Homeland Security

United States Coast Guard Risk Management Overview

LCDR David Cooper
CG-512: Office of Performance Management and Assessment
David.w.Cooper@uscg.mil
202-372-2588

U.S. COAST GUARD

“Because it is not feasible to secure our homeland against every conceivable threat, we have instituted risk management as the primary basis for policy and resource allocation decision making.”

» *- DHS Strategic Plan 2008-2013*

U.S. COAST GUARD

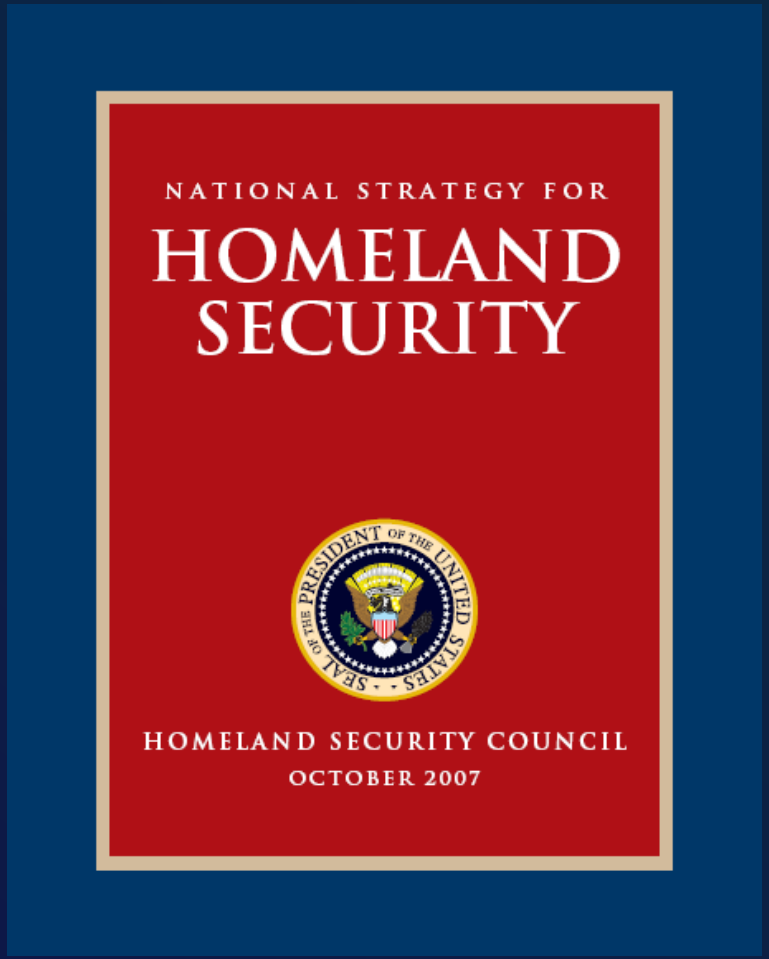
Secretary of Homeland Security

"Given the extensive number of vulnerabilities to manmade and natural disasters and the limitations on resources, determining national priorities and the judicious distribution of resources are a major element of the department's mission. What is the status of risk analysis metrics and what is the plan and time frame for setting up a full-blown system to govern the establishment of critical infrastructure programs, the priorities among national planning scenarios, and the distribution of grants to state, local, and tribal entities? More broadly, how can DHS enhance risk management as the basis of decision making?

Secretary Napolitano Issues First in a Series of Action Directives 21JAN09

National Strategy for Homeland Security

. . . We must apply a risk-based framework across all homeland security efforts in order to identify and assess potential hazards (including their downstream effects), determine what levels of relative risk are acceptable, and prioritize and allocate resources among all homeland security partners …



USCG & Risk Management

- A Principle of USCG Operations
- Challenging due to the multi-mission nature of the organization
- One criteria in USCG decision making
- Ultimately – an Integrated Performance Management System for Risk, Readiness & ROI

Basic Elements of Risk

Foundation for Risk Assessment		
• Historical experience	• Analytical methods	• Knowledge and intuition

Key Coast Guard Risk Efforts

- Maritime Security Risk Analysis Model (MSRAM): field level risk analysis tool to support terrorism risk management decisions at all levels; integrates national level threat with geo-specific vulnerability and consequence data.
- Ports, Waterways and Coastal Security (PWCS) Outcome measure: Built off MSRAM we utilize a simplified, scenario based, event tree model to calculate the expected risk reduction of CG operational, regime and domain awareness activities.
- National Maritime Strategic Risk Assessment (NMSRA): an all hazard / all mission risk assessment; shows the residual risk or the risk after Coast Guard intervention in the maritime domain.
- Risk Management Module: Builds a field level, all mission risk analysis tool based off the NMSRA to support operational planning, and risk management decisions.

Challenges:

- For terrorism profiles, we have a data-poor problem set with significant uncertainty of expected attack frequencies, and to some extent consequence.
- Heavy reliance on Subject Matter Expert judgment
- assessing public “risk tolerance”,
- accepted/equated values across consequence types and indirect or secondary impacts,
- geographic risk factors, including dealing with threat shifting and changes over time.
- Still a burgeoning field

Collaborative Efforts

- DHS Risk Management and Analysis (RMA) efforts
  - Homeland Security National Risk Assessment
- CREATE: Strong partnership to include:
  - Review of Coast Guard terrorism risk efforts
  - exchanging ideas and best practices
  - discussing and sharing methods, models, data, etc
- Leveraging CREATE strengths in
  - Risk analysis
  - Economic assessment, particularly calculation of indirect/secondary economic impact consequences
  - Resource allocation methodology

Questions?

- Back-up slides

Risk Assessment Phase

…is focused on defining the "problem"

FY11 Risk Assessment

- Strategic Risk
- Operational Risk
  - National Maritime Strategic Risk Assessment
- Mission Support Risk
- Institutional Risk

Risk Assessment Methodology

- **Name the undesirable incidents and scenarios within purview that cause public loss**
  - Statutes, Mandates, Roles and Missions
- **Scope**
  - Time horizon
- **Consequence Table**
- **Describe, for each incident the best way to estimate and represent the risk:**
  - Likelihood:
    - Threat * Vulnerability * Consequence
    - Frequency * Consequence
- **Assess the Risk**
  - Systematic approach based on the HAZOP analysis technique
  - Performed using a team of subject matter experts
  - Leverages historical incident information and applicable models/studies.

Incidents

- Grounding
- Collision/Allision
- Flooding/sinking
- Fire/explosion
- Personal injury/illness
- Oil spills
- Discharge of debris/sewage
- Release of HAZMAT
- Species damaged by marine operations
- Invasive species introduction
- U.S. EEZ encroachment
- Fish stock non-sustainability
- Drug smuggling
- Illegal migrant entry
- Seasonal conditions affecting waterways
- Interruption of military operations
- Periodic/expected natural disaster
- Non-maritime incident affecting a waterway
- Nation state attack
- Attack on Port Infrastructure
- Transfer of WMD
- Transfer of Terrorist

Example Maritime Accident

Grounding of a Container Ship that results in:

Property Damage
$15M of Damage to Ship and Cargo

Deaths / Injuries
1 Crew Member Killed

Environmental Impacts
5K Barrels of Fuel Oil Spilled

Risk assessment process estimates the national expected frequency that groundings of container ships result in impacts of each type and severity level

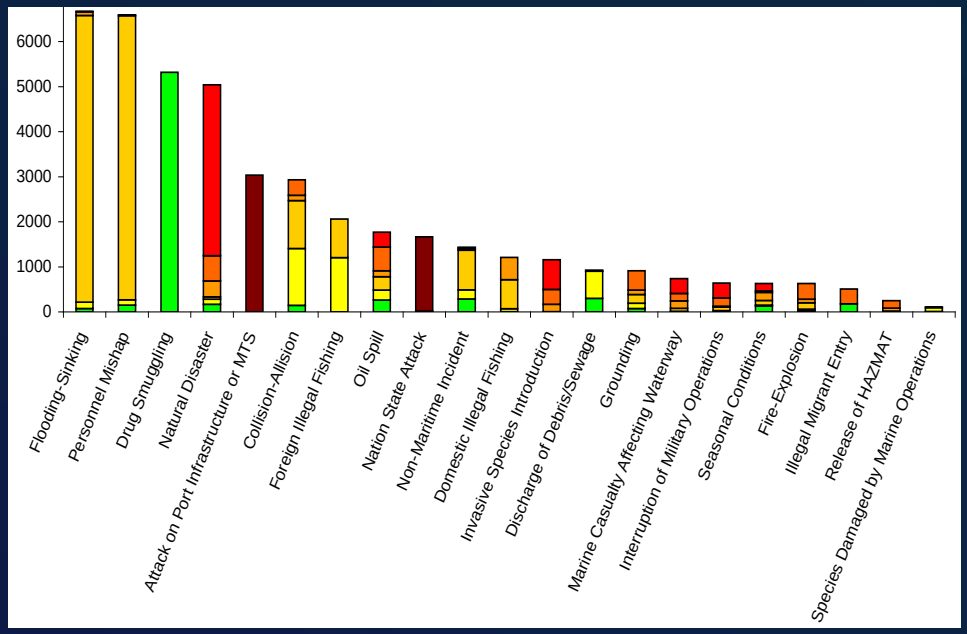
Process Overview

Expert judgment

Facilitated analysis of scenarios

Enterprise Data Sources

Method & Tool

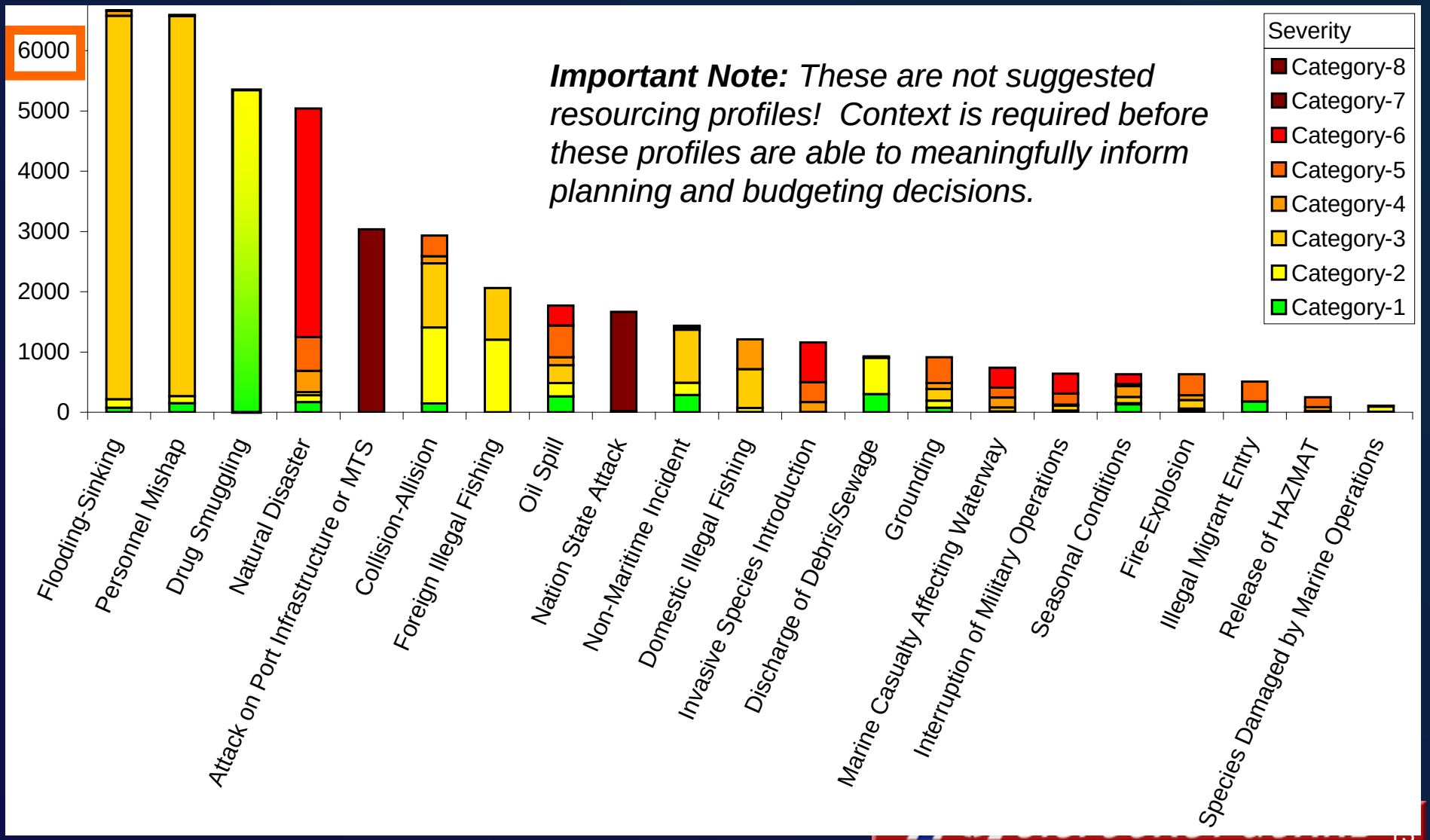


Risk Profiles

U.S. COAST GUARD

2006 Residual Risk Results

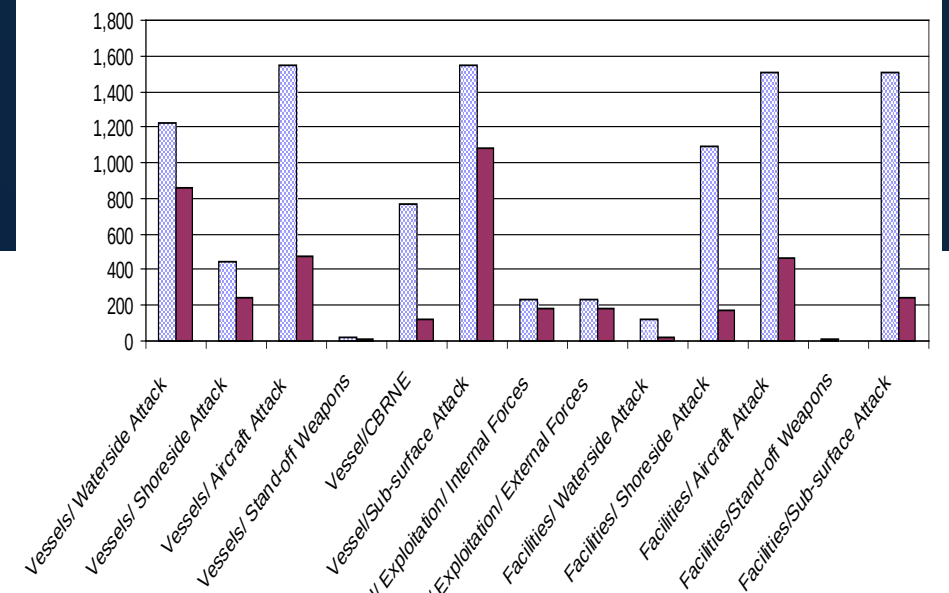
All incidents (excluding transfer of WMD or terrorists)



2006 Residual Risk Results

All incidents

Due to the highly uncertain nature of terrorism attacks, we conduct sensitivity analyses on the credible range of frequencies and consequences for these attacks.



From MSRAM

Uses of NMSRA Risk Information

- Strategic Planning Direction
- Commandant's budget intent
- Performance target setting process
- Operational effectiveness modeling
- Requirements development
- Mission analysis
- Resource Proposal development and evaluation
- Resource allocation

Maritime Security Risk Analysis Model

Objective

Create a field-level risk analysis tool to support risk management decisions at all levels

- Support tactical decisions at the field level by enabling users to consider the full spectrum of terrorist risks to assets within their AOR
- Support operational and strategic decisions by rolling up of field-level risk assessments to portray risk density of targets Sector, District, Area, HQ

How our PWCS / CMT Measure Works

1) Assessment of Risk - the 15 Scenarios that cause the most risk

- Transfer through the Maritime Domain of Terrorists
- Transfer through the Maritime Domain of WMD
- Waterside attack on Vessel
- Shoreside attack on Vessel
- Aircraft attack on Vessel
- Stand-off Weapons attack on Vessel
- CBRNE attack on Vessel
- Sub-surface Attack on Vessel
- Use of Vessel as Weapon - Exploitation by Internal Forces
- Use of Vessel as Weapon - Exploitation by External Forces
- Waterside attack on Facility
- Shoreside attack on Facility
- Aircraft attack on Facility
- Stand-off Weapons attack on a Facility
- Sub Surface attack on a Facility

Threat x **Vulnerability** x **Consequence** = **Risk the CG can Impact (we own)**

2) Assessment of Performance

Coast Guard T Reduction x **Coast Guard V Reduction** x **Coast Guard C Reduction** = **Risk the CG Reduced**

$$\frac{\text{Risk we Reduced}}{\text{Risk we can Impact (own)}} = \text{Our Annual Performance (\% Risk Reduction)} = \text{2007: 15\%} = \text{2008: 20\%}$$

U.S. COAST GUARD

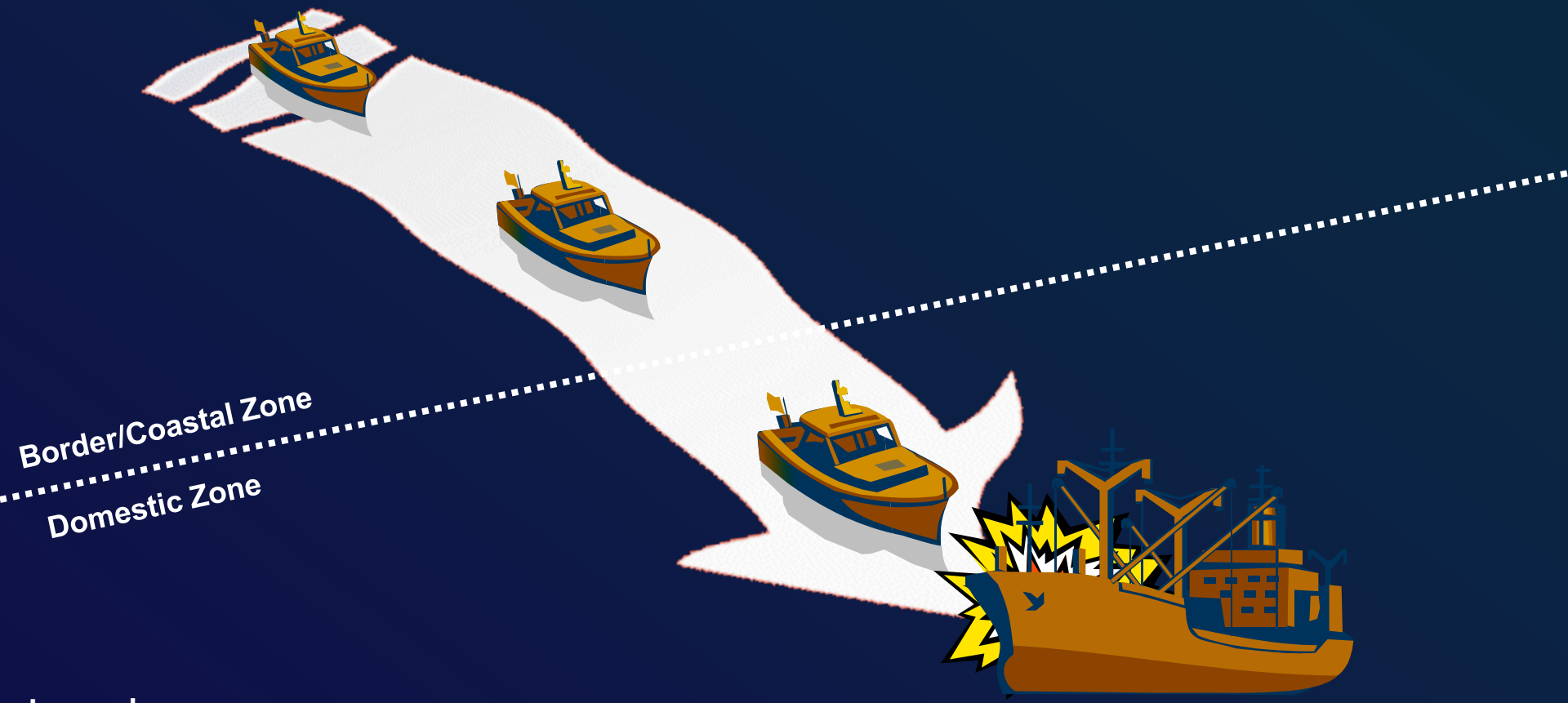
CMT Strategic Risk Model

A simplified, scenario-based, event tree model used in planning efforts to:

- Illustrate the layered security strategy that the USCG provides/could provide against each meta-scenario's continuum to prevent, protect, respond, and recover
- Define the roles of USCG activities and how they relate to one another (e.g., detection, intervention, support)
- Calculate the magnitude of risk that is being reduced by the layered security strategy
- Provide a mechanism for estimating the risk reduction importance of individual activities within the layered security strategy for a scenario
- Estimate the cost associated with performing each activity/groups of activities

Step 1 – Define the Scenario

Waterside attack on Vessel Scenario



Legend:

Prevention (Threat Reduction)
Protection (Vulnerability Reduction)
Response & Recovery (Consequence Reduction)

U.S. COAST GUARD

Step 2 – Identify USCG Interventions

Waterside attack on Vessel Scenario

Suspect Vessel Boarding 1

Specialized Use of Force 2

End Game Prosecution 3

Escort Vessel 4

Intervene After Attack - Response 5

Border/Coastal Zone

Domestic Zone

Legend:

Prevention (Threat Reduction)
Protection (Vulnerability Reduction)
Response & Recovery (Consequence Reduction)

U.S. COAST GUARD

Step 3 – Identify which interventions depend on external detection

Waterside attack on Vessel Scenario

Provides detection function to cue "dependent" activities

MDA/AIS

Intel

Suspect Vessel Boarding 1

Specialized Use of Force 2

End Game Prosecution 3

Escort Vessel 4

Intervene After Attack - Response 5

Border/Coastal Zone

Domestic Zone

Legend:

Prevention (Threat Reduction)
Protection (Vulnerability Reduction)
Response & Recovery (Consequence Reduction)

U.S. COAST GUARD

Step 4 – Estimate the probability that the activity fails to perform its role

Waterside attack on Vessel Scenario

93%

Provides detection function to cue "dependent" activities

MDA/AIS

Intel

Suspect Vessel Boarding 1

50%

Specialized Use of Force 2

18%

End Game Prosecution 3

5%

Escort Vessel 4

83%

Intervene After Attack - Response 5

93%

Border/Coastal Zone

Domestic Zone

Legend:

Prevention (Threat Reduction)
Protection (Vulnerability Reduction)
Response & Recovery (Consequence Reduction)

U.S. COAST GUARD

What types of activities were assessed?

- Probability that USCG activities successfully perform their role:
  - **Detection Activities (e.g., MDA)** Probability of successfully detecting, tracking, and communicating attack information to dependent activities
  - **Dependent Activities** Probability of successfully intervening given cuing by MDA
  - **Independent Activities** Probability of successfully detecting *and* intervening

Who assessed the various types of activities?

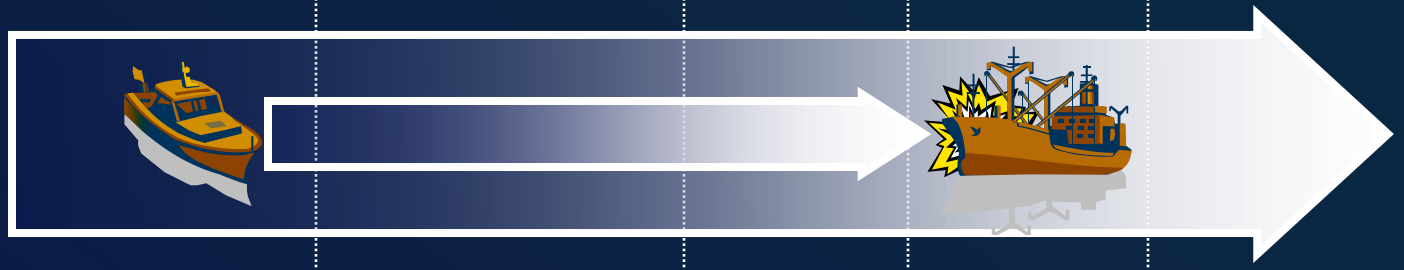
- **Detection Activities**
  - **MDA** - Asked MDA team to assess the capability and capacity of MDA to detect, track, and communicate attack information
  - **Tactical Surveillance** - Asked group of operations SMEs to assess the capability of surveillance assets to track underway attacks
  - **Intelligence** – CMT team assumed a range of probabilities (5% to 25%) for outside intelligence cuing of an attack
- **Dependent Activities**
  - **Capability** - Asked group of operations SMEs to assess the capability of the activity to successfully intervene if “on the target”
  - **Capacity** – CMT team performed modeling to determine probability of getting the activity “on the target”
- **Independent Activities**
  - **Capability** - Asked group of operations and regime SMEs to assess the capability of the activity to detect that an attack is underway and successfully intervene if “on the target”
  - **Capacity** – CMT team performed modeling to determine probability of getting the activity “on the target”

How did they assess the activities?

- **Highly Effective (HE)** - 90-100%
- **Effective (E)** - 75-90%
- **Substantial (S)** - 25-75%
- **Limited (L)** - 10-25%
- **Very Limited (VL)** - 5-10%
- **Measurable (M)** - 1-5%
- **Not Measurable (NM)** - <1%

Step 5 – Calculate the risk impact of USCG interventions

Threat | Vulnerability | Consequence



Raw Risk 700 RIN * **Line of Assurance Failure Probabilities** 96% * 94% * 93% * 83% * 93% = **Residual Risk** 448 RIN

Targets directly protected by USCG activities

1. Suspect Vessel Boarding*
2. Specialized Use of Force*
3. End Game Prosecution*
4. Escort Vessel
5. Intervene After Attack - Response

700-448 = 252 RIN

300-233 = 67 RIN

319 RIN

Risk Reduction

32%

Raw Risk 300 RIN * **Line of Assurance Failure Probabilities** 96% * 94% * 93% * 93% = **Residual Risk** 233 RIN

Targets not directly protected by USCG activities

1. 2. 3. 5.

*Lines of Assurance dependent on external detection activities (e.g., MDA)

U.S. COAST GUARD