Maritime Security: Potential Terrorist Attacks and Protection Priorities

(name redacted)
Specialist in Energy and Infrastructure Policy

(name redacted)
Specialist in Transportation Policy

May 14, 2007

Congressional Research Service
7-....
www.crs.gov
RL33787

Summary

A key challenge for U.S. policy makers is prioritizing the nation's maritime security activities among a virtually unlimited number of potential attack scenarios. While individual scenarios have distinct features, they may be characterized along five common dimensions: perpetrators, objectives, locations, targets, and tactics. In many cases, such scenarios have been identified as part of security preparedness exercises, security assessments, security grant administration, and policy debate. There are far more potential attack scenarios than likely ones, and far more than could be meaningfully addressed with limited counter-terrorism resources.

There are a number of logical approaches to prioritizing maritime security activities. One approach is to emphasize diversity, devoting available counter-terrorism resources to a broadly representative sample of credible scenarios. Another approach is to focus counter-terrorism resources on only the scenarios of greatest concern based on overall risk, potential consequence, likelihood, or related metrics. U.S. maritime security agencies appear to have followed policies consistent with one or the other of these approaches in federally-supported port security exercises and grant programs. Legislators often appear to focus attention on a small number of potentially catastrophic scenarios.

Clear perspectives on the nature and likelihood of specific types of maritime terrorist attacks are essential for prioritizing the nation's maritime anti-terrorism activities. In practice, however, there has been considerable public debate about the likelihood of scenarios frequently given high priority by federal policy makers, such as nuclear or "dirty" bombs smuggled in shipping containers, liquefied natural gas (LNG) tanker attacks, and attacks on passenger ferries. Differing priorities set by port officials, grant officials, and legislators lead to differing allocations of port security resources and levels of protection against specific types of attacks. How they ultimately relate to one another under a national maritime security strategy remains to be seen.

Maritime terrorist threats to the United States are varied, and so are the nation's efforts to combat them. As oversight of the federal role in maritime security continues, Congress may raise questions concerning the relationship among the nation's various maritime security activities, and the implications of differing protection priorities among them. Improved gathering and sharing of maritime terrorism intelligence may enhance consistency of policy and increase efficient deployment of maritime security resources. In addition, Congress may assess how the various elements of U.S. maritime security fit together in the nation's overall strategy to protect the public from terrorist attacks.

Contents

Introduction 1
Characterizing Potential Maritime Terrorist Attacks 1
- Perpetrators 2
- Objectives 2
- Locations 4
- Targets 4
- Tactics 5
- Unlimited Scenarios 5

U.S. Maritime Security Activities 6
- Maritime Security Exercises 7
  - PortSTEP Scenarios 7
  - AMSTEP Scenarios 7
  - Asymmetric Warfare Initiative 8
  - Other U.S. Attack Scenarios 9
  - Overseas Exercises 9
  - Emphasizing Scenario Diversity 10
- DHS Port Security Grants 11
  - Emphasizing High Priority Scenarios 12

Likelihood of U.S. Maritime Terrorist Attacks 13
- The "Bomb in a Box" Scenario 13
  - Type of Bomb 13
  - Method of Delivery 16
- Liquefied Natural Gas (LNG) Tanker Attacks 17
- Passenger Ferry Attacks 18
- Overall Likelihood of Maritime Terrorism 19

Policy Issues for Congress 21
- Consistency of Terrorism Scenario Assessment 21
- Intelligence Gathering 22
- Responding to New Intelligence 22

Conclusion 23

Tables

Table 1. Example Maritime Attack Characteristics 6

Contacts

Author Contact Information 23

Introduction

Maritime security is a principal protective element of United States' global war on terrorism. The Bush Administrations' *National Strategy for Maritime Security* states that "the infrastructure and systems that span the maritime domain ... have increasingly become both targets of and potential conveyances for dangerous and illicit activities."[1] Widely reported maritime attacks against the United States and its allies, such as the bombings of the U.S.S. *Cole* in 2000 and the French oil tanker *Limburg* in 2002, have focused Congressional attention on maritime threats.[2] In 2006, debate over the failed attempt by Dubai Ports World to operate marine terminals at some U.S. ports raised additional Congressional concerns about U.S. maritime security activities.[3] Questions have emerged regarding both the nation's overall strategy for maritime security and its level of commitment to specific components of that strategy.

As debate about U.S. maritime security continues, policy makers seek a better understanding of the nature and likelihood of potential terrorist attacks against the United States, and how federal programs prioritize their efforts to prevent such attacks. This report outlines the key dimensions of maritime terrorism and how these dimensions may characterize specific attacks in the global maritime domain. The report illustrates credible maritime attack scenarios based on actual past attacks or potential attacks developed for maritime security exercises or other U.S. counter terrorism activities. It discusses the challenge to maritime security planners of facing a virtually unlimited number of potential attack scenarios and how certain federal programs address this challenge. It also reviews various perspectives on the overall likelihood of maritime terror attacks on the United States. Finally the report discusses implications for homeland security policy.[4]

Characterizing Potential Maritime Terrorist Attacks

Maritime terrorism encompasses a wide range of potential attack scenarios. While individual scenarios have distinct features, for purposes of this report they may be characterized along five common dimensions: perpetrators, objectives, locations, targets, and tactics. These dimensions are useful for discussing both historical instances of maritime terrorism and potential scenarios for future maritime attacks.

[1] U.S. Dept. of Homeland Security (DHS) and U.S. Dept. of Defense (DOD). *The National Strategy for Maritime Security*. September 2005. p. 2.

[2] "Ships as Terrorist Targets." *American Shipper*. November, 2002. p. 59; The *Limburg*, under French registry, was attacked on October 6, 2002 in the Gulf of Aden while carrying approximately 400,000 barrels of crude oil from Iran to Malaysia.

[3] For more information see CRS Report RL33383, *Terminal Operators and Their Role in U.S. Port and Maritime Security*, by (name redacted) and (name redacted).

[4] Information in this report is based solely on publicly available information. In this report, attacks on the United States are broadly defined to include attacks on U.S. maritime assets (globally), military allies, and commercial partners if motivated by their relationship with the United States.

Perpetrators

Identifying potential perpetrators is important in evaluating maritime attacks because perpetrator capabilities vary widely and, therefore, bear on the types of attacks they might attempt. Disgruntled shipping workers, for example, may exploit privileged port access to circumvent security safeguards and mount an "insider" attack on maritime infrastructure. An Al Qaeda cell, on the other hand, may mount an entirely different type of attack on the same type of infrastructure, exploiting sophisticated training in terrorist tactics and privileged access to weapons and explosives, especially overseas. Although many terrorist groups may pose a credible threat to the United States, not all may pose a *maritime* threat.

Al Qaeda and its affiliates have been a primary focus of U.S. maritime security policy given the terror network's hostility to U.S. interests and its record of past attacks. Al Qaeda or its operatives, for example, appear to have been responsible for both the *Cole* and *Limburg* bombings.[5] Likewise the Abu Sayyaf Group, Islamist separatists based in the Philippines and tied to Al Qaeda, appears to have been behind the bombing of the Philippine vessel *Superferry 14* in 2004.[6] Groups or individuals not necessarily affiliated with Al Qaeda may also attack the United States, however. It is noteworthy that the only sustained international terrorist campaign in U.S. waters over the last 40 years was carried out by anti-Castro Cuban groups between 1968 and 1976.[7] Independent Islamist terrorist cells may also emerge as Al Qaeda is disrupted or disaggregated by the U.S. war on terror. According to a State Department review of Al Qaeda activity in 2005, "what was once a relatively structured network appeared to be a more diffuse worldwide movement of like-minded individuals and small groups, sharing grievances and objectives, but not necessarily organized formally."[8] Given this evolution among terrorist groups, maritime terrorism scenarios increasingly require consideration of a broad spectrum of potential perpetrators.

Objectives

Acts of maritime terrorism may have many objectives. They may seek to cause human casualties, economic losses, environmental damage, or other negative impacts, alone or in combination, of minor or major consequence.[9] If human casualties are the principal objective, passenger vessels such as cruise ships and ferries, which together account for less than 4% of U.S. commercial vessel inventory, may be more attractive terrorist targets than cargo and other vessels.[10] Consistent with this reasoning, federal agencies reportedly concluded in 2004 that the Washington

[5] National Memorial Institute for the Prevention of Terrorism (MIPT). Terrorism Incident Database. Incident profiles. July 20, 2006. http://www.tkb.org/Home.jsp.

[6] Council on Foreign Relations. "Backgrounder: Abu Sayyaf Group." November 2005. http://www.cfr.org/publication/9235/.

[7] MIPT. July 20, 2006.

[8] U.S. Dept. of State. *Country Reports on Terrorism.* p. 13. April 28, 2006.

[9] For further discussion, see Enders, Walter and Sandler, Todd. *The Political Economy of Terrorism.* Cambridge University Press. Chap. 1. November 2005; Lutz, James M. and Lutz, Brenda J. "Terrorism as Economic Warfare." *Global Economy Journal*. Vol. 6. No. 2. 2006; U.S. Army, Training and Doctrine Command. *A Military Guide to Terrorism in the Twenty-First Century*. October 12, 2004. pp. 6.3-6.5.

[10] U.S. Army Corps of Engineers. *Waterborne Transportation Lines of the United States, Calendar Year 2004, Volume 1 – National Summaries*. Tab. 4 and Fig. 14. December 15, 2005.

state ferry system had been under surveillance as a possible terrorism target.[11] A weapon of mass destruction (WMD) attack on a heavily populated U.S. port could inflict the greatest number of human casualties. The Defense Department's Joint Task Force–Civil Support developed such a scenario in a 2005 exercise involving the smuggling and detonation of a 10-kiloton nuclear device in the port of Charleston, SC.[12]

If economic loss is the primary objective, terrorists may seek to carry out different types of attacks, with potentially few human casualties but significant impacts to critical infrastructure or commerce. The *Limburg* bombing may have been an attack of this type, threatening to disrupt the global oil trade and causing considerable consternation among tanker operators.[13] Although the bombing killed only one member of the *Limburg's* crew, it caused insurance rates among Yemeni shippers to rise 300% and reduced Yemeni port shipping volumes by 50% in the month after the attack.[14] The bombing also caused significant environmental damage, spilling 90,000 barrels of oil into the Gulf of Aden.[15] Other types of maritime attacks could disrupt more directly the shipping operations of key commercial ports. For example, in a 2005 Department of Homeland Security (DHS) exercise, terrorists hypothetically destroyed the International Bridge in Sault Ste. Marie, MI, blocking the shipping channel below with debris, by exploding a fuel tanker truck on the bridge.[16]

The potential consequences of a terror attack are also an important consideration in evaluating terrorist objectives. Terrorists groups such as Al Qaeda appear to choose the scale (and timing) of their attacks in order to maximize media coverage, and hence, public awareness and psychological impact. As one academic study concluded,

> To make it into the news, terrorists operating in Western countries can commit some minor terror incident with few fatalities, whereas terrorists in developing countries need to "produce" a lot of blood to attract the attention of Western media.[17]

Accordingly, attack scenarios must consider consequences, and how such consequences would align with the objectives of potential perpetrators. The study cited above suggests that terrorists attacking the United States may achieve their media objectives even with relatively minor attacks.

[11] Carter, Mike. "Why Feds Believe Terrorists are Probing Ferry System." *Seattle Times*. October 12, 2004.

[12] Hodges, James. "An Exercise in Disaster: Preparing for the Worst" *Daily Press*. Newport News, VA. August 19, 2005.

[13] Vieth, Warren. "Owners of Oil Tankers Jittery." *Los Angeles Times*. November 25, 2003. p. 1.

[14] U.S. Dept. of State. "Yemen's Economy Suffering Due to October Terrorist Attack." November 8, 2002. http://usinfo.state.gov/is/Archive/2004/Apr/01-745388.html.

[15] Hendawi, Hamza. "Yemen Acknowledges Terror Attack." Associated Press. October 17, 2002.

[16] Purvis, Michael. "Bridge Out: Forces Plan for Terrorist Attack." *Sault Star*. Sault Sainte Marie, Ontario. May 4, 2005.

[17] Frey, Bruno S. and Rohner, Dominik. "Blood and Ink! The Common-Interest-Game Between Terrorists and the Media." Center for Research in Economics, Management, and the Arts. Basel, Switzerland. Working Paper No. 2006-8. p. 18

Locations

Where a potential maritime attack could occur is also essential to defining a terrorism scenario. Examples above have already illustrated that maritime attacks targeting U.S. interests may occur in U.S. ports (of which there are over 360)[18] or among the ports of the nation's 165 maritime trading partners.[19] Specific types of attacks, such as the smuggling of WMDs in ship-borne cargo containers, may involve both a foreign port of departure and a U.S. port of entry. Maritime terror attacks may also occur at sea in areas of concentrated shipping like the Straits of Gibraltar where, in 2002, Al-Qaeda operatives reportedly plotted to attack U.S. and British warships, and possibly commercial vessels.[20] The Straits of Malacca in southeast Asia is another location frequently identified by security analysts as a potential locus of maritime terrorism activity. In 2001, Jemaah Islamiyah terrorists reportedly had plans to attack U.S. navy vessels visiting the region.[21] The Organization for Economic Cooperation and Development (OECD) has identified nine similar shipping bottlenecks around the world where potential terrorist activities are a concern.[22]

Terrorist attacks in U.S. waters may have the greatest potential to injure U.S. citizens if they occur in populated areas. They may also have the greatest potential for economic impact in the event of the closure of a major U.S. port. Nonetheless, future attacks on U.S. interests in foreign ports, or on vessels at sea in transit to the United States, may be easier for terrorists to execute than attacks in U.S. waters.

Targets

Another key aspect of maritime terrorism scenarios is identifying potential targets. There are numerous possibilities, especially in and around ports. As a U.S. Government Accountability Office (GAO) analyst testified before Congress in 2006,

> Ports contain a number of specific facilities that could be targeted by terrorists, including military vessels and bases, cruise ships, passenger ferries, terminals, dams and locks, factories, office buildings, power plants, refineries, sports complexes, and other critical infrastructure.[23]

In addition to vessels and infrastructure, terrorists may seek to attack maritime communities using ships as delivery vehicles for WMDs or by exploiting chemicals or explosives in cargo ships or onshore storage tanks in populated port areas. The Homeland Security Council included terrorist attacks on ships carrying flammable and toxic chemical cargoes in a U.S. port among the hazard

[18] American Association of Port Authorities. "U.S. Public Port Facts." Internet page. Alexandria, VA. July 18, 2006. http://www.aapa-ports.org/Industry/content.cfm?ItemNumber=1032.

[19] U.S. Maritime Administration. "U.S. Waterborne Trade by Trading Partners, 1997-2005." Online database. July 18, 2006. http://www.iwr.usace.army.mil/ndc/usforeign/index.htm.

[20] Sawer, Patrick. "Terror Plot to Blow Up Navy Warships is Foiled." *The Evening Standard*. London. June 11, 2002. p.4.

[21] Raymond, Catherine Z. "The Threat of Maritime Terrorism in the Malacca Straits." *Terrorism Monitor*. Vol. 4 . No. 3. February 9, 2006. p. 8.

[22] Organization for Economic Cooperation and Development (OECD). *Security in Maritime Transport: Risk Factors and Economic Impact*. July 2003. p. 14.

[23] Caldwell, Stephen L., U.S. Government Accountability Office. Statement at the House Committee on Government Reform, Subcommittee on Government Management, Finance, and Accountability hearing on "Securing Our Ports: Information Sharing is Key to Effective Maritime Security." July 10, 2006.

scenarios it developed in 2004 as the basis for U.S. homeland security national preparedness standards.[24] Because the characteristics of infrastructure targets or human targets may be unique to any specific category of target (e.g., propane tankers) or community (e.g., Charleston), understanding how target characteristics relate to terrorist capabilities and objectives may offer valuable insights into the credibility of particular attack scenarios.

Tactics

Maritime security analysts have discussed numerous potential tactics for terrorist attacks on U.S. maritime targets. The following passage from the *National Strategy for Maritime Security* summarizes many of the tactics most commonly mentioned in maritime security discussions:

> Terrorists can also develop effective attack capabilities relatively quickly using ... explosives-laden suicide boats and light aircraft; merchant and cruise ships as kinetic weapons to ram another vessel, warship, port facility, or offshore platform; commercial vessels as launch platforms for missile attacks; underwater swimmers to infiltrate ports; and unmanned underwater explosive delivery vehicles. Mines are also an effective weapon.... Terrorists can also take advantage of a vessel's legitimate cargo, such as chemicals, petroleum, or liquefied natural gas, as the explosive component of an attack. Vessels can be used to transport powerful conventional explosives or WMD for detonation in a port or alongside an offshore facility.[25]

General tactics of maritime attacks like those above have been further described in security bulletins based on specific terrorism intelligence. For example, in 2004 the Federal Bureau of Investigation warned of possible improvised marine mines in "waterborne flotsam commonly seen around waterways" or attached to buoys.[26] More specific tactics have also been articulated as part of U.S. maritime security exercises discussed later in this report.

As the previous citations suggest, analysis of terrorist tactics must take into account the specifics of the attack in question. Some analysts believe that there is a "low probability" that terrorists would try to use a large ship as a weapon because of the complexity of doing so, but that attacks by small boats are more likely because they "satisfy the overwhelming terrorist requirement for simplicity."[27] Similarly, the Commandant of the U.S. Coast Guard (USCG) has reportedly stated that "there is a significant threat by vessel-borne improvised explosive devices" and that "vulnerability to small-boat attacks stood out" during a 2006 threat assessment.[28]

Unlimited Scenarios

The dimensions of maritime terrorism defined above may be used to characterize both historical terrorist attacks and potential future attacks against the United States. **Table 1** provides a set of illustrative characteristics which could serve as the basis for the development of potential attack scenarios.

---

[24] Homeland Security Council. *Planning Scenarios: Executive Summaries.* July 2004. p. 6-1.

[25] DHS and DOD. September 2005. p.4.

[26] "FBI Warns of Maritime Terror Threat." *The Journal of Commerce Online.* June 28, 2004.

[27] See for example: Murphy, Martin. "Maritime Terrorism: The Threat in Context," *Jane's Intelligence Review,* February 1, 2006.

[28] Dress, Caroline and Ang, Edgar. "U.S. at Risk from Boats Packed with Explosives." Reuters. June 1, 2006.

Table 1. Example Maritime Attack Characteristics

Dimensions	Example Characteristics	
Perpetrators	• Al Qaeda and affiliates • Islamist unaffiliated • Foreign nationalists	• Disgruntled employees • Others
Objectives	• Mass casualties • Port disruption	• Trade disruption • Environmental damage
Locations	• 360+ U.S. ports • 165 foreign trade partners	• 9 key shipping bottlenecks
Targets	• Military vessels • Cargo vessels • Fuel tankers • Ferries / cruise ships	• Port area populations • Ship channels • Port industrial plants • Offshore platforms
Tactics	• Explosives in suicide boats • Explosives in light aircraft • Ramming with vessels • Ship-launched missiles • Harbor mines	• Underwater swimmers • Unmanned submarine bombs • Exploding fuel tankers • Explosives in cargo ships • WMDs in cargo ships

Source: CRS.

What is apparent from **Table 1** is the possibility of generating numerous unique, logically consistent, and operationally credible attack scenarios based on different combinations of perpetrators, objectives, locations, targets, and tactics. Doing so exhaustively, however, leads to far more potential attack scenarios than likely ones, and far more than could be meaningfully addressed with limited counter-terrorism resources. As one security analyst has articulated the problem,

> An accurate assessment of the current nature and scope of the global maritime terrorist threat should be driven by an assessment of what is probable, rather than merely possible. However, sober analysis of this issue has been clouded amid the anxiety created by the current global security climate, with much discussion turning on the notion that terrorists could potentially strike any target with virtually any means available....[29]

A key challenge, therefore, for U.S. security analysts and policy makers is prioritizing the nation's maritime security activities among a virtually unlimited number of potential attack scenarios. How federal agencies have been addressing the "unlimited scenarios" problem is discussed in the following section.

U.S. Maritime Security Activities

A number of logical approaches to prioritizing maritime security activities exist given the unlimited number terrorism scenarios. One approach is to emphasize diversity, devoting available counter-terrorism resources to a broadly representative sample of credible scenarios. Another approach is to focus counter-terrorism resources on only the scenarios of greatest concern based on overall risk, potential consequence, likelihood, or related metrics. U.S. maritime security agencies appear to have followed policies consistent with one or the other of these approaches in

[29] Murphy, Martin. February 1, 2006.

federally-supported exercise and grant programs. These approaches lead to differing allocations of resources and levels of protection against specific types of attacks. How they ultimately relate to one another under a national maritime security strategy remains to be seen.

Maritime Security Exercises

The USCG, the U.S. Navy, and other federal agencies conduct ongoing port security training exercises domestically and overseas. Taken collectively, the terrorism scenarios in these exercises to date have spanned an extremely broad range of objectives, locations, targets, and tactics. Specific scenario characteristics are discussed below in the context of particular maritime security exercise programs.

PortSTEP Scenarios

In collaboration with the USCG, the Transportation Security Administration (TSA) has developed U.S. maritime terrorism scenarios under the agency's Port Security Training Exercises Program (PortSTEP).[30] PortSTEP fulfills the annual exercise requirements for Area Maritime Security Plans under the Maritime Transportation Security Act of 2002 (P.L. 107-295) through a combination of basic tabletop, advanced tabletop, and field exercises. The PortSTEP program began in 2005 and plans to complete exercises in 40 port areas by October 2007. According to the PortSTEP program office, the 25 exercises conducted through 2006 have involved chemical, biological, and radiological ("dirty bomb") attacks, as well as various kinds of explosives and improvised explosive devices. The scenarios have targeted or exploited cruise ships, container ships, a harbor truck, a barge, a rail yard, port industrial facilities, bridges, and a national landmark. Because the TSA is responsible for the security of all major surface transportation modes, it is a specific goal of the PortSTEP program to incorporate surface transportation modes such as rail and trucking into its maritime security exercises. While the list of ports in PortSTEP includes many of the largest U.S. ports, it covers a broad cross-section in terms of size and geography, including Buffalo, NY, Chicago, IL, Corpus Christi, TX, Juneau, AK, Long Beach, CA, Pittsburgh, PA, and Tampa, FL.[31]

AMSTEP Scenarios

The USCG has developed additional U.S. maritime terrorism scenarios under its Area Maritime Security Training and Exercise Program (AMSTEP), initiated in October 2005. Like the PortSTEP program, AMSTEP conducts tabletop and field exercises to fulfill annual exercise requirements for Area Maritime Security Plans under P.L. 107-295. AMSTEP differs from PortSTEP in that it emphasizes surface transportation modes less deliberately in its terrorism scenarios. The program plans to conduct up to 28 exercises through FY2007, specifically in ports not covered by the PortSTEP program. The AMSTEP program office states that its exercises are designed around Area Maritime Security Committee objectives in individual ports; there are no

[30] For more information on PortSTEP, see the TSA's program brief, an electronic copy of which is available at http://www.tsa.gov/interweb/assetlibrary/program_brief.pdf.

[31] Transportation Security Administration (TSA), PortSTEP program office. Personal communication. December 20, 2006 and "PortSTEP Program Initiated." Press release. August 18, 2005; Daniel, Mac. "Terror Preparedness Put to Test." *Boston Globe*. September 20, 2005.

requirements to conduct exercises under any specific scenario.[32] According to the limited public information available, the program's exercise scenarios in 2006 involved terrorist stowaways on an inbound hazardous cargo vessel, an explosion at a jet fuel receiving terminal, a suspicious package at a port facility, surveillance of petrochemical terminals, a potential improvised explosive device (IED) attached to the hull of a freighter, theft of gasoline tanker truck, and explosion aboard an oil tanker in a shipping channel, among others.[33] The USCG has conducted AMSTEP exercises in port areas including Key West, FL; Duluth, MN; Long Island, NY; Charleston, SC; Corpus Christi, TX; Houston/Galveston, TX; and Washington, DC, among others.[34]

Asymmetric Warfare Initiative

Port security exercises have also been conducted jointly by the U.S. Navy, USCG, FBI, local law enforcement, and other agencies under the federally sponsored Asymmetric Warfare Initiative (AWI). The AWI exercises, carried out annually since 2003, have reportedly included the following terrorist attacks scenarios:

- Explosives attack on a chlorine storage tank in port
- Hostage-taking and executions aboard a vessel in port
- A marine mine attack on a Navy frigate in port
- Underwater explosive devices planted on multiple vessels in port
- A nuclear device aboard an incoming vessel in a 55-gallon drum
- Attack on a port with a biological disease agent[35]
- Detonation of a "dirty" bomb in a shipping container in port[36]
- Aircraft attack on a passenger ferry or cruise ship
- Ammonium nitrate bombs shipped by rail to a port[37]
- Sarin gas attack on a cruise ship in port[38]

The AWI has held its exercises in Port Hueneme, CA, Los Angeles, CA, San Diego, CA, and the Puget Sound, WA, and Hampton Roads, VA areas.

---

[32] U.S. Coast Guard, Area Maritime Security Training and Exercise Program (AMSTEP) Program Office. Personal communication. January 4, 2007.

[33] Tully, Tasha, U.S. Coast Guard, 7th District. "Tampa Bay Agencies Test Security Plans." *Coastline*. https://www.piersystem.com/go/doc/586/136318; Karl, Richard C., Director.

Superfund Division, U.S. Environmental Protection Agency, Region 5. "Reports of Significant Developments and Activities Ending on September 8, 2006." Memorandum. September 18, 2006. http://www.epa.gov/region5superfund/significant_actions/2006/060908.pdf.

[34] Hanewich, Steve, Cpt., U.S. Coast Guard. "Coast Guard Plan of Action and Milestones: Natural Disaster Preparedness 2006." Slide presentation. December 20, 2006. p. 15. http://www.scaa-spill.org/events/ppt/hurricane_prep_briefhanewich.ppt.

[35] Chawkins, Steve. "Agencies Get a Taste of Terrorism in Action." *Los Angeles Times*. November 6, 2003.

[36] O'Sullivan, Mike. "Five-Day Exercise Simulates Coordinated Terror Attacks." *Voice of America*. August 5, 2004.

[37] Shukovsky, Paul. "Terrorism Simulation Exercises Set Today." *Seattle Post-Intelligencer*. May 23, 2006.

[38] Shear, Michael D. "Va. Terror Drills Set Up Worst-Case Scenarios." *Washington Post*. p. B01. August 3, 2004.

Other U.S. Attack Scenarios

In addition to the scenarios listed above, the USCG, the U.S. Navy, other government agencies, and security analysts have reportedly developed attack scenarios as part of other maritime security exercises or planning activities. These scenarios have included:

- Various types of an explosives attack on a ship in port[39]
- "Dirty" bombs in cargo containers at multiple U.S. ports[40]
- Radioactive materials carried on a cargo ship 90 miles offshore[41]
- Underwater and fishing boat explosives attacks on a riverboat[42]
- Bombing and sinking of a liquefied propane gas (LPG) tanker in a major commercial and naval shipping channel[43]
- Hijacking of a river tanker for use as a "floating bomb"[44]
- Ramming and "dirty" bombing a ferry with a hijacked cargo ship[45]
- Coordinated bombing of docks and bridges, and mining of the harbor at a major commercial port[46]
- Attack on a liquefied natural gas (LNG) terminal and tanker in port[47]

Again, although these exercises may have been conducted independently of one another, they encompass a broad range of potential attack scenarios.

Overseas Exercises

Apart from exercises in U.S. territorial waters, the U.S. Navy, USCG, and other federal agencies participate in maritime security exercises overseas, often in cooperation with other countries. For example, in 2006, the U.S. Navy and USCG joined with the Thai Navy and other international participants in simulating the hijacking of a vessel with military cargo in the Strait of Malacca.[48] In 2006, the U.S. Navy also participated in a multi-national maritime exercise involving the

[39] California Maritime Academy. "'Terrorists' Attack Training Ship *Golden Bear*." Press release. October 29, 2004.

[40] Booz Allen Hamilton. *Port Security War Game: Implications for U.S. Supply Chains.* 2003.

[41] Dorsey, Jack. "Coast Guard, Navy, FBI to Team up for Security Exercise." *Virginian-Pilot.* June 12, 2006; U.S. Coast Guard (USCG). "Coast Guard Atlantic Area, Navy Second Fleet, FBI Participate in Maritime Homeland Security Exercise." Press release. June 12, 2006.

[42] Nelson, Tim. "Is That a Speargun, or Are You Just Glad to See Me?" *City Hall Scoop.* Internet blog. July 22, 2005. http://blogs.twincities.com/city_hall_scoop/2005/07.

[43] Pinto, C. Ariel. and Talley, Wayne K. "The Security Incident Cycle of Ports." Old Dominion Univ., Maritime Institute. Working paper. Norfolk, VA. July 2006.

[44] Purvis, Michael. May 4, 2005.

[45] Pyle, Richard. "Agencies Analyze Responses to Nightmare Scenario at U.S. Ports." Associated Press. June 7, 2006.

[46] Fuentes, Gidget. "Training Drills Test Threat Response at California Ports." *Navy Times*. June 13, 2005.

[47] Daniel, Mac. "Drill Will be Gauge of Terror Readiness." *Boston Globe.* August 29, 2006.

[48] Baxter, Edward. "Thai Forces Board Button in Maritime Security Exercise." U.S. Military Sealift Command. Press release. May 22, 2006.

hypothetical placement of sea mines by terrorists in coastal waters of the South China Sea.[49] In 2003, the U.S., Japanese, Australian, and French Navies conducted an exercise involving the seizure of illegal WMD-related cargo aboard a commercial vessel in the Coral Sea.[50] These are only three illustrations of what appear to be numerous maritime counter-terrorism exercises carried out by U.S. agencies around the world over the past five years.

Emphasizing Scenario Diversity

Based on the scenario summaries above, it appears that the USCG, the U.S. Navy, and other agencies have structured their maritime terrorism exercises in a manner that addresses diverse terrorism scenarios across many ports. Given that the PortSTEP, AMSTEP, and AWI programs, in particular, are geared toward training and evaluation, there are logical reasons they would employ such diverse scenarios. The PortSTEP program, for example, states that its exercises "are scaled and tailored to each specific port's needs" based on the recommendations of individual Area Maritime Security Committees.[51] Since many aspects of terrorism prevention and response (e.g., communications) are common to a range of attack scenarios in a given port area, the choice of one scenario or another may reveal similar things about security plan performance. Scenario diversity also maximizes the operational and geographical experience among senior U.S. agency planners in an environment of great uncertainty about future maritime terror attacks. Emergency responders may therefore be more likely to have at least some level of preparedness for any kind of maritime attack, anywhere.

Terrorism scenario diversity is also relatively simple, with a limited need for complex and time consuming risk assessments to establish scenario priorities. The only key requirement common to all of the aforementioned scenarios appears to be credibility, or, as stated in USCG port security guidelines, that they be "within the realm of possibility and, at a minimum, address known capabilities and intents as evidenced by past events and available intelligence."[52] It may be sufficient, therefore, that scenarios are credible and meet the particular needs of local port security officials, not that they are demonstrably more or less critical than one another.[53] The principal disadvantage of a diverse scenarios approach is that it may devote too many security resources to relatively unlikely scenarios and not enough to more likely ones. An alternative approach, for example, might be to conduct repeated exercises involving only a few high-consequence scenarios (e.g., container WMDs) and only in the largest or most populous U.S. ports.

[49] "Navy Takes in Pacific Exercise." Associated Press. June 07, 2006.

[50] "Anti-Weapons Marine Exercise to Target 'Japanese' Vessel." Agence France-Presse. September 09, 2003.

[51] Transportation Security Admin. (TSA). "PortSTEP: Mission and Goals." August 1, 2006. http://www.tsa.gov/what_we_do/layers/portstep/editorial_with_table_0060.shtm.

[52] U.S. Coast Guard (USCG). "Guidelines for Port Security Committees, and Port Security Plans Required for U.S. Ports." Navigation and Vessel Inspection Circular No. 902. September 30, 2002. p.13.

[53] According to a PortSTEP official, the USCG did rank U.S. ports based on risk, but the selection of ports for the program was based on broader criteria, including port diversity.

DHS Port Security Grants

The Department of Homeland Security (DHS) initiated its Port Security Grant Program (PSGP) in 2002 to provide competitive security enhancement grants to U.S. ports. The PSGP awarded approximately $870 million in port security grants by the end of 2006.[54]

The first four rounds of PSGP grants appear to have been awarded in a manner consistent with the "broad scenarios" approach described above. For example, the DHS awarded round two grants to over 125 U.S. port areas ranging from major ports such as Baltimore, MD, Houston, TX, and Long Beach, CA, to relatively minor ones, such as Christiansted, VI, Fernandina Beach, FL, and Homer, AK. These awards also appear to have been granted for protection of a wide range of potential terrorist targets, including container terminals, rail yards, sightseeing vessels, ferries, chemical plants, energy facilities, and port operations.[55] Consistent with this conclusion, a 2005 review of the PSGP by the DHS Inspector General determined, among other findings, that "the evaluation and selection process focused on awarding funds to as many applicants as possible."[56] According to the report, this focus was influenced by tension between the "fair and equitable" award criteria mandated under the MTSA and the competitive criteria mandated under TSA appropriations. The report also noted, that PSGP awards were not based on a national risk assessment because a mechanism to perform such an assessment did not yet exist within TSA.[57]

In 2005, the DHS began to award PSGP grants on a more selective basis as determined by the agency's new national assessment and ranking of port risk. For its fifth round in 2005, the DHS evaluated the 129 largest U.S. ports using a risk-based formula to identify 66 ports eligible to apply for the grants. DHS subject matter experts further reviewed and prioritized grant applications within this pool of eligible ports based on specific risk scenario, among other factors. Note that the PSGP round five grant application materials state that the program

> places a strong emphasis on prevention and detection relative to improvised explosive devices (IEDs), as well as chemical, biological, radiological, and nuclear devices.... Of great concern to port security are IEDs delivered via small craft, underwater and in vehicles on ferries. Areas of focus for grantees should include protection of facilities such as public cruise lines, ferry terminals, and vessels from tampering and attack.[58]

PSGP round five awards were granted to 36 ports, predominantly the largest U.S. ports in terms of cargo tonnage or passenger traffic. According to the DHS, this approach was intended to allocate grant resources according to the overall risk among eligible ports and to fund projects with the greatest potential to reduce the risk of "high-priority" threats.[59]

---

[54] This figure includes $75 million in port security grants awarded under the DHS's Urban Area Security Initiative in FY2003.

[55] Transportation Security Administration (TSA). Port Security Grant Program Awards, Round 2. June 12, 2003. Available at http://www.aapa-ports.org/govrelations/attachA.doc.

[56] Dept. of Homeland Security, Office of Inspector General. *Review of the Port Security Grant Program.* OIG-05-10 January 2005. p. 17.

[57] Ibid.

[58] Dept. of Homeland Security. "FY2005 Port Security Grant Program." Fact sheet. May 13, 2005.

[59] Dept. of Homeland Security, Office of Inspector General. *Follow Up Review of the Port Security Grant Program.* OIG-06-24 February 2006 (Revised). p. 5.

The PSGP's round six grant eligibility was expanded to what the DHS has determined are the nation's 100 "most critical" ports [60] This was an apparent reversal of the program's strategic shift in round five which focused on larger ports. On the other hand, the PSGP round six grant application materials also appeared to focus on a smaller range of specific attack scenarios, placing a "strong emphasis" only on improvised explosive devices (IED) placed underwater, in vehicles on ferries, or in small craft and not on chemical, biological, radiological, and nuclear devices, as stated in round five.[61] According to press reports, the Coast Guard's Maritime Security Risk Assessment Model (MSRAM), which was used by the DHS to help evaluate its 2006 grant program applications, dealt only with "plausible" scenarios, such as small boat attacks on oil terminals, and did not attempt to evaluate the consequences of attacks using weapons of mass destruction.[62] Projects which demonstrated enhanced "Maritime Domain Awareness" such as access controls and standardized credentialing, command and control, communications, and intelligence sharing and analysis were added as an additional criteria for reviewing grant applications in round six. PSGP round six awards were granted to 50 ports of the 100 eligible to apply.

For the seventh round of grants, to satisfy the requirements in the SAFE Port Act (P.L. 109-347), DHS expanded the list of eligible ports to all those required to have an Area Maritime Security Plan, but the bulk of the funds are still reserved for the highest risk ports.[63] Selection criteria for grantees continues to emphasize IEDs, MDA, and standardized credentialing but adds emergency drills and exercises and regional port collaboration as priorities.

Emphasizing High Priority Scenarios

The PSGP's current focus on specific types of weapons and targets and on the nation's largest ports demonstrates an approach to the "unlimited scenarios" problem which emphasizes key scenarios. While not excluding other scenarios, the PSGP round six and seven application materials appear to narrow down priority scenarios in terms of locations (major ports), targets (ferries and cruise ships), and tactics (IED's). Port Security officials have also focused on priority scenarios, although not necessarily the same stated by the PSGP.

> There are ... a number of threat concerns that are believed to be more likely and therefore are the ones that most maritime security programs today are built around. These include the use of ports or vessels as a means to smuggle weapons of mass destruction or terrorist operatives into the United States, the use of ships as a weapon to attack critical infrastructure, the scuttling of ships in major shipping channels and terrorist attacks on ships such as ferries or oil tankers.[64]

As indicated by DHS, the priority scenarios approach has the advantage of applying the nation's limited maritime security resources against terrorism attack scenarios of greatest relative concern

[60] Dept. of Homeland Security. "FY2006 Port Security Grant Program." Fact sheet. July 7, 2006. p. 1.

[61] Ibid, p. 2.

[62] Edmonson, R.G. "Coast Guard: Risk-Assessment Tools Aid Consistency." *Pacific Shipper*. October 27, 2006. Numerical ratings from the MSRAM program reportedly accounted for 25% of port security grant applicants' overall application score in round six.

[63] Dept. of Homeland Security. "Fiscal Year 2007 Infrastructure Protection Program: Port Security Grant Program, Program Guidance and Application Kit," January 2007.

[64] Rooney, Beth. Manager of Port Security, Port Authority of NY and NJ. Statement before the House Government Reform Committee, Government Management Finance and Accountability Subcommittee. July 10, 2006.

based on intelligence and risk assessment. The approach may also create potentially beneficial competition among grant applicants seeking funds for similar security activities in different ports. It reflects the DHS's move towards risk-based distribution of all homeland security grants, maritime and non-maritime, as recommended by the 9/11 Commission.[65]

One significant disadvantage of emphasizing priority scenarios is dependence upon intelligence and risk assessment in an environment where neither may be robust. As the President's *National Strategy for Homeland Security* stated in 2002, "the ambiguous nature of most intelligence on terrorist threats means that ... decisions must often be made in conditions of great uncertainty."[66] To the extent that priority attack scenarios identified by DHS or port security officials are not the right ones, serious threats to U.S. maritime security may remain. Perhaps predictably, there appears to be disagreement among security analysts about the credibility and likelihood of specific attack scenarios frequently cited in maritime security policy discussions. Specific examples are discussed in the following section.

Likelihood of U.S. Maritime Terrorist Attacks

Clear perspectives on the likelihood of specific types of maritime terrorist attacks are essential for prioritizing the nation's maritime anti-terrorism activities. Especially when security policies seek to concentrate resources against a relatively limited number of terrorism scenarios, as appears to be the case for DHS port security grants, the responsible agencies must be confident that these scenarios are credible and do, indeed, pose the greatest threat to the United States. In practice, however, there has been considerable public debate about the likelihood of scenarios frequently identified as having high priority by federal policy makers. As a 2006 RAND study of maritime security concluded "many perceptions of maritime terrorism risks do not align with the reality of threats and vulnerabilities."[67] The following section discusses perceptions and uncertainties pertaining to three prominent maritime attack scenarios, including nuclear or "dirty" bombs smuggled in shipping containers, liquefied natural gas (LNG) tanker attacks, and attacks on passenger ferries.

The "Bomb in a Box" Scenario

Type of Bomb

The Bush Administration's *National Strategy for Maritime Security* states that "WMD issues are of the greatest concern since the maritime domain is the likely venue by which WMD will be brought into the United States."[68] One arms control expert believes that, under current maritime security practices, the likelihood of such an attack within the decade "is more likely than not."[69]

---

[65] For more information see CRS Report RL33583, *Homeland Security Grants: FY2003 - FY2006 Evolution of Program Guidance and Grant Allocation Methods*, by (name redacted).

[66] U.S. Office of Homeland Security. *National Strategy for Homeland Security*. July 16, 2002.

[67] Greenberg, Michael D., Chalk, Pete, Willis, Henry H., Khilko, Ivan, and Ortiz, David S.; *Maritime Terrorism: Risk and Liability*. RAND Center for Terrorism Risk Management Policy. 2006. p. xxi.

[68] Executive Office of the President. *The National Strategy for Maritime Security*. September 20, 2005. p. 4.

[69] Allison, Graham. Remarks on "CNN Presents: Nuclear Terror." *CNN Presents*. Broadcast transcript. September 12, 2004. http://transcripts.cnn.com/TRANSCRIPTS/0409/12/cp.00.html.

According to a press report, the operations and emergency management director for the Port of Los Angeles has stated that the probability of a nuclear attack at his port is "not low," and that measures to prevent such an attack are the port's top priority.[70]

Although much attention is paid to the threat of nuclear terrorism, there are divergent opinions about the likelihood of a terrorist group such as al Qaeda constructing or otherwise obtaining a workable nuclear weapon.[71] Expert estimates of the probability of terrorists obtaining a nuclear device have ranged from 50% to less than 1%.[72] Among other challenges to obtaining such a device, experts believe it unlikely that countries with nuclear weapons or materials would knowingly supply them to a terrorist group.[73] It also may be technically difficult to successfully detonate such a nuclear device. North Korea experienced technical failures in conducting its 2006 nuclear weapons test, and this test took place under highly controlled conditions.[74] Attempting to detonate a nuclear device in a maritime terror attack could pose even greater operational challenges. Consistent with these perspectives, Secretary of Homeland Security Michael Chertoff has stated, "I don't think that in the near term there's a significant likelihood of a traditional nuclear device being detonated" in the United States.[75]

Other experts concede that evaluating the likelihood of nuclear terrorism is inherently uncertain, but that such potential attacks warrant attention even if they are unlikely.

> The probability of a terrorist attack with an actual nuclear weapon cannot be reliably estimated, and it is surely lower than the probability of virtually any other type of terrorist attack. But the devastation from such an attack would be so overwhelming that, based on expected damages—the probability multiplied by the consequences—this threat must be considered one of the greatest dangers America faces....[76]

Terrorist attacks on U.S. ports with radiological dispersion devices ("dirty" bombs) is also considered among the gravest maritime terrorism scenarios.[77] A 2003 simulation of a series of such attacks concluded that they "could cripple global trade and have a devastating impact on the nation's economy."[78] Many terrorism analysts view such a dirty bomb attack as relatively likely. In a 2005 survey, for example, nuclear non-proliferation experts expressed their beliefs (on average) that there was a 25% chance of a dirty bomb attack in the United States by 2010 and a 40% chance of such an attack by 2015.[79] Studies suggest that the materials required to make a

[70] Gorman, Siobhan and Sydney J. Freedberg, Jr. "Early Warning." *The National Journal*. June 11, 2005.

[71] For further analysis on this topic, see CRS Report RS21293, *Terrorist Nuclear Attacks on Seaports: Threat and Response*, by Jonathan Medalia.

[72] Hegland, Corine and Webb, Greg. "The Threat," *National Journal.* April 15, 2005. http://nationaljournal.com/members/news/2005/04/0415nj1.htm#; Senator Richard G. Lugar. "The Lugar Survey on Proliferation Threats and Responses." June 2005. p. 6. http://lugar.senate.gov/reports/NPSurvey.pdf.

[73] Bunn, Matthew and Weir, Anthony. *Securing the Bomb 2006*. John F. Kennedy School of Government Harvard University. Commissioned by the Nuclear Threat Initiative. July 2006. p. 29.

[74] Collins, Graham P. "Kim's Big Fizzle: The Physics Behind A Nuclear Dud." *Scientific American*. January 2007.

[75] Department of Homeland Security (DHS). Remarks by Secretary of Homeland Security Michael Chertoff at George Mason University. Fairfax, VA. April 26, 2006.

[76] de Rugy, Veronique. "Is Port Security Spending Making Us Safer?" American Enterprise Institute. Working Paper #115. September 7, 2005. p. 8.

[77] For further information on dirty bombs, see CRS Report RS21528, *Terrorist "Dirty Bombs": A Brief Primer*, by Jonathan Medalia.

[78] Ibid. Booz Allen Hamilton. 2003. p. 1.

[79] Senator Richard G. Lugar. "The Lugar Survey on Proliferation Threats and Responses." June 2005. p. 6.
(continued...)

dirty bomb may be widely available and poorly controlled internationally.[80] According to some press reports, U.S. and British intelligence agencies have reportedly concluded that Al Qaeda has succeeded in making such a bomb.[81] Port operators have testified before Congress that they believe "it is just a question of time" before terrorists with dirty bombs successfully attack a U.S. port.[82]

Although many experts consider attacks with dirty bombs among the most likely maritime terrorism scenarios, other experts dispute this conclusion. Scientists have long questioned whether terrorists could actually build a dirty bomb with catastrophic potential since handling the necessary radioactive materials could cause severe burns and would likely expose the builders to lethal doses of radiation.[83] Building and transporting such a bomb safely and to avoid detection would likely require so much shielding that it would be "nearly impossible" to move.[84] Weaker dirty bombs made from less radioactive (and more common) materials would be easier to build and deploy, but would have a much smaller physical impact and would likely cause few human casualties. Consequently, some analysts argue that terrorists will forego dirty bombs, restricting themselves to the use of more conventional explosives.[85] In support of this argument, analysts point to the fact that there have been no U.S. dirty bomb attacks, notwithstanding the supposed ease of perpetrating such attacks.[86] They also note that the 2005 U.S. indictment of alleged "dirty bomber" Jose Padilla, in fact, contained no evidence of, or references to, a dirty bomb plot.[87]

Faced with contradictory perspectives on the likelihood of a dirty bomb attack scenario at a U.S. port, analysts and policy makers draw qualified conclusions about such an attack. If a "weak" dirty bomb attack is more likely than a "strong" one, but a weak attack will have limited effects, it is unclear whether such an attack would meet terrorist objectives. On the other hand, the effects on the general public of any dirty bomb attack, even a weak one, may be great enough to motivate potential attackers. As one analyst has stated, notwithstanding the challenges to dirty bombers, "the chances of a dirty bomb being deployed by al Qaeda cannot be discounted... Given the exponential psychological and economic effects of such a weapon, the benefits of deploying one may far outweigh the costs and difficulties entailed in its construction."[88]

(...continued)

http://lugar.senate.gov/reports/NPSurvey.pdf.

[80] Government Accountability Office (GAO). *Nuclear Nonproliferation: U.S. and International Assistance Efforts to Control Sealed Radioactive Sources Need Strengthening.* GAO-03-638. May 16, 2003. p. 65.

[81] Mayer, Josh. "Al Qaeda Feared to Have Dirty Bombs." *Los Angeles Times*. February 8, 2003. p. 1.

[82] Gilbert, Gary. Senior V.P., Hutchison Port Holdings. Statement before the Senate Homeland Security and Governmental Affairs Committee, Permanent Investigations Subcommittee. March 30, 2006.

[83] Singer, S. Fred. Hoover Institution, Stanford Univ. "Nuclear Terrorism: Facts and Fantasies." *Washington Times* (Commentary). April 5, 2002.

[84] *"Dirty Bomb" Fact Sheet*. Center for International Security and Cooperation, Stanford University. October 2006. http://iis-db.stanford.edu/pubs/20769/dirty_bomb_facts.pdf.

[85] Burgess, Mark. "Pascal's New Wager: The Dirty Bomb Threat Heightens." Center for Defense Information. Washington. February 4, 2003. http://www.cdi.org/terrorism/dirty-bomb.cfm.

[86] Sterngold, James. "Assessing the Risk of Nuclear Terrorism" *San Francisco Chronicle*. April 18, 2004.; Dotinga, Randy. "After the Beep, Exit the Premises." *Wired News*. May 6, 2004. http://www.wired.com/news/technology/1,63328-0.html.

[87] Taylor, Guy. "Padilla Case Mum on 'Dirty Bomb'." *Washington Times*. November 24, 2005. p. A03.

[88] Burgess, Mark. February 4, 2003.

Method of Delivery

The potential smuggling and detonation of a nuclear or dirty bomb device in a shipping container at a U.S. port is one of the threats most specifically and frequently mentioned by legislators in the context of maritime security.[89] Shipping containers may be particularly vulnerable to terrorist infiltration compared to other types of cargo for three reasons. First, shipping containers are relatively large. They come in standard sizes from 20 to 53 feet long, although the most common are 40 feet or longer—about the size of a truck semi-trailer. Second, the containers on any given ship are packed at the factories or warehouses of many different companies that can be dispersed far and wide from the loading port, making it impossible for government authorities to ensure that only legitimate cargo has been packed. Third, the containers are typically trucked to the port of loading, during which the integrity of the shipments rests entirely on the trustworthiness or due diligence of the truck drivers. A maritime security expert at the Council on Foreign Relations, who is a former Commandant of the U.S. Coast Guard, outlines a scenario that most concerns him:

> Let me share with you the terrorist scenario that most keeps me awake at night.... A container of athletic foot wear for a name brand company is loaded at a manufacturing plant in Surabaya, Indonesia. The container doors are shut and a mechanical seal is put into the door pad-eyes. These designer sneakers are destined for retail stores in malls across America. The container and seal numbers are recorded at the factory. A local truck driver, sympathetic to al Qaeda picks up the container. On the way to the port, he turns into an alleyway and backs up the truck at a nondescript warehouse where a small team of operatives pry loose one of the door hinges to open the container so that they can gain access to the shipment. Some of the sneakers are removed and in their place, the operatives load a dirty bomb wrapped in lead shielding, and they then refasten the door.

Other analysts assert that, if terrorists were to attempt a nuclear or dirty bomb attack in a U.S. port, they would be unlikely to do so using a shipping container because it would put the device beyond a terrorist group's control. These analysts question whether the container shipping system offers the routing or scheduling precision required by terrorists to position the bomb in the right place at the right time. Other observers assert that some types of non-containerized cargo could also be used for smuggling a bomb.[90] The manager of port security at the Port Authority of New York and New Jersey states that their biggest concern is roll-on/roll-off cargo (ships that carry automobiles, trucks, and other vehicles).[91] Non-containerized cargo is more plentiful. By tonnage, containers carry only 11% of U.S. overseas waterborne trade[92] and container ships account for about one in every three U.S. port calls.[93] Other types of cargo also face less security screening.[94] Relatively low-value cargo might be targeted if terrorists perceive it receives less attention from

[89] See, for example, Hon. Edward J. Markey. "Rep. Markey Urges Scanning for Nuclear Devices in Container Ships Before They Arrive at U.S. Ports." Press release. September 28, 2006; Office of Senator Patty Murray. "Cargo Security: Floor Remarks by Senator Patty Murray Introducing the GreenLane Bill for Senate Consideration." Press release. September 7, 2006.

[90] For an analysis of smuggling a nuclear weapon in an oil tanker, see CRS Report RS21997, *Port and Maritime Security: Potential for Terrorist Nuclear Attack Using Oil Tankers*, by Jonathan Medalia.

[91] Ibid.

[92] U.S. Department of Transportation (DOT). *An Assessment of the U.S. Marine Transportation System.* Report to Congress. September 1999.

[93] U.S. Maritime Administration (MARAD). *Vessel Calls at U.S. and World Ports 2005.* April 2006. p. 1.

[94] Stables, Eleanor. "For Better Cargo Security, Government Needs to Think 'Outside the Box,' Experts Say." *CQ Homeland Security*. October 1, 2006.

U.S. Coast Guard and customs officials. For instance, a federal official familiar with New York harbor, pointing to a scrap metal terminal in Jersey City, stated the following to a reporter, "If I wanted to bring an atomic bomb into the port, I'd do it through that scrap operation."[95]

The Government Accountability Office (GAO) investigated the potential for maritime terrorists to use weapons of mass destruction (WMDs) in 2005. In its report, the GAO states that

> An extensive body of work on this subject by the Federal Bureau of Investigation and academic, think tank, and business organizations concluded that while the likelihood of such use of containers is considered low, the movement of oceangoing containerized cargo is vulnerable to some form of terrorist action. Such action, including attempts to smuggle either fully assembled weapons of mass destruction or their individual components, could lead to widespread death and damage.[96]

Liquefied Natural Gas (LNG) Tanker Attacks

Potential terrorist attacks on LNG tankers in U.S. waters have been a key concern of policy makers in ports with LNG facilities because such attacks could cause catastrophic fires in port and nearby populated areas. The Coast Guard's FY2006 budget specifically requested funding for "additional boat crews and screening personnel at key LNG hubs."[97] To date, no LNG tanker or land-based LNG facility in the world has been attacked by terrorists. However, similar natural gas and oil assets have been favored terror targets internationally. The attack on the *Limburg*, although an oil tanker, is often cited as an indication of LNG tanker vulnerability. The Department of Homeland Security (DHS) specifically included LNG tankers among a list of potential terrorist targets in a security alert late in 2003.[98] The DHS also reported that "in early 2001 there was some suspicion of possible associations between stowaways on Algerian flagged LNG tankers arriving in Boston and persons connected with the so-called 'Millennium Plot'" to bomb targets in the United States. While these suspicions could not be proved, DHS stated that "the risks associated with LNG shipments are real, and they can never be entirely eliminated."[99] A 2004 report by Sandia National Laboratories concluded that potential terrorist attacks on LNG tankers, could be considered "credible and possible."[100] The Sandia report identified LNG tankers as vulnerable to ramming, pre-placed explosives, insider takeover, hijacking, or external terrorist actions (such as a *Limburg*-type, missile or airplane attack).[101] Former Bush Administration counter-terrorism advisor Richard Clarke has asserted that terrorists have both the desire and capability to attack LNG shipping with the intention of harming the general population.[102]

---

[95] Finnegan, William. "Watching the Waterfront." *The New Yorker*. June 19, 2006. p. 63.

[96] Government Accountability Office (GAO). *Cargo Security: Partnership Program Grants Importers Reduced Scrutiny With Limited Assurance of Improved Security*. GAO-05-404. March, 2005. p. 7.

[97] Dept. of Homeland Security (DHS). *Budget-in-Brief, Fiscal Year 2006*. https://www.dhs.gov/xlibrary/assets/Budget_BIB-FY2006.pdf.

[98] Office of Congressman Edward J. Markey. Personal communication with staff. January 5, 2004.

[99] Turner, Pamela J., Assistant Secretary for Legislative Affairs, Department of Homeland Security (DHS). Letter to U.S. Representative Edward Markey. April 15, 2004. p. 1.

[100] Sandia National Laboratories (SNL). *Guidance on Risk Analysis and Safety Implications of a Large Liquefied Natural Gas (LNG) Spill Over Water*. SAND2004-6258. Albuquerque, NM. December 2004. pp. 49-50.

[101] SNL. December 2004. pp. 61-62.

[102] Clarke, Richard A., et al. *LNG Facilities in Urban Areas*. Good Harbor Consulting, LLC. Prepared for the Rhode Island Office of Attorney General. GHC-RI-0505A. May 2005.

Although they acknowledge the security information put forth by federal agencies, many experts believe that concern about threats to LNG tankers is overstated.[103] In 2003, the head of one university research consortium remarked, for example, "from all the information we have ... we don't see LNG as likely or credible terrorist targets."[104] Industry representatives argue that deliberately causing an LNG catastrophe to injure people might be possible in theory, but would be extremely difficult to accomplish. Likewise, the Federal Energy Regulatory Commission (FERC) and other experts believe that LNG facilities are relatively secure compared to other hazardous chemical infrastructures which receives less public attention. In a December 2004 report, the FERC stated that

> for a new LNG terminal proposal ... the perceived threat of a terrorist attack may be considered as highly probable to the local population. However, at the national level, potential terrorist targets are plentiful.... Many of these pose a similar or greater hazard to that of LNG.[105]

The FERC also remarked, however, that "unlike accidental causes, historical experience provides little guidance in estimating the probability of a terrorist attack on an LNG vessel or onshore storage facility."[106] Former Director of Central Intelligence, James Woolsey, has stated his belief that a terrorist attack on an LNG tanker in U.S. waters would be unlikely because its potential impacts would not be great enough compared to other potential targets.[107] LNG terminal operators which have conducted proprietary assessments of potential terrorist attacks against LNG tankers, have expressed similar views.[108] In a September, 2006, evaluation of a proposed LNG terminal in Long Island Sound, the USCG states that "there are currently no specific, credible threats against" the proposed LNG facility or tankers serving the facility.[109] The evaluation also notes, however, that the threat environment is dynamic and that some threats may be unknown.[110]

Passenger Ferry Attacks

Congressional policy makers frequently cite passenger ferries as a key maritime security concern. For example, in 2005, one Member of Congress stated that "there is a serious security gap in our ferry systems and we need to ensure that passengers on our nation's waterways are protected."[111] A RAND study in 2006 argued that attacks on passenger ferries in the United States might be

[103] McLaughlin, J. "LNG is Nowhere Near as Dangerous as People Are Making it Out to Be." *Lloyd's List*. February 8, 2005. p5.

[104] Behr, Peter. "Higher Gas Price Sets Stage for LNG." *Washington Post*. July 5, 2003. p. D10.

[105] Federal Energy Regulatory Commission (FERC). *Vista del Sol LNG Terminal Project, Draft Environmental Impact Statement*. FERC/EIS-0176D. December 2004. p. 4-162.

[106] FERC. FERC/EIS-0176D. December 2004. p4-162. Notwithstanding this assertion, in its subsequent draft review of the Long Beach LNG terminal proposal, the FERC states that "the historical probability of a successful terrorist event would be less than seven chances in a million per year..." See FERC. October 7, 2005. p. ES-14.

[107] Woolsey, James. Remarks before the National Commission on Energy LNG Forum, Washington, D.C., June 21, 2006.

[108] Grant, Richard, President, Distrigas. Testimony before the Senate Committee on Energy and Natural Resources, Subcommittee on Energy hearing on "The Future of Liquefied Natural Gas: Siting and Safety." February 15, 2005.

[109] U.S. Coast Guard. *U.S. Coast Guard Captain of the Port Long Island Sound Waterways Suitability Report for the Proposed Broadwater Liquefied Natural Gas Facility*. September 21, 2006. p. 146.

[110] Ibid.

[111] Congressman Frank Pallone, Jr. "Pallone Calls for Increased Funding for Ferry Security." Press release. July 15, 2005.

highly attractive to terrorists because such attacks are easy to execute, may kill many people, would likely draw significant media attention and could demonstrate a terrorist group's salience and vibrancy.[112] One U.S. Coast Guard risk analyst reportedly has stated that "in terms of the probability of something happening, the likelihood of it succeeding and the consequences of it occurring, ferries come out at the very high end."[113] Such attacks have occurred overseas. As noted earlier in this report, terrorists linked to Al Qaeda attacked and sank the Philippine vessel *Superferry 14* in 2004.

In a 2006 report, the U.S. Department of Justice (DOJ) identified a ferry bombing as among the most likely types of maritime terror attacks.[114] The DOJ report reached this conclusion based largely on the number of suspicious incidents reported at marine facilities in the Seattle area and at other U.S. ports. However, officials in the Seattle office of the Federal Bureau of Investigation (FBI) reportedly suggested at the time that the DOJ's high ranking of the passenger ferry threat might be due to more aggressive reporting of suspicious incidents in that region than elsewhere in the country.[115] Seattle FBI officials also reportedly stated that they had never been able to tie a specific suspicious incident to a terrorist group or terrorist plan.[116] Thus, while there appears to be a logical case why ferries may be a key type of terrorist target, questions remain about actual terrorist activities related to ferries.

Overall Likelihood of Maritime Terrorism

The prior discussion illustrates the uncertainty surrounding some of the maritime terrorism scenarios of greatest concern to U.S. maritime security officials. Questions about the likelihood of these specific, high priority scenarios beg the larger question of how likely is *any* maritime terrorism attack against the United States. Some experts suggest that some such attack, in one form or another, is almost inevitable. For example, one senior U.S. military officer has reportedly asserted that "it's just a matter of time until the terrorists try to use a ... maritime attack against us."[117] Security analysts also point to known terrorist plots to attack U.S. maritime targets, such as those passing the Straits of Gibraltar, as evidence that global terrorist groups continue to plan maritime terrorism activities. Information from captured Al Qaeda member Abd al Rahman al Nashiri reportedly included plans for attacks on a wide range of Western maritime targets, including military vessels, oil tankers, and cruise ships.[118]

Other analysts believe future maritime attacks against the United States are relatively unlikely, especially in U.S. waters. Notwithstanding specific acts of terrorism in the past, such as the *Cole* bombing, they note that fewer than 1% of all global terrorist attacks since 1997 have involved

[112] Greenberg, M.D. et al. 2006. p. 95.

[113] Lipton, Eric. "Trying to Keep the Nation's Ferries Safe from Terrorists." *New York Times*. March 19, 2005.

[114] U.S. Dept. of Justice, Office of the Inspector General. *The Federal Bureau of Investigation's Efforts to Protect the Nation's Seaports*. Audit Report 06-26. March 2006. p. 52.

[115] Shukovsky, Paul and Barber, Mike. "Ferries a Top Terror Target, FBI Cautions." *Seattle Post-Intelligencer*. April 21, 2006. p. A1.

[116] Ibid.

[117] Gen. Ralph Eberhart, U.S. Northern Command, as quoted in "Militants Eyeing Seaborne Attack, U.S. General Says." Reuters. August 25, 2004.

[118] Köknar, Ali M. "Maritime Terrorism: a New Challenge for NATO." *Energy Security*. Institute for the Analysis of Global Security (IAGS). January 24, 2005.

maritime targets.[119] Furthermore, international terrorists have attacked no maritime targets in U.S. territory since the anti-Castro attacks in 1976 despite their demonstrated ability to do so overseas.[120] Analysts also argue that U.S. ports and waterways are increasingly well-protected against terrorists due to the ongoing security activities of the U.S. Coast Guard, U.S. Customs and Border Protection (CBP), provisions of the Maritime Transportation Security Act (P.L. 107-295), protections added using DHS port security grants, and other U.S. maritime security measures.[121] Classification issues may also influence differing perceptions of maritime terrorism risk since piracy unrelated to terrorism is common in Southeast Asia and may be conflated with terrorism in maritime security statistics.[122]

A key consideration in assessing the general likelihood of a maritime attack against the United States is the inherent operational difficulty in mounting such attacks, especially compared to land attacks which may alternatively satisfy terrorist objectives. One U.S. naval analyst has identified a number of specific challenges for terrorists in the maritime environment:

- Maritime targets are relatively more scarce than land targets;
- Surveillance at sea offers less cover and concealment than surveillance on land;
- Tides, currents, wind, sea state, visibility, and proximity to land must all be factored into a maritime terror operation;
- Maritime terror operations may require skills that are not quickly or easily acquired such as special training in navigation, coastal piloting, and ship handling;
- Testing weapons and practicing attack techniques, hallmarks of Al Qaeda's typically meticulous preparation, are harder and more difficult to conceal at sea than on land;
- The generally singular nature of maritime targets, the low probability of damage and casualties secondary to the intended target, and the problems associated with filming attacks at sea for terrorist publicity may also reduce the desirability of maritime targets.[123]

Given these challenges, it remains an open question how likely maritime attacks against the United States may be. In terms of the scenario framework in this report, although a successful attack on U.S. maritime targets would likely satisfy certain objectives of known international perpetrators such as Al Qaeda, tactical uncertainties and security deterrents may lead terrorist planners to turn their attention elsewhere. It bears repeating, however, that maritime terror attacks against the U.S. have occurred and there is evidence they have been planned for the future,

[119] National Memorial Institute for the Prevention of Terrorism (MIPT). Terrorist incident reports. July 20, 2006. http://www.tkb.org/IncidentTargetModule.jsp.

[120] MIPT. July 20, 2006.

[121] For further discussion, see CRS Report RL31733, *Port and Maritime Security: Background and Issues for Congress*, by (name redacted).

[122] Valencia, Mark J. and Young, Adam J. "Conflation of Piracy and Terrorism in Southeast Asia: Rectitude and Utility." *Contemporary Southeast Asia*. Vol. 25. No. 2. August 2003. pp. 269-283.

[123] Captain James Pelkofski, U.S. Navy. "Before the Storm: al Qaeda's Coming Maritime Campaign." *Proceedings*. U.S. Naval Institute. Vol. 132. No. 12. December 2005. http://www.usni.org/proceedings/Articles05/Pro12Pelkofski.html.

despite the operational challenges. The same naval analyst cited above calls for continued vigilance:

> Rather than develop a false sense of security based on the belief that inherent difficulties will limit maritime terrorism ... caution is warranted in light of al Qaeda's adaptability, ingenuity, tenacity, and audacity. Successful development and application of maritime tactics, techniques, and procedures has already occurred within the terrorist community.[124]

It appears, therefore, that while maritime terrorist attacks against the United States may be more difficult to execute and, consequently, less likely to occur than other types of attacks, they remain a significant possibility and warrant continued policy attention.

The key challenge in determining the overall likelihood of a terrorist attack on a U.S. port is reducing uncertainty about specific types of attacks and potential attackers. Because historical terrorist activity is not necessarily a reliable predictor of future activity, scenarios derived from attacks like that on the U.S.S *Cole* may not help prepare for actual future attacks. Furthermore, information about the ongoing motivations, capabilities, and plans of terrorist groups is limited and typically not in the public domain. Terrorist intelligence gathered by U.S. and foreign agencies may reduce this uncertainty, but is unlikely to eliminate it. Faced with this uncertainty, decision makers are to some extent forced to rely upon their own best judgment to reach conclusions about the likelihood of maritime terrorist attacks.

Policy Issues for Congress

Maritime terrorist threats to the United States are varied, and so are the nation's efforts to combat them. As Congress continues its oversight of ongoing U.S. maritime security activities, it may focus on issues related to the consistency of maritime terrorism scenario assessment, intelligence gathering, and responding to new intelligence.

Consistency of Terrorism Scenario Assessment

Development and assessment of maritime terrorism scenarios is a key element of federal port security exercises, grant administration, and legislative oversight. It appears, however, that these three dimensions of the nation's maritime security strategy emphasize terrorism scenarios in different ways. Port security exercises (conducted under a number of independent programs) address the broadest range of terrorism scenarios, with no obvious focus on any particular scenario. The DHS port security grant program currently emphasizes a subset of these scenarios—IED attacks on ferries and cruise ships in major ports, for example. Federal legislators appear to focus oversight on a different subset of scenarios, notably WMD's aboard container vessels and attacks on LNG tankers. As this report states, there is a logical basis underlying the scenario priorities established for exercises, grants, and oversight. Nonetheless, if these activities are intended to derive from a uniform federal maritime security strategy the question arises to what degree these activities are complementary or inconsistent.

If port officials, grant administrators, and legislators disagree on what types of attack scenarios are of greatest priority, either because their security assessments are inconsistent, or because they

[124] Ibid.

lack sufficient intelligence about terrorist threats, port security resources may be deployed inefficiently. For example, sharply increasing security against specific types of maritime attacks in specific locations may have limited benefits for overall port security if other significant vulnerabilities are not addressed as a result. A key question is whether policymakers are too focused on a narrow spectrum of the threat. A former Federal Maritime Commissioner has stated that "it [is] fair to say there has been little to no emphasis on non-containerized cargo in the political arena," while in contrast, "'virtually everyone' in the industry thinks non-containerized cargo is in 'many respects a more vulnerable path.'"[125] While concern, in this case, for container security may not be misplaced, there are other forms of cargo that terrorists could exploit just as effectively.

Intelligence Gathering

Because intelligence about terrorist capabilities and activities is a key factor in terrorism scenario assessment, Congress may act to ensure that the responsible U.S. intelligence agencies work to improve their intelligence gathering and reduce terrorism scenario uncertainty. As a Department of Defense official has reportedly remarked,

> We have the operational capabilities to defeat any of these threats ... if we see the threat approaching....The most important thing we can do is to dramatically improve our overseas intelligence collection, with a specific orientation toward the maritime threat.[126]

Better intelligence may also help ensure that various federal maritime security activities are more closely aligned. The Government Accountability Office (GAO) evaluated in December 2005 the port risk assessment practices of the U.S. Coast Guard, the Office for Domestic Preparedness, and the Information Analysis and Infrastructure Protection Directorate—all agencies within the Department of Homeland Security. The GAO report concluded:

> Each component faces many challenges in making further progress... For example, obtaining better quality data from intelligence agencies would help DHS components estimate the relative likelihood of various types of threats—a key element of assessing risks. In the longer term, progress will depend increasingly on how well risk management is coordinated across agencies, because current approaches in many ways are neither consistent nor comparable.[127]

Responding to New Intelligence

Given the dynamic nature of the terrorist threat, Congress may consider whether federal funding mechanisms for anti-terrorism measures are flexible enough to respond to new threat intelligence. Between the time Congress decides on the allocation of security grants among the various transportation modes in the annual appropriations process and the time that those grants are actually awarded can be almost a year. Within this time frame, new intelligence may indicate that security resources be reallocated to respond to a different threat. A related oversight issue for

---

[125] Robert Quartel, as quoted in Stables, Elanor. "For Better Cargo Security, Government Needs to Think 'Outside the Box,' Experts Say." *CQ Homeland Security*. October 1, 2006.

[126] McHale, Paul F., Asst. Sec. of Defense for Homeland Defense quoted in Pyle, R. "Agencies Analyze Responses to Nightmare Scenario at U.S. Ports." Associated Press. June 7, 2006.

[127] Government Accountability Office. *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure*. GAO-06-91. December 15, 2005.

Congress is the capability of the U.S. Coast Guard and CBP to shift staff and resources as new threat information becomes available. For instance, the U.S. Coast Guard has developed Maritime Safety and Security Teams consisting of about 75 personnel that are designed to provide a rapid surge capacity at any port as the need arises. CBP may have more difficulty in shifting resources because, in addition to operating in seaports, it operates in airports and at land border crossings and not all of its inspection equipment is easily adaptable across these three environments.

Conclusion

Public information suggests that the threat of maritime terrorism is significant, and can take myriad forms, but that different dimensions of the nation's maritime security activities prioritize these activities in different ways. As oversight of the federal role in maritime security continues, Congress may raise questions concerning the relationship among these activities, and the implications of differing terrorism scenario priorities among them. Improved gathering and sharing of maritime terrorism intelligence may enhance consistency across various U.S. maritime security activities and increase the efficient deployment of maritime security resources.

In addition to these issues, Congress may assess how the various elements of U.S. maritime security fit together in the nation's overall strategy to protect the public from terrorist attacks. For example, bulk quantities of hazardous chemicals are found in marine vessels, in rail and highway tankers, and in chemical facilities on land. Terrorists may seek to exploit such chemicals in any of these sectors. Balancing the nation's homeland security resources across the maritime and non-maritime sectors is a policy challenge because specific sectors may fall under different homeland security authorities and regulations. Uncertainty about terrorist capabilities and activities complicates this problem by making it difficult to compare terrorist attack scenarios across sectors. Without such a comprehensive perspective on terrorist threats, security analysts may have difficulty identifying which assets to protect and how well to protect them with the limited security resources available. Reviewing how these security priorities and activities fit together to achieve common goals could be an oversight challenge for Congress.

Author Contact Information

(name redacted)
Specialist in Energy and Infrastructure Policy
[redacted]@crs.loc.gov, 7-....

(name redacted)
Specialist in Transportation Policy
[redacted]@crs.loc.gov, 7-....