Architectural Challenges in Countering Existential Terrorist Threats:
Lessons from a decade of studying "Loose Nukes"

Presentation by Ambassador Henry F. Cooper

46th IEEE International Carnahan Conference
On Security Technology

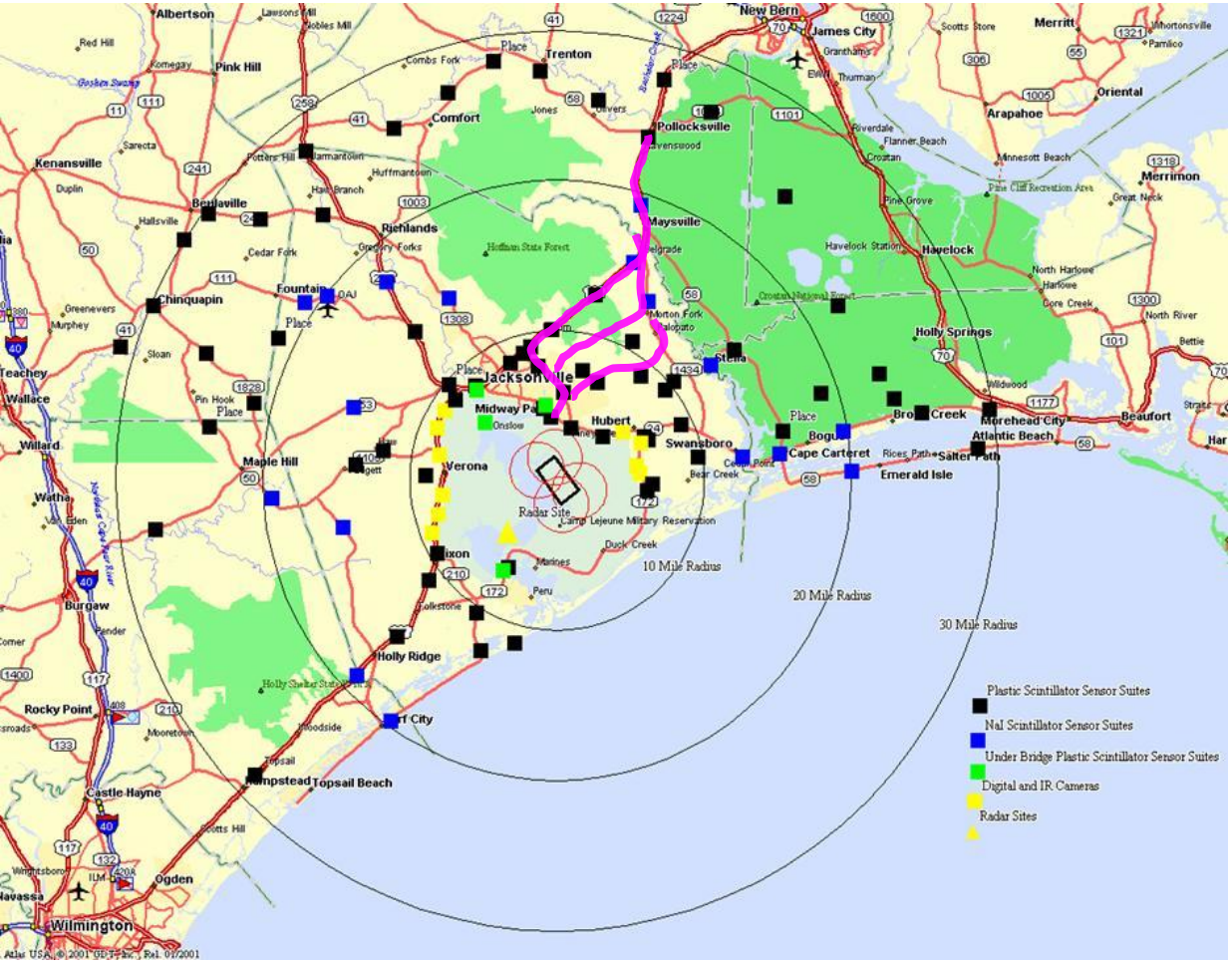
October 16, 2012

Boston Marriott Newton

Architectural Challenges in Countering Existential Terrorist Threats: Lessons from a decade of studying "Loose Nukes"

- Drawn from studying how to counter terrorist threat of smuggling a nuclear weapon to attack the US:
  - Camp Lejeune Unconventional Nuclear Weapon Defense (UNWD) Test Bed Demonstration
    - Successful legacy being extended to protect other Marine Bases
  - DHS/HSARPA—DHS/DNDO Architecture Study
    - Bottom Line: Give priority to overseas countermeasures
  - DTRA Bosporus Study
    - Early ("Left of go") Indications and Warning (I&W) is the key to success
- Key Bottom Lines:
  - Technology is important but there is no silver bullet
  - Bureaucratic Impedance is a big problem
  - Empowering Local Authorities is the key to success

Starting Point: Camp Lejeune/Onslow County, NC Layered Detection Concept



- **Camp LeJeune UNWD Testbed**
  - Operational since Feb 03
  - Includes JSIPP Sensors
  - Fully integrated military and civil law enforcement and disaster response activities
  - DSB: MCTFER "Best of Class"

Military-Civilian Task Force for Emergency Response (MCTFER)

- **Layered Detect/ID Sensors**
  - Front Gate to 30 miles out
  - Highway, rail, and water
  - Passive tracking with cameras
  - Red-Blue-White Team design

Successfully transferred to Marines for operations—sensor improvements now included and operations being extended to other Marine bases—perhaps including Pacific bases

Camp Lejeune-Onslow County UNWD Sensors

Rail Rad Sensors

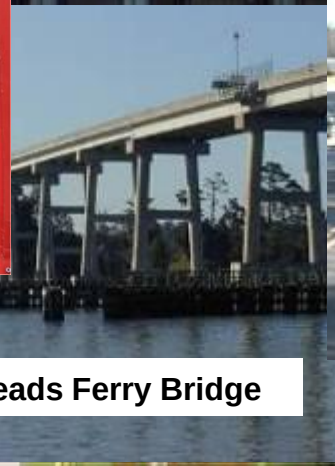
Portable MobileRad in Police Car

Radar for Tracking Boats

Electrical Box Detector

Hand-Held/Gate Inspections

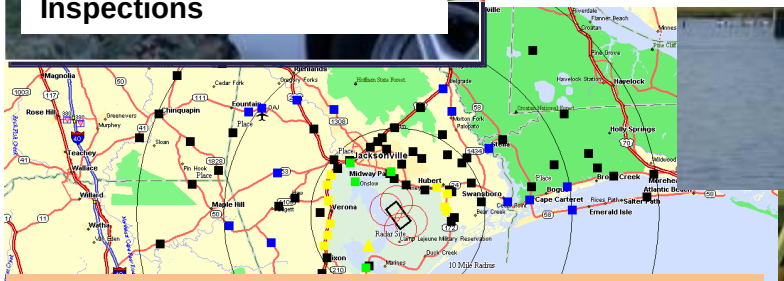
Nal Gamma Detector



Sneads Ferry Bridge

Automatic Tag Photo @ 70 mph

Jersey Barrier Detector



Neutron Detector

Onslow Beach Bridge

Notional Sensor Distribution – Out to ~30 Miles

- 4 Radiation Sensor Layers – Detect, ID and Track
- Camera/Radar/Seismic Aid Tracking
- Alarm/Alert System Informs EOC/Responders
- Respond in Time to Prevent Attack on Base
  - By Road, Off-Road, Water, or Rail

Key Lessons from Camp Lejeune UNWD Effort

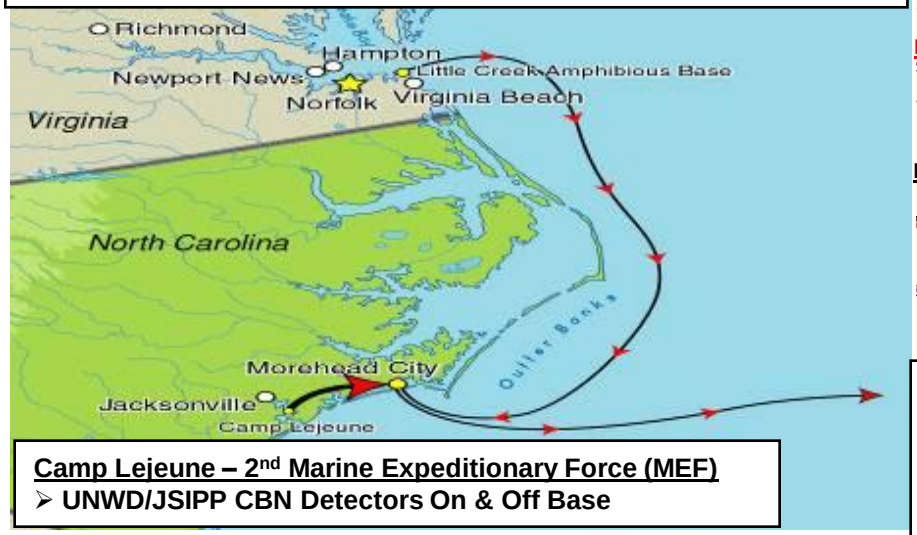
- Demonstrated/Validated Red-Blue-White Team Design Approach
- Unattended Ground Sensor Suites Feasible
  - Synthesized RN & Other Sensor Data
    - Unshielded and Lightly Shielded Devices
    - On Open Highway and at Portals (Slow and Not-So-Slow Traffic)
  - This Important ARA Conclusion was Controversial
    - Marines/Onslow County Officials Very Impressed
    - Operations continue after a decade and are being improved and extended
- Heavy Shielding to Avoid Detection
  - Precludes Manhandling Weapons Off-Road
  - Provides an Exploitable Signature (Concentrated Mass)
- Most Difficult Threat Scenarios Involve "Light" Devices
  - Man-Portable/ATV Transport to Avoid Choke Points
  - Water Approaches Particularly Troublesome, Especially with Effective Shielding
  - "Upstream" Tip-Off Information Very Useful
- Excellent Military-Civilian Operations Possible
  - Train Together to Operate Together

<u>The bad news</u>:

After effective DoD and DHS operations were demonstrated as a congressionally mandated program, and as the Marines accepted and expanded the Force Protection aspects, bureaucratic interests disconnected the DHS and DoD support for off-base operations.

Missed Opportunity to Extend Force Protection to Norfolk: Critical to Deploying Marines

Hampton Roads-Norfolk Essential to 2nd MEF Deployment



Camp Lejeune – 2nd Marine Expeditionary Force (MEF)
- UNWD/JSIPP CBN Detectors On & Off Base

Key Hampton Roads-Norfolk Commands
- Four 4-star Service, Joint and NATO Commands
- 12 Military Bases – 5 Guardian Bases in Red
- Nation's Only Shipyard Building A/C Carriers
- Medical, Research, Intel & Training Facilities

Exploiting Camp Lejeune Proving Ground

Camp Lejeune Testbed – Only UNWD/JSIPP Base:
- Military Civilian Task Force for Emergency Response (MTFER) Distinctive – Called "Best-of-Class" by 2003 DSB
- Significant Off-Base "Outside the Fence" Operations
  - A Rare Capability Recommended by 2003 DSB
- CBRNE Protection Model to be Followed
  - Being Done by Fairfax County EOC
  - Prove Technology/Response Architecture at Lejeune
    - Validate Operations For More Complex Military-Civilian Environments, e.g., Norfolk

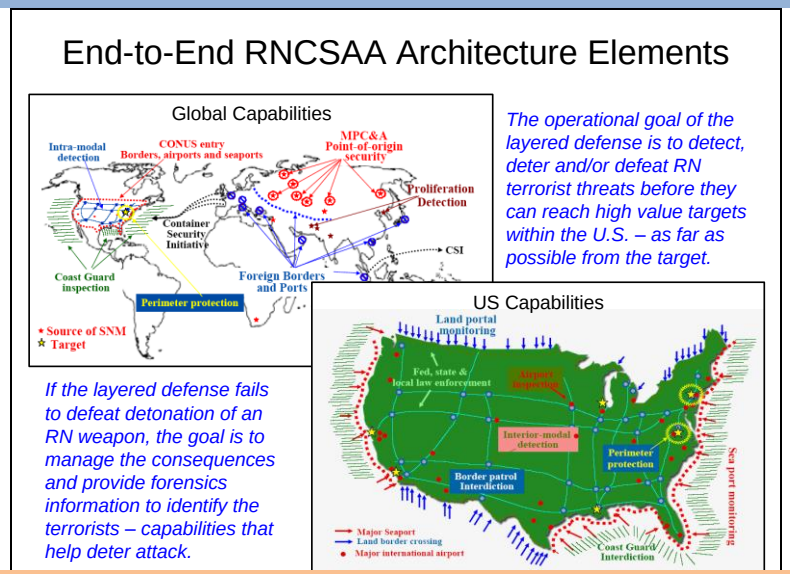
Recommended Strategy:
- Enable Camp Lejeune/MCTFER as a Proving Ground
- Demonstrate Prototype at Major Port – Norfolk
- Proliferate Proven Capability

Recommended UNWD Program Extension

FY2005 Objective: Within 12 Months for $20 million
- Expand Camp Lejeune Sensors to Morehead City
- Deploy Norfolk Testbed Using Camp Lejeune Pattern
- Integrate Defense & Homeland Security Dept. Efforts
- Establish/Validate Military-Local/State/Federal Regional
- Protection – In Support of Critical National Security Mission

Follow-on Long-Term Objectives:
- Integrate with Coast Guard/Navy Operations
- Fill-in Jacksonville, NC to Norfolk Regional Defense
- Complete Full Spectrum CBRNE Protection
- Improve by Spiral Development
- Extend to Entire East Coast & Gulf Coast

Radiological & Nuclear Countermeasure System Architecture (RNSAA) Analysis for DHS/HSARPA and DHS/DNDO



The operational goal of the layered defense is to detect, deter and/or defeat RN terrorist threats before they can reach high value targets within the U.S. – as far as possible from the target.

If the layered defense fails to defeat detonation of an RN weapon, the goal is to manage the consequences and provide forensics information to identify the terrorists – capabilities that help deter attack.

***Objective** – Prevent attack, as far away and as early as possible; "Keep the terrorists in a re-planning mode." Layered Defense Architecture is the Key*
No Wide Open Paths to Targets!

Architectural Layers

- **Point of Origin**
- **Transit to POD/Border/Coast**
- **Exit from POD/Border/Coast**
- **Transit to US (Including Intermediary Stops)**
- **Entry to US (POE/Border/Coast)**
- **Transit to Target**
- **Terminal Layer**

- Worldwide Threat Context
  - Maritime/Overseas Threat Analysis
  - Complementary ARA NORTHCOM Futures Effort
- **Red-Blue-White (RBW) Team Approach**
  - **Independent Red Team**
  - **Blue Team Architect**
  - **White Team Referee**
- Phase I Focused on RN Threats to the National Capitol
- Phase II – Proposed to Extend Upstream as far as possible

***Key Conclusions**: - Camp Lejeune concept of proliferated sensors very expensive*
- Very difficult to counter "loose nuke" once within the US
- Priority should be given to stopping loose nuke overseas

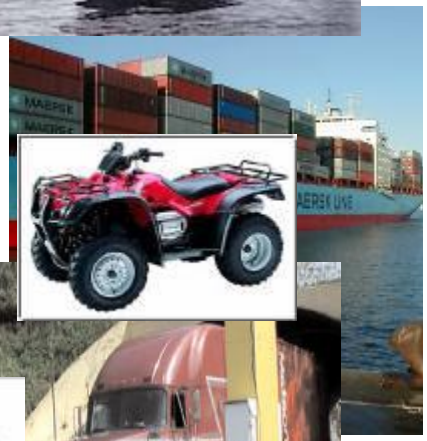
Infiltration– Key Red Team Considerations of Threat to Washington, DC

Careful, Deliberate, Patient

- Avoid high traffic areas
- Continuously monitor approach routes – Avoid choke points
- Armed response/escorts keep device in sight

Device

- Movement not likely surrendered to commercial transportation
- Armed and multi-triggered for immediate detonation while in-transit
- Shielded as necessary (Pu device) and effectiveness checked with high-quality radiation detector equipment



Key Observations

- Air transport/delivery best choice
- Pleasure water craft (20-26')
- Rail transport not attractive
  - Few if any contingency options
  - Lack of positive control
  - Channelized routes
- SUV, Utility Trucks, and Limousine-type vehicles for roadway delivery preferred
- Avoid Interstates; likely choke points
- Off-road vehicles/routes where possible
- Adopt Diversionary Tactics
- Communications protected (secure/encrypted) throughout

Key Bottom Lines:

- Avoid Stream-of-Commerce and obvious chokepoints, primary DHS/DNDO focuses
- Red has an advantage once the weapons are on the move
- Effective response depends critically on local law enforcement capabilities

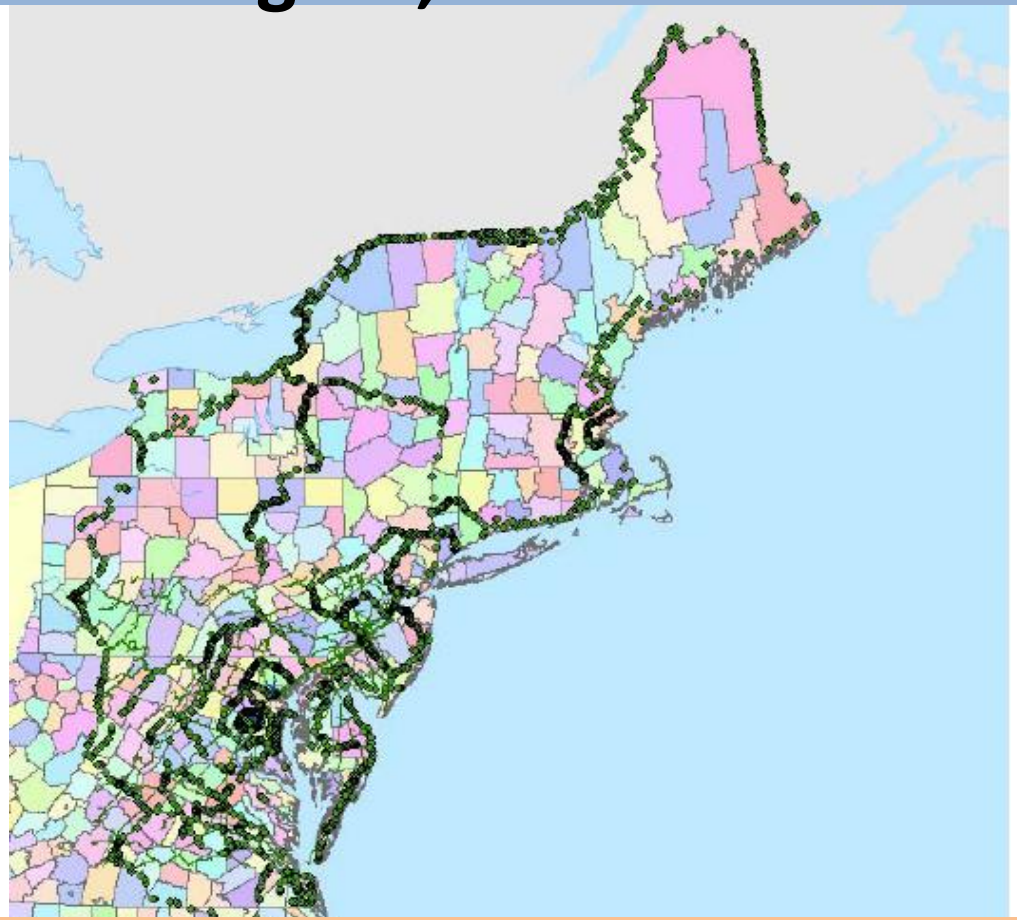
Observations From 17 RBW Scenarios

Scenario	Number of Safe-houses	Transportation Method Used to Reach the Target							Number of Potential Detections
		Roads			Off-Road	Rail	Water	Air	
		Interstate	Major	Secondary					
P1 Richmond, VA to the Capitol/White House	2		X	X		X			4
V1 Westminster, MD to L'Enfant Plaza	1		X	X		X			9
V2 Richmond, VA to the Capitol/White House	2		X	X		X			10
V3 Martinsburg, WV to CIA Headquarters	1		X	X		X			5
V6 Culpepper, VA to Federal Triangle Metro	1		X	X		X		X	3
V7 Culpepper, VA to the Capitol/White House	2		X	X				X	3
V8 Leesburg, VA to CIA Headquarters	2		X	X		X			6
V9 Charlottesville, VA to the Pentagon	1		X	X				X	12
V10 Winchester, VA to the White House	1		X	X		X			5
M1 Owings Mill, MD to the White House	2		X	X		X			4
M2 West Virginia to Fed Ex Field	2		X	X		X			7
M4 Odenton, MD to the Capitol	2		X	X				X	2
M5 Owings Mill, MD to L'Enfant Plaza	1		X	X		X			3
D1 Delmarva Peninsula to the Capitol	2		X	X	X		X		3
D2 Delmarva Peninsula to Washington Navy Yard	1		X	X			X		3
D3 Delmarva Peninsula to Washington Navy Yard	1		X	X			X		2
D4 Delmarva Peninsula to FedEx Field	2		X	X			X		2

- **No Scenarios used Interstate, POEs – All avoided "Stream-of-Commerce"**
- **Rail & Roadway approaches usually produced many detection opportunities**
  - **Crisis/Response Management is key problem – Beltway "Last Ditch" Case Study**
- **Safe-houses cut both ways – slower attack helps defender; intermittent "hits" help attacker**
- **Small A/C overflew sensors reducing hits – of more concern is they could fly all the way**
  - **Consider Threat form Air in more detail – LAX Case Study**
- **Waterway approaches generally had fewer, intermittent detection opportunities**
  - **Recreational/Fishing Boats to Delmarva Peninsula a key threat**
  - **Consider Threat from the Atlantic in more detail – Norfolk Area Case Study**

Possible Eventual Northeastern Regional Testbed to Protect Washington, DC

- **Comprehensive Detector Array**
  - US financial and political centers
  - 12 States and their capitols
  - ~70M People, ~25% of US population
  - 35 Major cities (>100,000), including Boston, New York, Philadelphia, Washington, Richmond, Norfolk
  - Hundreds of counties, cities, small towns, etc.
- **Significant part of potential backbone of internal US layer**
  - Internet with ports of entry (POEs) – seaports, airports, border crossing
  - Integrate with strategy to detect crossings other than these POE
  - ***Overlay with mobile/transportable detectors and strategy for decoys***
  - Integrate with intelligence, sensors & analysis
  - Engage Ops of Coast Guard, Navy, Border Patrol, NTM, etc. to develop & demonstrate detection/interdiction CONOPS
- **Spiral Development of S&T**



Estimated Northeast US Detector "Virtual" Layout

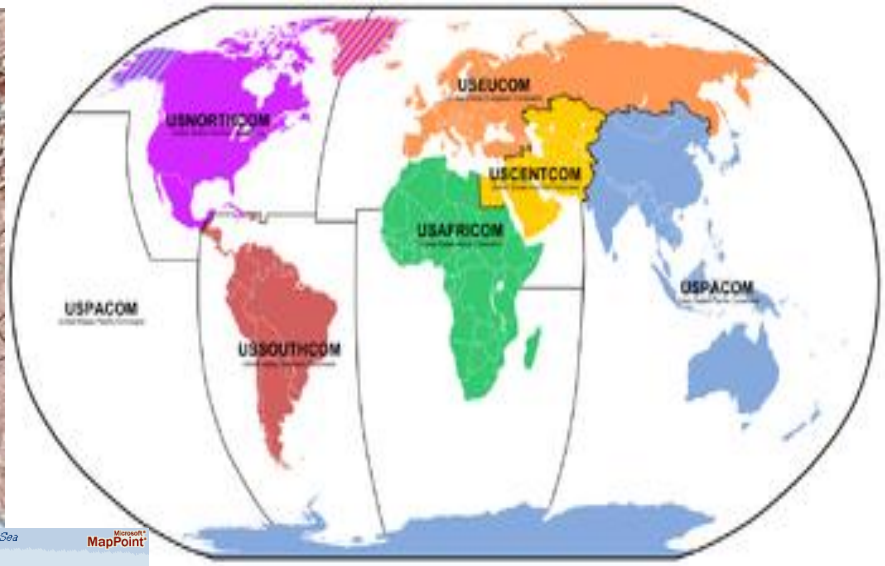
- ~3500 fixed detector locations – fill as testbeds develop
- Reduce Costs with Fixed/Mobile Mix, Decoys & Deception
- Develop local, state and federal cooperative procedures
- Obviously a very complex, expensive effort

These Considerations Prompted Seeking to Stop the Threat Overseas

- Sought sponsor with overseas responsibilities
  - Settled on the Defense Threat Reduction Agency
  - Had sponsored our UNWD effort
  - Nunn-Lugar and DoD “overseas” missions
  - Ret. VADM Pete Nanos was interested
- Focused on “loose nukes” in Black Sea region
  - Near key threat areas—Former Soviet Tactical Nuclear Weapons
  - Historic Smuggling Routes introduce significant complexities

Bosporus Study Objectives

- Understand better the complex, "end-to-end" technical and political-military issues that an effective CONOPS must address to counter nuclear smuggling through the Black Sea Region
- Recommend appropriate PolMil, Intelligence and Technical solutions



How best to exploit geographic and other choke points?

How best to engage Intelligence/Ops to counter WMD?

Key Role of Roundtables & Tabletop Exercises: Understand Issues & Gain Stakeholder Buy-in

Technology Community

Intelligence Community

Pathway Analysis

PolMil/Ops Community

Assume Typical WgPu-ID Sources

Small Atomic Demolition Munitions (SADM) in Transport Container (~150 pounds) – Yield = 10 tons-1 kiloton; according to http://en.wikipedia.org/wiki/Special_Atomic_Demolition_Munition

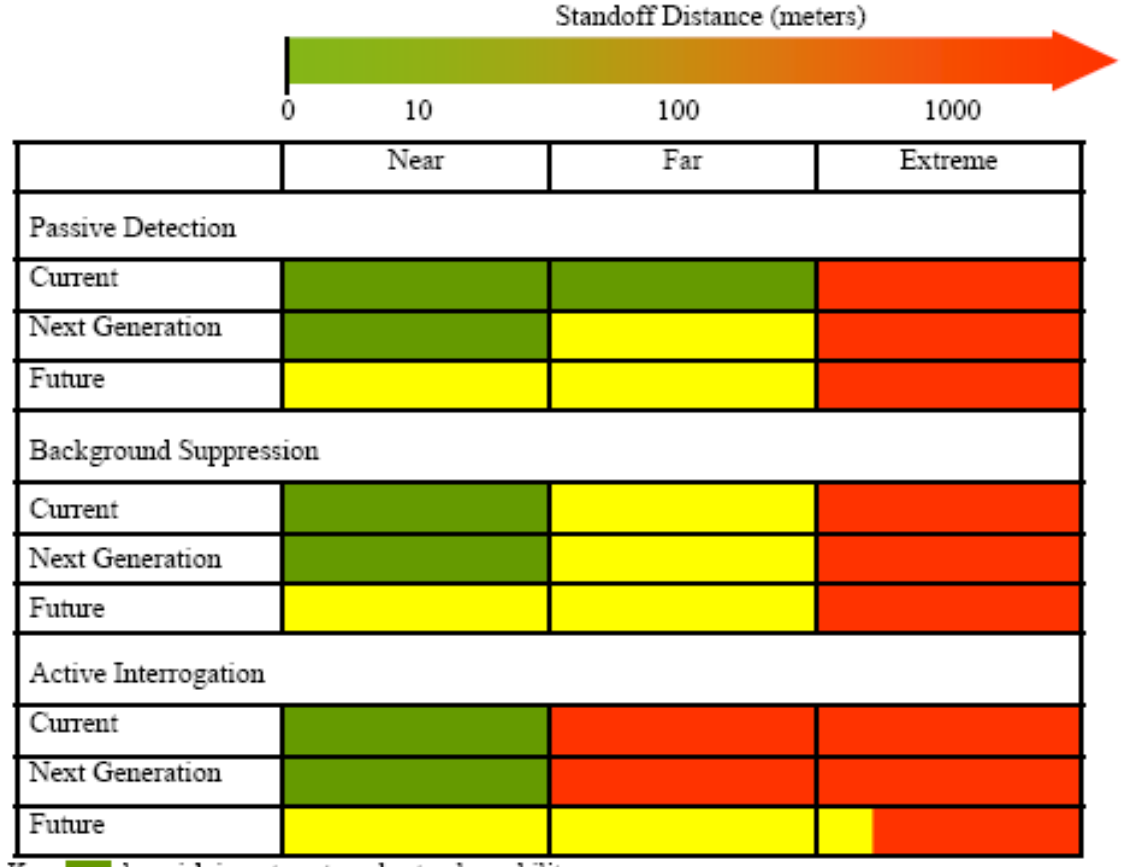
Medium Atomic Demolition Munitions (MADM) – Fully Assembled (left) and Unassembled (right). Assembled package weighs ~400 pounds – Yield = 1-15 kilotons ; according to http://en.wikipedia.org/wiki/Medium_Atomic_Demolition_Munition

- Decades-old nuclear warheads could weigh 150-400 pounds, including transportation container.
- Passive detectors can detect such unshielded devices at 10s-to-100s meters
  - Manhandling operations would be detectable if carried out near such detectors.
- Shielding to prevent detection would weigh many tons, reducing the transportation flexibility and possibly providing additional exploitable I&W signatures—particularly at transfer points where one person or a few people move from one shielded mode to another.
- Alternatively, if moved in a shielded configuration, cranes or other heavy moving equipment would be required at transfer points, such as docks from land to water transport.
- An effective CONOPS to counter smuggling of these devices is a necessary but not sufficient condition for countering shielded weapons in general—some weapons grade uranium devices are much more difficult to detect

August* Assessment of Detection Potential

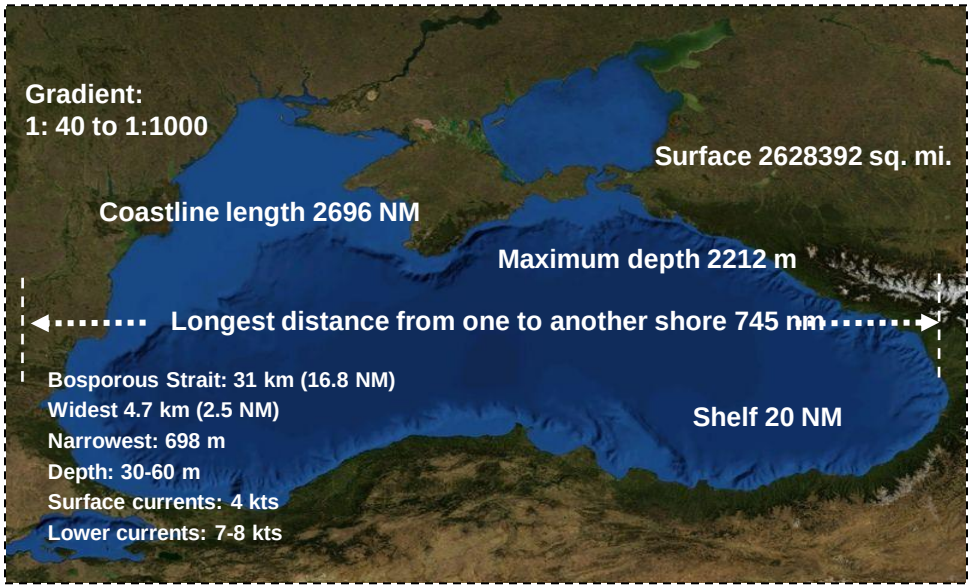
- **Near-term passive detector technology is capable of detecting and identifying unshielded RN sources at 10s to ~100 meters range**
- **Active interrogation technology for >10 meters range is a future possibility**
- **Nothing is likely to work at ranges of ~1000 meters**
- **A successful CONOPS requires a multi-layered "systems" approach that fuses data from a full complement of a variety of sensors—and an integrated responder community**

Table 2: Investment guide to SNM Detection Solutions vs Standoff Distance



*Robert A. August, "Technology Independent Metrics that Bound the SNM Detection Problem," Journal of Homeland Security, January, 2008; and available at: (http://www.homelandsecurity.org/newjournal/Articles/displayArticle2.asp?article=168).

Black Sea Wide-Area Search Challenge



- **Once on a large vessel, relatively easy to shield**
  - Numerous possible pathways to a large vessel
  - Black Sea "perimeter" is potential last line of defense
- **Brute Force countermeasure solutions not feasible**
  - Sufficient RN sensors for wide-area search impractical
    - Mobile/Transportable sensors, decoys and deception could have deterrent effect
  - Need fusion of sensors and all source information
- **Role for multiple regional information fusion centers**
  - Local responder participation required to provide I&W

- **Note: Large vessel on Don River near road and local marina**
- **~40 miles upstream from Sea of Azov**

- **Note: Dense traffic pattern**
- **~35 miles upstream from Sea of Azov, near Rostov**

Other Challenging Aspects of the Smuggling Threat

ARA Studies of Small Vessels Suggest:

- <20 meter recreational boat unlikely to carry shielded device
- But smaller fishing vessels might—and many regularly fish in the Atlantic
- Large yachts can go the whole distance in a shielded configuration—but they stand out

ARA Studies of Small Aircraft Suggest:

- Many airfields/landing strips
  - Near nuclear storage sites—including airports with direct flights to the U.S.
  - Near Black Sea coast

Warhead can be taken aboard an Al Qaeda-controlled break-bulk cargo ship, at sea away from main ports

Meeting the challenge requires integrated operations for Black Sea region Coast Guard—also for local Law Enforcement/Responders of the littoral states

- ***Possible US/NATO Surge Capabilities if/when their proximity permits***

Most Stressful Red Team Threat Scenario

- Three men imbedded in a “regular” process:
  - Colonel Ivan Petrovich, commander of nuclear weapons facility near Krasnoarmeyskoye, Russia—works through a “broker” to sell weapon to Terrorists
  - Lt. Vasily Yugov supervises the diversion of the weapon inside the facility and hands it off to
  - Sergeant Vukov, a veteran NCO who served in Afghanistan with Petrovich, who in turn commands the escort troops for a “regular” Scrap metal convoy to Novorossiysk
- Only Petrovich knows the “broker,” who arranges the deal with terrorists for money exchange for weapon in Novorossiysk
  - Petrovich, Yugov, and Vukov take their money and vanish
  - Terrorists transfer weapon to large vessel in Black Sea, shield it in 15 tons of water and head to a US port via the Turkish Straits
  - Possibly in the Aegean Sea in 12 hours after “go”

Typical Nuclear Weapon disassembly facility – e.g., Krasnoarmeyskoye, Russia

A typical break-bulk carrier can be loaded in port, along the coast or at sea

Scenario Key Players and Context

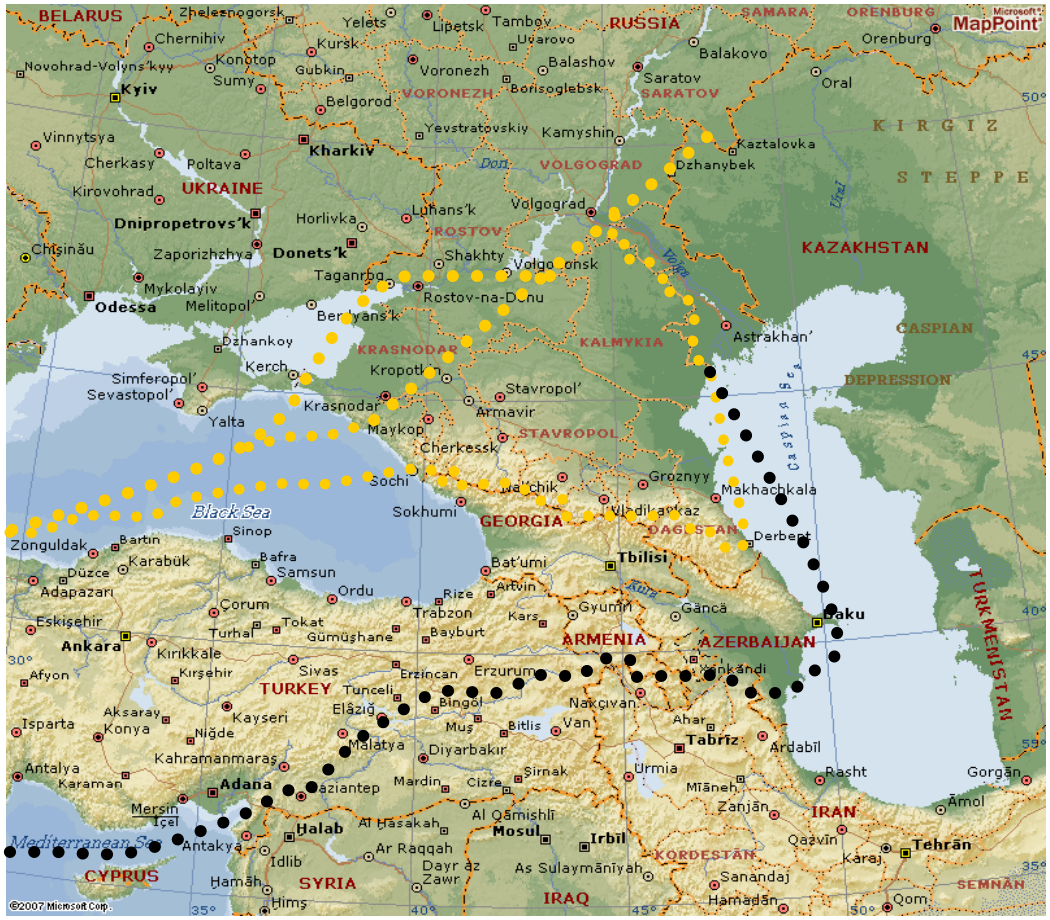
- **Suppliers/Sellers** – want to avoid detection, be paid and get lost ASAP
  - From among known (at least to Russians) insiders
- **Broker** -- wants to avoid detection, assure device works, be paid and get lost ASAP
  - Likely from among a knowable group engaged in smuggling
- **Buyers/Terrorists** – wants to assure device works and can be armed at will, and to avoid detection and interdiction before reaching the target
  - Likely from a known terrorist group
  - Will develop end-to-end detailed plans, including diversions, distractions and contingencies—**such activities probably will be exercised**
  - Will include at least one **true believer "nuclear expert"** on team to
    - Validate device is workable before paying broker or seller
    - Arm and detonate device if challenged en route
- **Key chokepoints other than geography**
  - Money: Exchange between Broker, Suppliers and Terrorists
  - Key People, e.g., nuclear weapons technologists
  - Other, e.g., key technology, components, etc.

Design countermeasures/CONOPS strategy to:

- ***Engage littoral "locals" to look for "tip-off" I&W signatures & empower "responders"***
  - ***Issue: How to look for key indicators that a scenario is being planned or is happening?***
- ***Couple to Black Sea maritime CONOPS—led by Turkey via Black Sea Harmony***

Considered Other Red Team Threat Scenarios

- **24-hour Direct to Port**
  - Money exchange in Port
  - Through Black Sea, Turkish Straits to Aegean
- **"Blend-in" thru Sea of Azov**
  - Change modes—Don River to & thru Sea of Azov—days to a week
  - Money exchange when boarding ship
- **"Blend-in" via Volga River to Caspian & across Caucuses**
  - Days to weeks
  - Money exchange on Volga or at Caspian coast
- **Around the Black Sea to the Mediterranean Sea**
  - Days to weeks
  - Numerous payout Opportunities



Numerous additional scenarios with various perturbations, e.g.

– Changes in transportation mode, including safe houses, aircraft and recreation/fishing vessels

– Suppliers sell to Chechens—with Moscow a plausible target

– HEU ingots smuggled to a foundry/machine shop where a "gun device" is built

Organize Counters to Exploit Central Agreements for Black Sea

		Turkey	Bulgaria	Romania	Ukraine	Russia	Georgia	Armenia	Azerbaijan	Key other members	U.S.
Black Sea	**OBSH** Operation Black Sea Harmony (2004)	✓		✓	✓	✓					
	PSI Proliferation Security Initiative (2003)	✓	✓	✓	✓	✓	✓	✓	✓	✓ Greece, Cyprus ✓	✓
Mediterranean	**GI** Global Initiative to Combat Nuclear Terrorism (2006)	✓	✓	✓	✓	✓	✓	✓		✓ Greece, Cyprus ✓	✓
	NATO North Atlantic Treaty Organization	✓	✓	✓	Member of Partnership for Peace	Member of Partnership for Peace	Member of Partnership for Peace	Member of Partnership for Peace	Member of Partnership for Peace	Greece ✓	✓

Give priority to working with Turkey, Russia, Ukraine and Romania as primary participants in Operation Black Sea Harmony

Effective Countermeasures depend on Cooperation of Littoral States

- Russia and Turkey are key
  - Growing Turkish interest in related maritime ops; a new opportunity!
  - But Russia backing away from Nunn-Lugar
- But involvement of all is essential
  - Sea of Azov threat scenarios are interesting OBSH challenges
    - Turkey, Russia, Ukraine & Romania are currently the only OBSH states
    - But what is role of Turkey and Romania in Sea of Azov?
    - And how does maritime response hand-off work into the Black Sea?
  - OBSH may simplify Black Sea operations, but. . .
    - How to deal with non-OBSH littoral states?
    - How to manage the OBSH/OAE hand-off at the Aegean?
- Strategy must fit technical/political possibilities

Integrated I&W/PolMil/Ops (including Coast Guard operations in the Black Sea—important diplomatic roles for the Global Initiative & PSI)

Such Considerations Lead to Emphasis on Requirements for Early Warning

- In principle, can exploit existing regional fusion centers to counter smuggling/terrorism
  - NATO Centers of Excellence
  - Regional Centers in Bucharest, Kiev and Almaty
- Key Challenges
  - Empowering Regional and Local Authorities
  - Open source information fusion tools to provide local authorities with timely nuclear smuggling I&W
  - Linked with effective detect, track and interdict technology and operations

The US can help, but the regional authorities must lead!

Facts are stubborn things; and whatever may be our wishes, our inclinations, or the dictates of our passion, they cannot alter the state of facts and evidence.

John Adams, *'Argument in Defense of the Soldiers in the Boston Massacre Trials,' December 1770*
US diplomat & politician (1735 - 1826)

- ***For the foreseeable future, radiation detectors will have limited range capability, even against unshielded nuclear sources—e.g., plutonium nuclear devices. Under the best of circumstances, passive detectors might be able to identify nuclear isotopes at 100 meters range. Active interrogation detectors at ranges greater than 10 meters is a possibility, but nothing is likely to be effective at a range of kilometer or more.***
- ***If an informed, competent terrorist cell can obtain a nuclear device, it can rapidly move it from the source region to a shielded condition on a ship destined for transport to attack nearby or far away cities with little likelihood of detection and/or interdiction.***

Therefore:

- ***An effective CONOPS will require a multi-layered "systems approach" that integrates information from a full complement of a variety of sensors with observations by the indigenous population who recognize suspicious activities and inform local authorities.***
- ***The key challenge is to lock down nuclear weapons in their storage sites and to enable local authorities to recognize suspicious behavior sufficiently early to enable operations to counter any attempt to circumvent these lockdown conditions.***
- ***These conditions should be developed and regularly exercised to help deter the threat and/or enable an effective response should deterrence fail.***

Architectural Challenges in Countering Existential Terrorist Threats: Lessons from a decade of studying "Loose Nukes"

- Lessons from studying how to counter terrorist threat of smuggling a nuclear weapon to attack the US, drawn from:
  - Camp Lejeune Unconventional Nuclear Weapon Defense (UNWD) Test Bed Demonstration
    - Legacy being extended to protect other Marine Bases
  - DHS/HSARPA—DHS/DNDO Architecture Study
    - Bottom Line: Give priority to overseas defenses
  - DTRA Bosporus Study
    - Early ("left of go") Indications and Warning (I&W) is the key to success
- Key Bottom Lines:
  - Technology is important but there is no silver bullet
  - Bureaucratic Impedance is a big problem
  - Empowering Local Authorities is the key to success

Many of these same lessons and bottom lines expected also to apply for countering the existential Bioterrorism threat—also all too real

- Have not studied this problem in depth, but expect
  - Red-Blue-White Team threat analyses are key to understanding the threat and framing effective countermeasures
    - A few personnel, some with key technical skills, can pose a severe threat
    - Some believe more threatening than "loose nukes"
  - Early Indications and Warning information is key to an effective defense, which must be prepared for rapid response
    - Expensive exquisite point detection methods inadequate to counter wide area threat
    - Anticipate effective I&W will depend on proliferated information sources (including inexpensive sensors) coupled to rapid data fusion capabilities
    - Expect open source information fusion ability to support local authorities is very important in identifying potential threat long before it materializes

Without effective Indications and Warning, people dying in large numbers could be the first indication—possibly too late to avoid catastrophic consequences of bioterrorism that could overwhelm responders