CHAPTER 4

Protecting America's Seaports: The Vulnerability of Intermodal Commerce

L. Edward Mayer

Few Americans appreciate the fact that liner shipping and container ports are key elements through which flows the vast array of products available for their purchase.

—Jon S. Helmick
Society of Logistics Engineers

Introduction

Liner shipping is the backbone of international trade in manufactured goods. Liners, sailing on regular schedules along established ocean trade lanes, move vast quantities of consumer, industrial, and military commodities. Liners transport 95 percent of peacetime commerce and wartime equipment and supplies. Containerized cargo is the method of choice between developed economies, and 16,000 containers enter the U.S. every day at any one of 361 seaports; the biggest U.S. seaports being Los Angeles, Long Beach, and New York/Jersey City.[1]

Intermodal Commerce

Intermodal commerce, or the container trade, is the containerized shipping of cargo. Ships loaded with as many as 6600 Twenty Equivalent-foot Unit containers (TEU) arrive in seaports worldwide and quickly transfer their cargo onto various forms of land transportation. In one eight hour period, a 6600 TEU "mega ship" can be off-loaded and readied for reload.[2] The TEUs are double stacked on railcars adjacent to the seaport or are placed on flatbeds and driven out using tractor-trailers.

In the intermodal business, time is money. Ninety percent of the TEUs clear customs electronically using the U.S. Customs Service's Automated Commercial Environment (ACE). ACE is a comprehensive system used by the U.S. Customs Service to track, control, and process all commercial goods imported into and exported from the United States. Shipping companies transmit manifests for their ships in advance so when the containers are offloaded they can be immediately transferred to land transportation.[3] This is one reason why only 2 percent of all TEUs entering the U.S. are searched by the U.S. Customs service.[4]

The Security Dilemma

The terrorist attacks on September 11, 2001, brought to light the vulnerability of America's critical infrastructure. In November 2001, Admiral James Loy, U.S. Coast Guard Commandant, met with the International Maritime Organization in London to propose sweeping changes to the international shipping industry. His point was clear, "The security challenges are enormous," referring to the world's seaports. Admiral Loy went on to say, "Are [seaports] secure? I am afraid my answer is no."[5]

The U.S. is dependent on liner shipping and intermodal commerce. The security dilemma lies in the fact that there must be a balance between seaport security and the ability to flow commerce. Strict seaport security will insure safety but lose trade dollars to other countries. Loose seaport security will increase trade dollars but risk shutting down the industry with a single terrorist event. This chapter will explore the critical vulnerabilities of U.S. seaports, the government agencies charged with U.S. seaport security, and the security measures in place to protect them. The author's views on the success of seaport security are summarized in the conclusion.

Seaport Vulnerabilities

> *A terrorist act involving weapons of mass destruction at one of these seaports could result in extensive loss of lives, property, and business, affect the operations of harbors and*

> *the transportation infrastructure, and cause extensive environmental damage.*
>
> —F. Amanda Debusk
> Commissioner of the Interagency Commission
> on Crime and Security in U.S. Seaports

U.S. shipping can be characterized as a system composed of seaborne shipping routes, seaports and their critical support infrastructure, and air and rail corridors. In many cases like New York/Jersey City, Los Angeles, or Long Beach the seaports are designed for maximum throughput with the docks, rail, air, highways, and some production facilities in close proximity.[6] The ports themselves can be strategic targets. They are typically in heavily populated areas, hold significant national infrastructure, and are terminals for multiple shipping vessels that can be targets themselves. Also, they are often associated with important economic or national security sectors (Strategic Sealift, Refineries, Airports) that are prime targets for adversaries.[7] The Center for Naval Analysis points out that an attack on a critical port or its adjacent waterways might not only destroy high value assets and shipping, but could cripple the U.S. economy.

In April 1999, President Clinton directed the Secretary of the Treasury, the Attorney General, and the Secretary of Transportation to establish an interagency commission to study the extent of crime and the state of security in U.S. seaports. The Interagency Report on Crime and Security in United States Seaports was released on September 7, 2000. A Presidential news release stated that the report documented the current crime problem in seaports, identified present and projected security threats, and recommended a number of measures aimed at reducing the vulnerability of maritime commerce and its supporting infrastructure. Some specific comments included:

1. U.S. seaports typically allow free access to docks and often to container storage areas.

2. Firearms are generally permitted at dockside.

3. The federal government has no unified plan for monitoring seaport security, although the ports are international gateways similar to the land portals at San Diego, Detroit, and Niagara Falls.

4. The ports receive no federal funding for creating or maintaining basic security systems. And at many ports, even such basic equipment as small boats, cameras, and vessel-tracking devices are lacking.

5. The agencies involved in port operations fail to share information, and they lack the kind of computer communication needed to adequately track vessels and cargo.

6. Lack of information about incoming vessels and their cargo, plus the freedom to enter ports, would allow ships loaded with explosives, jet fuel, or noxious chemicals to ram docks, devastating ports and surrounding areas.[8]

The general lack of security and relaxed policies at U.S. seaports help explain the high incidence of cargo theft and other dockside crime. Estimates of the annual cost of cargo theft run as high as $12 billion.[9] Free access to docks makes it possible for terrorists to retrieve illicit arms and explosives or even to hijack ships. This environment breeds opportunities with serious consequences. Last year in New Orleans, a container, labeled as empty, held oil exploration tools that became radioactive during work in Africa. When Customs officials opened the container in port, their radiation detector alarmed. The inspectors summoned a decontamination team to dispose of the equipment.[10] Another more devastating instance occurred in Mombassa, Kenya. Al Qaeda had shipped arms and bomb-making materials via Osama bin Laden's covertly owned freighters. The materials were subsequently used to blow up the U.S. embassies in Nairobi, Kenya and Dar es Salaam, Tanzania in August 1998.[11] To date, the world economy has enjoyed unencumbered trade at the cost of minimal security standards. Today, the security dilemma pendulum is at the extreme and is swinging back towards tighter security standards.

Commerce and Seaport Security

> *If the U.S. authorities find themselves having to turn off the maritime-container-trade spigot, we will have effectively self-imposed a blockade on our own economy.*
>
> —Stephen Flynn
> Senior Fellow, Council of Foreign Relations
> Testimony to Senate Government Affairs Committee

Security Agencies

Seaport security falls under the cognizance of the U.S. Coast Guard under the Department of Transportation, the U.S. Customs Service under the Department of Treasury, and the individual private or public Port Authorities who operate the seaport. *[Editor's note: With the passage of the Homeland Security Act in November 2002, the U.S. Coast Guard and the U.S. Customs Service now fall under the domain of the Department of Homeland Security.]*

The primary responsibility for defending U.S. ports and coastal areas in peacetime falls to the U.S. Coast Guard.

> The U.S. Coast Guard is responsible for enforcement of federal laws and international treaties and security of U.S. Ports and waterways. This includes but is not limited to: establishment of security zones, supervision over the loading of explosives, control of all vessel traffic within a port, harbor defense, and…law enforcement of limited access areas.[12]

This means that the Coast Guard protects U.S. maritime borders from intrusions and enforces federal law in U.S. waters. Unless overridden by an Executive Order, Posse Comitatus (18 USC 1385) prohibits the use of the Navy and other federal military services from the enforcement of local, state, and federal laws.[13]

The United States Customs Service is the primary enforcement agency protecting the Nation's border. They focus on commerce and are

chartered to enforce the laws of the U.S. pertaining to trade to foster lawful international trade and travel.[14]

The Port Authorities run the day-to-day operations of the seaport. A large port authority has a police force with the full authority of local police. Port Authority Police are responsible for the physical security of the seaport to include law enforcement, fire fighting, and rescue operations.[15]

Security Initiatives

Private Industry

In 1997 private industry, feeling the sting from stolen cargo, initiated a security regime for perspective freight carriers. The Technology Asset Protection Association (TAPA) is an association of high technology companies organized for the purpose of addressing emerging security threats. Members of TAPA include: COMPUSA, Hitachi America Ltd., Dell Computers Corporation, Sears, and Sun Microsystems Inc. As high tech items became smaller and more portable and the security for factories and warehouses became more sophisticated, criminals began to target the products in transit. Dan Purtell, the chairman of TAPA, stated TAPA demanded that shipping companies seal off cargo containers at the time they left overseas factories until their arrival in the United States.[16] Freight Security Requirements (FSR) were established to ensure the safe and secure in-transit storage and warehousing of TAPA assets. The FSR specify the minimum acceptable standards for security throughout the supply chain and the methods to be used in maintaining those standards. Security requirements depend on the value of the material but may include electronic container locks, surveillance cameras, Global Positioning System transmitters, and environmental sensors. Major freight service providers are moving toward TAPA-recognized security standards and are recognizing the inherent value of doing so.[17] For some companies the losses from theft are down 80 percent, yielding much lower insurance rates.[18] This form of shipping security not only protects the cargo, but also reduces the likelihood that a terrorist act could be performed with the container.

Coast Guard

The Coast Guard implemented *Operation Neptune Shield*, the maritime portion of *Operation Noble Eagle* on September 12, 2001. *Operation Neptune Shield* is the Service's largest homeland port security operation since World War II. It's comprised of 55 cutters, 42 aircraft, and hundreds of small boats patrolling 361 ports. Rear Admiral Terry M. Cross, Assistant Commandant for Operations, stated 2765 reservists and auxiliary were recalled to assist in port security operations. The goal of *Operation Neptune* is to allow risk-based decision-making to identify high-risk ports, high-risk vessels approaching our ports, and to strategically place Coast Guard resources where greatest threats lie.[19]

The heart of the Coast Guard port security plan is the Sea Marshal program. The Sea Marshal program was established to assign Coast Guardsmen to ride U.S. and foreign High Interest Vessels (HIV) entering port. A HIV is defined as a vessel over 300 Gross Tons:

1. entering a specific port for the first time.
2. having an intelligence hit on a crewmember.
3. coming from a specified list of ports.
4. defined by the Coast Guard Port Captain as a hazardous material carrier.[20]

Ships entering U.S. ports must now provide 96-hour advance notice of arrival to the U. S. Coast Guard along with crew, passenger, and cargo information. Previously, a 24-hour advance notice of arrival was standard. The longer advanced notice allows the Coast Guard and other U.S. law enforcement agencies time to review the information prior to arrival. The Coast Guard established the National Vessel Movement Center (NVMC) in Martinsburg, West Virginia, to track all vessels over 300 Gross Tons arriving or departing U.S. seaports. Previously, no national tracking system was in place and individual Coast Guard Port Captains of seaports were inconsistently notified.[21]

When a HIV is clear to enter port and within U.S. territorial waters a Sea Marshal and Safety and Security Team (SST) boards. The SSTs are comprised of specially trained Coast Guard law enforcement

officers from the Coast Guard Tactical Law Enforcement Team. The team performs an inspection following the requirements of the International Maritime Organization. Any deficiencies must be corrected prior to entering port. When the Sea Marshal approves final port entry, the SST station themselves in critical locations throughout the ship to insure ship operations are not hampered. The Sea Marshal will station in the pilothouse with SST members in the aft steering station and engine room.[22] A Coast Guard vessel establishes a security area around the ship as it transits through the port. The Sea Marshal and SST debark when the ship is moored. For ships carrying hazardous cargo, a Sea Marshal and a Safety and Security Team may be deployed for the outbound trip.[23]

In larger U.S. ports like Boston, New York/Jersey City, Los Angeles, and Long Beach, Maritime Security Squadrons (MSS) are deployed to assist the Sea Marshals and SSTs.[24] A MSS is comprised of 1 Medium Endurance Cutter (270ft), 2 Patrol Boats (110ft), and 1 Cyclone Class Patrol Craft. The Cyclone Class Patrol Craft are manned and operated by Navy crews with Coast Guard onboard to conduct law enforcement duties.[25]

Commander Chris Doane, director of *Operation Neptune*, Coast Guard Atlantic Command, stated it is important to level the playing field while applying the new security regime. If one Coast Guard Port Captain applies the new rules differently than another, one port may have an unfair trade advantage. These new security practices reinforce interagency cooperation, improve command and control, and use intelligence to screen vessels, cargo, and crew.

Customs

The new strategy of the U.S. Customs Service is to ensure proper security for cargo *before* it enters U.S. seaports. This will lessen the risk that a container will be used to deliver and detonate a weapon of mass destruction prior to entry inspections. Customs is pursuing this "beyond the border" security strategy in four ways; Customs-Trade Partnership Against Terrorism (C-TPAT), International Customs Zones (ICZ), Non-Intrusive Inspection Technology, and cargo-related intelligence databases.[26]

C-TPAT works with industry to improve security from factory to buyer similar to TAPA. Customs recognized that they couldn't provide the highest level of security while allowing the smooth flow of commerce without involving the shippers. In return, Customs would give "fast-track" status to containers meeting C-TPAT requirements.[27]

Customs is also seeking to establish International Customs Zones (ICZ) at major seaports around the world. ICZs would permit the same law enforcement authority to the U.S. Customs Service (power to question, search, and arrest) as if operating on U.S. soil. ICZs are to be established in Canada first followed by other countries with major seaports.[28]

Customs is also pursuing the installation of Non-Intrusive Inspection (NII) technology at foreign "mega-ports" such as Singapore and Rotterdam. In a speech to the Center for Strategic International Studies, U.S. Customs Commissioner Robert Bonner proposed the world's 10 biggest ports x-ray and electronically seal containers bound for the U.S. to circumvent potential terrorist threats. He painted a devastating picture of the end of container trade should a cargo box be used in a nuclear detonation. In return, he said the U.S. would tighten screening of U.S. exports, share technology and intelligence information, and "fast-track" cargo from shippers with airtight supply chains.[29]

The initiatives discussed above may take months or years to establish. In the meantime, Customs must accurately segregate "high-risk" containers warranting greater scrutiny from "low-risk" ones worthy of quick entry. Customs is doing this by screening incoming shipments with their Automated Commercial Environment. By "profiling" containers based on cargo and point of origin, Customs can make an educated guess on the containers that require inspection. The "high-risk" containers are then scanned by the VACIS system.[30] The Vehicle and Cargo Inspection System is a truck-mounted or permanently installed gamma-ray imaging system designed to non-intrusively inspect the contents of trucks, containers, cargo, and passenger vehicles for explosive devices and/or contraband. VACIS can scan two TEUs in one to three minutes. Customs has 29 units already installed at major U.S. seaports.[31]

Conclusion

> *The key is to meet the challenges of the 21st century and yet preserve globalization. To be a flexible border agency capable of working both at and beyond the border in its effort to protect America.*
>
> —U.S. Customs Strategy Memorandum

The U.S. Government finds itself in the unenviable position of balancing seaport security with U.S. economic viability. U.S. Customs Commissioner Robert Bonner hit the mark when saying that no country could afford a terrorist event using the container industry as its vehicle.[32] This scenario should be used as the impetus to make sweeping changes in worldwide shipping security.

Each agency charged with seaport security is making significant changes in their everyday security posture. The U.S. Customs Service has the proper long-term vision for container safeguards. International Customs Zones and the Customs-Trade Partnership Against Terrorism put the first line of defense overseas. Combined with these initiatives, a *worldwide* shipping database similar to the Customs Service's Automated Commercial Environment should be developed. The database would allow all nations to track goods from factory to buyer, anywhere in the world.

The new Coast Guard safeguards do well to defend against unsafe ships and rogue crews. But what the Coast Guard lacks is a worldwide maritime tracking system. Through the International Maritime Organization, the Coast Guard should require all transoceanic ships to have a Global Positioning System transponder similar to the ones used by the Federal Aviation Administration. The transponder would allow continuous tracking of all ocean-going ships and facilitate long-term surveillance. Knowing the seaports visited by a liner would give insight into possible terrorist activity.

Although little information was available on the physical security provided by the Port Authority Police Forces, strict border security and worker identification cards would reduce the number of unauthorized personnel on the docks.

Our seaports and intermodal transportation systems are strategic assets. Although not in the national news, I believe they are receiving the attention necessary to address their vulnerabilities. In the globalized world we live in, our seaport's protection will rely on our trading partners to combat economic terrorism.

Notes

1. Jon S. Helmick, "Intermodal Ports and Liner Shipping: A 21st Century Status Report," *Logistics Spectrum* 35, January-March 2001, 20.

2. Ibid., 2.

3. U.S. Customs Service, Importing and Exporting. On-line, Internet, January 2002, available from http://www.customs.ustreas.gov/impoexpo/impoexpo.htm.

4. Al Baker, John Sullivan, "Port of Entry Now Means Point of Anxiety," *New York Times,* Sunday, 23 December 2001, late edition (east coast), sec. B1.

5. Ibid.

6. Alarik Fritz, et al. *Navy Role in Homeland Defense Against Asymmetric Threats Volume One: Summary Report,* CNA Report CRM D0002158.A2. (Alexandria, Virginia: CNA, September 2001), 24.

7. Alarik Fritz, et al. *Navy Role in Homeland Defense Against Asymmetric Threats Volume Two: Appendices* CNA Report CRM D0002159.A2. (Alexandria, Virginia: CNA, September 2001), 47.

8. August Gribbin, "Seaports Seen as Terrorist Target," *Washington Times*, Monday, 22 January 2002, 1.

9. Adam Aston, John Cady, "Pandora's Cargo Boxes," *Business Week*, 22 October 2001, 48.

10. Al Baker, John Sullivan, "Port of Entry Now Means Point of Anxiety," *New York Times,* Sunday, 23 December 2001, late edition (east coast), sec. B1.

11. August Gribbin, "Seaports Seen as Terrorist Target," *Washington Times*, Monday, 22 January 2002, 1.

12. Quoted in Alarik Fritz, et al. *Navy Role in Homeland Defense Against Asymmetric Threats Volume Two: Appendices* CNA Report CRM D0002159.A2. (Alexandria, Virginia: CNA, September 2001), 18.

13. Ibid., 16.

14. U.S. Customs Service, Importing and Exporting. On-line, Internet, January 2002, available from http://www.customs.ustreas.gov/impoexpo/impoexpo.htm.

15. Port Authority of New York and New Jersey, *Port Commerce*. On-line, Internet, February 2002, available from http://www.panynj.gov/commerce/marframe.HTM.

16. Al Baker, John Sullivan, "Port of Entry Now Means Point of Anxiety," *New York Times,* Sunday, 23 December 2001, late edition (east coast), sec. B1.

17. Technology Asset Protection Association, *The Organization,* on-line, Internet, January 2002, available from http://www.tapaonline.org/organization.htm.

18. Al Baker, John Sullivan, "Port of Entry Now Means Point of Anxiety," *New York Times,* Sunday, 23 December 2001, late edition (east coast), sec. B1.

19. U.S. Coast Guard, Homeland Security. On-line, Internet, January 2002, available from http://www.uscg.mil/overview/Homeland%20Security2.htm.

20. CDR Chris Doane, Director, Homeland Security, U.S. Coast Guard Atlantic Command, interviewed by author, 25 January 2002.

21. U.S. Coast Guard, Homeland Security. On-line, Internet, January 2002, available from http://www.uscg.mil/overview/Homeland%20Security2.htm.

22. CDR Chris Doane, Director, Homeland Security, U.S. Coast Guard Atlantic Command, interviewed by author, 25 January 2002.

23. U.S. Coast Guard, Homeland Security. On-line, Internet, January 2002, available from http://www.uscg.mil/overview/Homeland%20Security2.htm.

24. Ibid.

25. CDR Chris Doane, Director, Homeland Security, U.S. Coast Guard Atlantic Command, interviewed by author, 25 January 2002.

26. U.S. Customs Service, draft memorandum, submitted by: U.S. Customs Service, Treasury Office of Enforcement, subject: Strategic Objectives.

27. U.S. Customs Service, Importing and Exporting. On-line, Internet, January 2002, available from http://www.customs.ustreas.gov/impoexpo/impoexpo.htm.

28. U.S. Customs Service, draft memorandum, submitted by: U.S. Customs Service, Treasury Office of Enforcement, subject: Strategic Objectives.

29. Beth Jinks, "MPA Backs Call to X-Ray Transhipments," *The Shipping Times*, January 2002, n.p., on-line, Internet, 29 January 2002, available from http://business-times.asia1.com.sg/shippingtimes/story/0,2276,34218,00.html?.

30. CDR Chris Doane, Director, Homeland Security, U.S. Coast Guard Atlantic Command, interviewed by author, 25 January 2002.

31. Science Applications International Corporation, *Safety and Security*, on-line, Internet, January 2002, available from http://www.saic.com/products/security/.

32. Beth Jinks, "MPA Backs Call to X-Ray Transhipments," *The Shipping Times*, January 2002, n.p., on-line, Internet, 29 January 2002, available from http://business-times.asia1.com.sg/shippingtimes/story/0,2276,34218,00.html?.