

CFF

Fleet input

Fleet input
Acquisition Coordination

SLG
- Coordinate AT programs
- Arbitrate SALT issues

SALT
- Assist PEO/PMs
- Coordinate effort
- Prevent duplication

PEO/PM NAVSEA
PM NAVFAC
SPAWAR
NAVSUP
NAVAIR

Afloat
N70
N3
4

Ashore
N46
Vulnerability Assessments

- Conducted by either the Joint Staff (JSIVA) or CNO (CNOIVA)
- Mandatory every 3 years; every 1 year for bases in high threat areas
- Are done for military installations only
- Conducted by security experts
- Port Integrated Vulnerability Assessments (PIVA) conducted by teams made of fleet representatives and NCIS security specialists
- Timing dependent on Fleet Commanders needs and risk assessment
- For expeditionary ports both CONUS and OCONUS
NAS North Island Overall Plan
Perimeter Security
Proposed Smart Gates

- Pier Gate
- Main Gate
- Golf Course Gate
Pier Gate

REFERENCE PLAN
VIEW FOR EQUIPMENT
DESCRIPTIONS

VEHICLE CONTROL DIAGRAM
AUTHORIZED ENTRY & EXIT
ONLY (4 LANES TYPICAL)
PRELIMINARY DESIGN
Waterside Security System
Waterside Security System

CCTV Color Cameras

L/R Thermal Imager; 100/500 mm lens (can view beyond the chart)

S/R Thermal Imager; 50/150 mm lens

Dunlop 22” Line of Demarcation

Underwater Swimmer Detection Sonar
Ashore C2 - Regional Structure

Navy Region
- Northeast
- Mid-Atlantic
- North Central
- South Central
- Midwest
- Northwest
- Hawaii
- Pensacola

Installation Claimants
- Korea
- Japan
- Guam

Naval District
- Washington
- Bahrain
- Europe

Naval Regions
- Northwest
- South Central
- South Central
- Naval Region
- Pensacola

Installation Claimants
- PACFL
- RESFOR
- CNET
- NAVSEA

Naval Commands
- NAVSEA
- NAVAIR
- REG CDR / REG COORD
- LANTFL
- CNE

Local Coordination
Technology vs. Manpower

- Technology cannot fully replace manpower
- Technology can assist to deter, detect, delay and assess, making manpower more efficient
  - CCTV and swimmer sonar “display a picture,” but someone must interpret it
  - Card swipe systems still require personnel to make badges, manage database and monitor systems
  - Technology use at Entry Control Point (ECP) adds risk (e.g., piggybacking) and some delay
- Response and neutralization (roving patrols and reaction force) always require personnel
Questions
Counter Bomb/Counter Bomber ACTD

- In beginning phase
- Demos begin in FY 04
- Assessment phase:
  - Relational analysis
- Detection phase:
  - Identify bomber threat
  - Characterizes potential threat
  - Standoff detection is goal
- Mitigation phase:
  - Long range neutralization
  - Blast and fragment
Cons Against N4 - N34

- No single focus on AT/FP
- Less speed and agility
- Loss of operational mindset
- Loss of synergy, “scattering the coals”
- Creates new seams
- No N4 link to intelligence, threat or law enforcement pieces of the FP continuum
- Less objectivity due to N4 being resource sponsor with constituencies
- CFFC does not possess necessary staff, experience or authority to take on N34 responsibilities
ASSESSMENTS

• Joint Staff Integrated Vulnerability Assessments
  - JS/DTRA Experts
  - Assess DOD Installations World-wide

• CNO Integrated Vulnerability Assessments
  - Completed by NCIS/CNO N34 Experts
  - Assess US Naval Installations World-wide

• Port Integrated Vulnerability Assessments
  - Completed by CINC staff and local NCIS agent
  - Assess non-US navy ports both in US and abroad
**Security Programs**

**Swimmer Detection**

- AN/WQX-2 swimmer detection sonar undergoing upgrade
- Also developing and testing COTS (e.g. Kongsberg) sonar head and others with help from NAVSEA

**Waterside Security Systems**

- Combined radar and electro-optics (both thermal and CCTV) to detect and classify targets
- Currently installing in La Maddalena, Gaeta, Sounda Bay, Augusta Bay, Rota and San Diego Region
Navy Explosive Detection Equipment

- EGIS II desktop, VaporTracer 2 handheld and Rapiscan 520 X-ray imaging system were judged best by the Navy/N34
- Mobile vehicle being evaluated for large vehicles.

Force Protection and Physical Security Communities of Practice Program

- Web enabled portal designed to collect, organize and disseminate information to the AT/FP and Physical security community
- Variety of tools available
Steel Port Security Barriers

• Will stop up to 38 foot go-fast boat weighing 8000 lbs at 52 mph

• 50 foot units; 8 ft tall; 8500 lbs

• $520 per linear foot; steel construct

Composite Port Security Barriers

• Design and testing

• Will stop up to 38 foot go-fast boat weighing 8000 lbs at 52 mph

• 50 foot units; 8 ft tall; 4200 lbs

• $720 per linear foot; fiberglass polymer

• Design and testing
Dunlop Security Barriers

- Will stop up to 38 foot go-fast boat weighing 8000 lbs at 52 mph
- 82 foot units; 8 ft tall; 3000 lbs
- $580 per linear foot; rubber coated textile with steel cable
  
  Lines of Demarcation
- 20 year life; little maintenance
- No boat stopping capability
- Physical line in water to show restricted area boundaries
- Can be of various sizes and constructs; depending on desired usage
- Design and testing
• **Vehicle control**

Large Vehicle Mobile X-ray Trucks for inspection at gates
- Presently in use at NSA Bahrain and NS San Diego
- Future sites: TBD

Access Control at gates includes barriers and new pass technology
Technology/Security Equipment

- Flightline Security - Electronic Sensors, Ongoing
  - NAS Rota
  - NAS LeMoore

- Special Weapons Access Upgrades
  - SWFPAC Bangor
  - SWFLANT Kings Bay
  - TACAMO Travis AFB, Tinker AFB, NAS Patuxent River

- General IDS for Bases, Upgrades/New
  - NSA Bahrain
  - Camp David
**Goals** -

Deliver ATFP Technology Systems with:

- Speed *and* Support
- Reduced Reliance on Manpower
- Interoperability and Tailor-ability

**Approach**

- A Common ATFP C2 System with Standard Interface for Sensors/Engagement Systems
- A “Catalog” of Available Sensors/Engagement Systems to feed the ATFP C2 System
- Transition for each of these into a SYSCOM Program of Record for ILS
Swimmer Detection Sonar (SDS)

• NAVSEA Testing at North Island
  - 4-6 COTS types expected
  - Test & Evaluation in progress
  - Long poles:
    • Environmental assessment
    • Contracting / solicitation
    • Platform availability
    • Diving services
Waterside Security System—North Island

Operational in April 2003
Area Security Operations Command and Control (ASOCC) Deployment

Information Management

Situation Management

Collaboration

ASOCC is fully integrated multi-echelon decision and collaboration C2 System.

1. The ASOCC Mission needs statement developed as a direct result of USS Cole bombing.
2. All requirements have been validated and mapped through the Joint process.
3. Licensed to operate for 3 years on SIPR net by DISA. Interim authority to operate on NIPR net for 1 year by DISA.
4. ASOCC is GOTS, no re-occurring licensing fees and designed for open architecture exploitation.
**JHOC using ASOCC**

**Common Operating Picture**

- USN Escort PBs
- USCG Escort Vessel
- Customs Inspections
- Border Patrol Interest
- Security Zone Management
- Story Boards
- Incident Briefing
- Weather and Tides
- Incident Action Plans
- Response Objectives
- Resources-At-Risk Summary
- Situation Display Map
- Incident Area Map/Chart
- Digital Photos
- Organization Chart
- Incident Status Summary
- Resource Status
- Meeting Schedule
- Blue Force Locator

**Shared Features**
- Vessel and asset real-time position tracking on Radar
- 96 Hr Notice of Arrival
- Port Security alerts
- Broadcast Notice to Mariners
- Chat Room
- Port Security Video Surveillance Monitoring
- Vessel Schedule Calendars
- General Port Info and Dir
- Vessel Characteristics
- Marine Terminal Database
- Marine Event Permits
- Hazardous Cargo Tracking
- Ad Hoc Web Reporting & Analysis
- Secure shared database
- Incident log tracking
- Wireless PDA Integration

**Non-Federal Features (state, non-profit, private sector, and public)**
- Chat Room
- Automatic Alerts
- Smart Scheduling / auto schedule de-confliction
- Pilot and Tug Dispatching
- Biometrics for Access Control to Port Facilities
ASOCC Deployments

**Bold** = Installed
Regular = Near term installations planned
*Italics* = NORTHCOM Sponsorship
FY03 Physical Security Equipment (PSE) OPN

- FY03 OPN = $107.1M
- MSC: $40.2M
- Boat barriers: $20.5M
- Waterside Security Systems: $21.2M
- MILCON Intrusion Detection Systems: $15.0M
- Other: $6.35M
- JHOC: $2.5M
- NDW: $1.0M
- LRAD: $0.35M
- Contingency: --
  - Due to recent transfer to SSP and AAUSN inflation adjustment
Waterside Security Systems (WSS)

• WSS installations in progress or in planning:
  - In progress: North Island
    • Issue: contractor performance
  - In planning:
    • Souda Bay
    • La Maddalena, Gaeta, Augusta Bay
    • Norfolk

• Long-term plan (FY04 to FY07): WSS and boat barrier installations in 13 other significant CONUS and OCONUS Navy ports

• Key to long-term plan: NAVFAC execution of OPN funding
US Port Security

- **Waterside Security Systems**
  - Provides 24/7 surface RADAR, electro-optical and sub-surface SONAR coverage with integrated command and control.
  - Installed at NAS North Island and NSA Bahrain, NSBs Kings Bay/Bangor
  - Future Installations: NS San Diego, NSB Point Loma, Norfolk, La Maddalena, Gaeta, Augusta Bay, and Souda Bay
• Camp David
  - Perimeter IDS
  - Perimeter CCTV
  - New Monitoring Equipment

• Brunswick - “Gate Keeper/Smart Base”
  - CAC with new “contactless” technology
  - Wearable Wireless Computers for Gate Guards
  - Fully automated access control and visitor passes

• Guantanamo Bay, Cuba
  - Emergency Command Center
  - Perimeter Optics to thermal and long range CCTV
  - Camp Delta perimeter security system
  - Flightline / Waterside security system