MILITARY LAW REVIEW

Volume 185 **Fall 2005**

PROTECTING U.S. PORTS WITH LAYERED SECURITY MEASURES FOR CONTAINER SHIPS

LIEUTENANT COMMANDER (SEL) RACHAEL B. BRALLIAR*

When it comes to dealing with the new security agenda, Americans need to grow up. We cannot afford to act as though 9/11 was just a freak event. Nor can we expect our government to secure a permanent victory in a war on terrorism . . . Terrorism is simply too cheap, too available, and too tempting ever to be totally eradicated. We must have the maturity both to live with the risk of future attacks and to invest in reasonable measures to rein in that risk. In other words, the best we can do is to keep terrorism within manageable proportions.[1]

---

* Judge Advocate, U.S. Coast Guard. Presently assigned as Advanced Operational Law Studies Fellow, Center for Law and Military Operations, The Judge Advocate General's Legal Center & School, U.S. Army, Charlottesville, Virginia. LL.M. 2005, The Judge Advocate General's School, Charlottesville, Virginia; J.D. 1997, Case Western Reserve University School of Law; B.A., 1993, Bryn Mawr College. Previous assignments include Legal Assistance Attorney, Legal Assistance Branch, Maintenance & Logistics Command Pacific, Alameda, California, 2003-2004; Claims Settlement Attorney, Claims and Litigation Branch, Maintenance & Logistics Command Pacific, Alameda, California, 2001-2003; Trial Counsel, Military Justice Branch, Maintenance & Logistics Command Pacific, Alameda, California, 1999-2001. Member of the bars of Ohio, California, the United States Court of Appeals for the Sixth Circuit, the United States District Court for the Northern District of Ohio, and the Supreme Court of the United States, and certified under Article 27(b) of the Uniform Code of Military Justice to perform as a Judge Advocate General of the Coast Guard. The author gives special thanks to the following individuals for their suggestions and support throughout the drafting of this article: Lieutenant Commander Robert J. Hunt, U.S. Navy, Associate Professor of International and Operational Law, The Army Judge Advocate General's Legal Center and School; Dr. Stephen E. Flynn, Jeane J. Kirkpatrick Senior Fellow for National Security Studies at the Council on Foreign Relations; and Lieutenant Commander Michael T. Cunningham, U.S. Coast Guard, Legal Counsel, U.S. Coast Guard Port Security Directorate.

[1] STEPHEN FLYNN, AMERICA THE VULNERABLE: HOW OUR GOVERNMENT IS FAILING TO PROTECT US FROM TERRORISM 59 (2004).

I. Introduction

The maritime transportation system presents tremendous opportunities for terrorists to attack the United States of America. One of the greatest threats to U.S. security is the maritime transportation system—the approximately 25,000[2] shipping containers (containers) that enter U.S. ports each day, and then infiltrate the mainland via railways, highways, interstates, and residential roads.[3] The consequences of a breach in the security of a single container have the potential to dwarf the devastation felt after the 11 September 2001 terrorist attacks (9/11) in a number of ways. For instance, the detonation of a single nuclear or radiological device smuggled on a container would have a far greater impact upon both global trade and the global economy than did the 9/11 attacks.[4] Not only could a port security breach cause mass casualties, but it would necessitate closing U.S. maritime import and export systems, causing maritime trade gridlock, economic collapse of many businesses, and possibly leading to economic losses of $1 trillion.[5] By contrast, the

---

[2] *See* Robert C. Bonner, Commissioner of the U.S. Customs and Border Protection, Speech at the Fourth Annual International Conference on Public Safety: Technology & Counterterrorism (Mar. 14, 2005) (stating that 25,000 containers arrive in U.S. ports each day and that nine million containers arrive in U.S. ports annually); *cf.* GARY HART ET AL., AMERICA STILL UNPREPARED—AMERICA STILL IN DANGER: REPORT OF AN INDEPENDENT TASK FORCE SPONSORED BY THE COUNCIL ON FOREIGN RELATIONS 8 (2002) (estimating in 2001 that 21,000 containers arrived in U.S. ports every day).

[3] *See* JOHN F. FRITTELLI, CONGRESSIONAL RESEARCH SERVICE REPORT FOR CONGRESS, PORT AND MARITIME SECURITY: BACKGROUND AND ISSUES FOR CONGRESS 3 (updated May 27, 2005). This article references only unclassified information. The Maritime Administration, U.S. Coast Guard, Customs and Border Protection, and Transportation Security Administration are part of the Container Working Group which generated classified recommendations on how best to ensure the security of marine container transportation. *Id*. at 12.

[4] *See* Robert C. Bonner, Commissioner of the U.S. Customs and Border Protection, Speech before the Center for Strategic and International Studies (Jan. 17, 2002), *at* http://www.cbp.gov/xp/cgov/newsroom/commissioner/speeches_statements/archives/2002 [hereinafter Bonner Speech].

[5] *See* MICHAEL E. O'HANLON, PROTECTING THE AMERICAN HOMELAND: A PRELIMINARY ANALYSIS 7 (Brookings Institution Press) (2002) (explaining that a maritime security breach would impact the American economy by drastically increasing the prices of imported goods, devastating cities and seaports that depend upon container trade, and destroying businesses which would trigger mass layoffs; "[i]ndeed, the layoffs of airport workers at Reagan National Airport after Sept. 11 would seem tiny compared to the layoffs associated with even a temporary shutdown of global trade"); *see also* Bonner Speech, *supra* note 4.

attacks on 9/11 claimed more than 3,000 lives, and led to the loss of approximately $100 billion.[6]

Part II of this article provides readers with a greater understanding of the multi-tiered domestic and international threat that container ships present to the United States. Additionally, Part II discusses the feasibility of a terrorist exploiting such weaknesses. Drawing upon the vulnerabilities assessed in Part II, Part III presents an overview of the potential consequences resulting from a terrorist act involving a single container.

Based on the multi-tiered threat posed by container ships, experts agree that the best defense is a layered defense with coordinated security measures overseas and nationally.[7] Congress and international organizations continue to work to improve the security of maritime transportation post-9/11, with mixed success. As Congress recognizes "[p]ort security legislation can have significant implications for public safety, the war on terrorism, the U.S. and global economy, and federal, state, and local homeland security responsibilities and expenditures."[8]

While Part III discusses the need for a layered defense in securing container ships, Part IV introduces the international players involved in securing the maritime transportation system. Specifically, Part IV focuses on the International Ship and Port Facility Security Code (ISPS

---

[6] O'HANLON, *supra* note 5, at 1.

[7] *See, e.g.*, CENTER FOR INT'L SECURITY & COOPERATION, THE STANFORD STUDY GROUP, CONTAINER SECURITY REPORT 5 (Jan. 2003) [hereinafter CISAC THE STANFORD STUDY GROUP]; FRITTELLI, *supra* note 3, at 18; FLYNN, *supra* note 1, at 69, 105; Customs-Trade Partnership Against Terrorism (C-TPAT), *C-TPAT Fact Sheet and Frequently Asked Questions*, *at* http://www.cbp.gov/xp/cgov/import/commercial_enforcement/ctpat/ [hereinafter *C-TPAT FAQ*] (last visited Mar. 19, 2005) (recognizing that "Customs can provide the highest level of security only through close cooperation with the ultimate owners of the supply chain, importers, carriers, brokers, warehouse operators and manufacturers"); U.S. GEN. ACCT. OFF., GAO-02-993T, PORT SECURITY: NATION FACES FORMIDABLE CHALLENGES IN MAKING NEW INITIATIVES SUCCESSFUL 4 (2002) [hereinafter PORT SECURITY] (testimony before the Subcommittee on National Security, Veterans Affairs, and International Relations House Committee on Government Reform) (testimony of JayEtta Z. Hecker, Director, Physical Infrastructure Issues); Admiral James M. Loy & Captain Robert G. Ross, *Global Trade, America's Achilles Heel*, DEF. HORIZONS, Feb. 2002, at 3, *available at* http://www.homelandsecurity.org/journal/articles/displayArticle.asp?article=33.

[8] FRITTELLI, *supra* note 3, at 1.

Code),[9] which was created post-9/11 to preserve the integrity of international maritime trade. In addition, Part IV analyzes the ISPS Code to determine if its security measures protect against the threats presented by container ships.

Part V approaches container security from the domestic realm, focusing on the distinct, yet inter-related, roles of the U.S. Coast Guard, the U.S. Customs and Border Protection, and the Transportation Security Administration. Many of the domestic initiatives of the United States are modeled after or initiated to implement international law. In particular, the Maritime Transportation Security Act of 2002 (MTSA)[10] implements the ISPS Code. Part V discusses the MTSA in detail and analyzes its effectiveness in creating layered security measures for container ships in conjunction with the Customs-Trade Partnership Against Terrorism (C-TPAT),[11] and its companion program, the Container Security Initiative (CSI).[12] While each of these domestic measures is separate, they function together to provide defensive layers in container ship security: the MTSA deals with security requirements for vessels and port facilities; the C-TPAT deals with the supply chain for goods loaded onto container ships; and the CSI deals with the containers.

Parts IV and V are designed to explain the layered defense in place to protect the United States from the threat of container ships and to show where the vulnerabilities discussed in Part III persist. Regulation of the international maritime transportation system requires a delicate balance between simultaneously protecting the United States and avoiding too many impediments to the flow of maritime commerce. Unfortunately, the international and domestic laws and initiatives do not

---

[9] International Ship and Port Facility Security Code, SOLAS/CONF.5/34, annex 1 (Dec. 12, 2002) [hereinafter ISPS Code] (providing Resolution 2 of the Dec. 2002 conference containing the ISPS Code). The ISPS Code is implemented through chapter XI-2 of the International Convention for the Safety of Life at Sea (SOLAS). *See* International Convention for the Safety of Life at Sea, Nov. 1, 1974, 32 U.S.T. 47, 1184 U.N.T.S. 276 [hereinafter SOLAS].

[10] Senator Hollings introduced The Maritime Transportation Security Act of 2002 in S. 1214 on 20 July 2001. Maritime Transportation Security Act of 2002, 46 U.S.C.S. §§ 70101-117 (LEXIS 2005). *See* FRITTELLI, *supra* note 3, at 1-2 (stating that the MTSA is attempting to strengthen U.S. port security).

[11] *C-TPAT FAQ*, *supra* note 7. A copy of a Voluntary Agreement to Participate in C-TPAT is *available at* http://www.cbp.gov/xp/cgov/import/commercial_enforcement/ctpat/sea_carriers/sea_carrier_voluntary.xml (last visited Mar. 20, 2005).

[12] Bonner Speech, *supra* note 4 (proposing the Container Security Initiative, which was then referred to as the "Container Security Strategy").

adequately address the threats posed by the voluminous contents of the 25,000 containers that enter U.S. ports each day. Individually, and collectively, the security layers are unable to confirm whether goods loaded on containers are legitimate and remain uncompromised during transit.[13]

While international and domestic laws attempt to focus on enhancing maritime security, they do not provide adequate protections against foreseeable security breaches. As a partial remedy, Part VI recommends the further development of detection devices imbedded within containers to address the remaining gaps in container ship security. According to the report of an independent task force sponsored by the Council on Foreign Relations, "we can transform the calculations of would-be terrorists by elevating the risk that (1) an attack on the United States will fail, and (2) the disruptive consequences of a successful attack will be minimal."[14] The development and implementation of smart, tamper-resistant containers with internal detection devices may be a viable and cost-effective final layer in container ship security.

II. Vulnerability of the Maritime Transportation System in the United States and Abroad

Investigations following the attacks on 9/11 highlight continuing concern over the security of the maritime transportation system and, in particular, container ships. Several reports indicate that al Qaeda either owns or controls approximately fifteen cargo ships.[15] Reports also state

---

[13] *See* FLYNN, *supra* note 1, at 107.

[14] HART, *supra* note 2, at 8.

[15] *See, e.g.*, RONALD O'ROURKE, CONGRESSIONAL RESEARCH SERVICE REPORT FOR CONGRESS, HOMELAND SECURITY: NAVY OPERATIONS—BACKGROUND AND ISSUES FOR CONGRESS 4 (updated May 17, 2004); John Mintz, *15 Freighters Believed to Be Linked to Al Qaeda*, WASH. POST, Dec. 31, 2002, *available at* http://www.washingtonpost.com/ac2/wpdyn?pagename=article&node=&contentId=A56442-2002Dec30&notFound=true (stating that "approximately 15 cargo freighters around the world that they believe are controlled by al Qaeda or could be used by the terrorist network to ferry operatives, bombs, money or commodities over the high seas, government officials said."); William K. Rashbaum & Benjamin Weiser, *A Tramp Freighter's Money Trail to bin Laden*, N.Y. TIMES, Dec. 27, 2001, *available at* http://query.nytimes.com/gst/abstract.html?res=F30810FD3B550C748EDDAB0994D9404482/. While this link may require the reader to subscribe to view the article, the same article is available without registration at http://news.pseka.net/index.php?module=article&id=135&PHPSESSID=46eca01da7d32

that al Qaeda terrorists may have smuggled themselves into foreign ports over long distances on ships.[16]

According to U.S. officials cited in a Washington Post article, al Qaeda's leader, Osama bin Laden, and his aides have owned ships for years.[17] More specifically, a New York Times article published three months after the 9/11 attacks reported that "[a]l Qaeda is now said to control at least 20 ships."[18] The same article pointed out a possible link between the tramp freighter Seastar, allegedly operated by al Qaeda, and a car bomb in Riyadh that killed several people, including five U.S. government employees in November 1995, which bin Laden extolled as "praiseworthy terrorism."[19] Likewise, officials purportedly found a startling link between one of bin Laden's ships and the explosives delivered to al Qaeda operatives and used in the 1998 bombing of two American embassies in Africa.[20] In addition, an article in the Washington Post reported an incident in February 2002 when eight Pakistani men jumped off of a freighter at an Italian port after a trip from Cairo.[21] According to the report, U.S. officials determined that the men were sent by al Qaeda and gained access to the freighter by fabricating their status as crewmen and using false documents.[22] Reports cite other incidents involving alleged crew members onboard vessels bound for foreign ports who knew nothing about seafaring. Upon further investigation, authorities discovered that these individuals had large volumes of cash, false documents, intricate maps of port cities, and evidence tying them to al Qaeda in Europe.[23] The threat of al Qaeda or other terrorist operatives is a reality, and the U.S. maritime transportation system's susceptibility makes it a ripe target.

---

a265f98dacd99f2f2c00; J. Ashley Roach, United States Initiatives to Enhance Maritime Security at Sea, Address at The Regime of the Exclusive Economic Zone: Issues and Reponses to the Tokyo Round in Tokyo, Japan 1 (Feb. 20, 2003).

[16] O'ROURKE, *supra* note 15, at 4 (discussing that al Qaeda may have used ships to invade foreign countries but failing to identify where the terrorists allegedly alighted).

[17] *See* Mintz, *supra* note 15.

[18] Rashbaum & Weiser, *supra* note 15.

[19] *Id.*

[20] *See* Mintz, *supra* note 15.

[21] *See id.*

[22] *See id.*

[23] *See id.*

Although international boundaries of the United States include its 361 public ports,[24] ports do not provide actual borders in the traditional sense. Instead, ports and borders function as a check-point in the infiltration of people and foreign goods onto the mainland. As Robert C. Bonner,[25] the Commissioner of the U.S. Customs and Border Protection, explained to the Senate Committee on Commerce, Science, and Transportation several months after the attacks on 9/11:

> We can no longer afford to think of "the border" merely as a physical line separating one nation from another. We must also now think of it in terms of the actions we can undertake with private industry and with our foreign partners to pre-screen people and goods before they reach the U.S. The ultimate aims of "pushing the border outward" are to allow U.S. Customs more time to react to potential threats—to stop threats before they reach us—and to expedite the flow of low-risk commerce across our borders.[26]

The attacks on 9/11 "highlighted the fact that our borders offer no effective barrier to terrorists [who are] intent on bringing their war to our soil."[27] The vulnerability of domestic ports and vessels is inextricably linked to the function of the ports and the tremendously fast-paced economy of the United States, as detailed below.

A. The Breadth of Maritime Transportation in the United States

United States ports, which include domestic ports located within the interior of the United States, deal with more than ninety-five percent of overseas trade domestically.[28] While ninety percent of the cargo tonnage

---

[24] *See* Maritime Transportation Security Act of 2002, H.R. 777, 107th Cong. § 101 (2002) (codified at 46 U.S.C.S. §§ 70101-70117 (LEXIS 2005)) (finding that "there are 361 public ports in the United States that are an integral part of our Nation's commerce").

[25] A biography of Commissioner Bonner is *available at* http://www.dhs.gov/dhspublic/interapp/biography/biography_0070.xml (last visited Sept. 8, 2005).

[26] Robert C. Bonner, Commissioner of the U.S. Customs and Border Protection, Statement at the Hearing on Security at U.S. Seaports, Senate Committee on Commerce, Science, and Transportation (Feb. 19, 2002) *available at* http://commerce.senate.gov/hearings/021902bonner.pdf. (last visited Mar. 20, 2005).

[27] FLYNN, *supra* note 1, at x.

[28] *See* Maritime Transportation Security Act of 2002, Pub. L. No. 107-295, tit. I, § 101, 116 Stat. 2064, 2066 (codified at 46 U.S.C.S. §§ 70101-117 (LEXIS 2005)) (listing

passing through domestic ports occurs in the top fifty U.S. ports, twenty-five U.S. ports process nearly ninety-eight percent of all container shipments.[29] Furthermore, "[t]he total volume of goods imported and exported through ports is expected to more than double over the next 20 years."[30] Additionally, ships carry more than ninety-five percent of the nation's "non-North American trade by weight and 75% by value. Trade now accounts for 25% of the U.S. Gross Domestic Product (GDP)."[31] Given the potential impact of a terrorist attack targeted against domestic ports, the United States has a fundamental interest in maintaining "a free flow of interstate and foreign commerce and . . . ensur[ing] the efficient movement of cargo."[32]

Within the 361 U.S. ports, there are more than 3,700 terminals for cargo and passengers, as well as over 1,000 harbor channels that extend throughout the coastline.[33] As such, U.S. ports are particularly vulnerable to breaches in security, and "may present weaknesses in the ability of the United States to realize its national security objectives; and may serve as a vector or target for terrorist attacks aimed at the United States."[34] Although the United States is the leading maritime trading nation, accounting for approximately twenty percent of the annual world ocean-borne overseas trade, the international community also has a substantial interest in protecting the maritime transportation system because ships transport "approximately 80% of world trade by volume."[35] By analyzing the tremendous economic link between the

---

Congressional findings); *see also* E-mail from Dr. Stephen E. Flynn, Jeane J. Kirkpatrick Senior Fellow for National Security Studies, Council on Foreign Relations, to author (May 31, 2005) (on file with author) [hereinafter Flynn E-mail].

[29] *See* Maritime Transportation Security Act of 2002 § 101 (listing congressional findings).

[30] *Id.* (listing congressional findings); *see* H.R. REP. No. 107-777, at 4.

[31] FRITTELLI, *supra* note 3, at 3.

[32] *Id.*; Maritime Transportation Security Act of 2002 § 101 (listing congressional findings).

[33] *See* U.S. DEP'T OF TRANSP., MAR. ADMIN., AN ASSESSMENT OF THE U.S. MARINE TRANSPORTATION SYSTEM 1 (Sept. 1999), *available at* http://www.marad.dot.gov/publications/MTSreport/ [hereinafter ASSESSMENT OF MARINE TRANSPORTATION].

[34] Maritime Transportation Security Act of 2002 § 101 (listing congressional findings); *see* Sean D. Murphy, *Contemporary Practice of the United States Relating to International Law: International Oceans, Environment, Health, and Aviation Law: Establishment of U.S. Antiterrorism Maritime Transportation System*, 98 AM. J. INT'L L. 588, 588 (2004**)**.

[35] FRITTELLI, *supra* note 3, at 3 (citing United Nations Conference on Trade and Development (UNCTAD), *Review of Maritime Transport 2002*).

maritime system and global economy, it is easy to envision the potential impact of terrorist activities, both domestically and internationally.[36]

B. The Foreign Element

The prevalence of foreign vessels in domestic ports contributes to the tremendous vulnerability of the United States, thereby making U.S. ports particularly susceptible to attack. Of the nearly 5,400 commercial ships that entered U.S. ports during approximately 60,000 port calls in 2001, most of the ships were owned and crewed by foreigners.[37] In fact, "less than 3% of U.S. overseas trade is carried on U.S.-flag vessels."[38] The prevalence of foreign vessels and crews creates a plethora of security concerns for U.S. ports due, in large part, to the lack of control that the United States has over the people and contents aboard the vessels. The opened and exposed nature of domestic ports, coupled with the vast foreign component to the shipping industry, makes ports "susceptible to large scale acts of terrorism that could cause a large loss of life or economic disruption."[39]

1. Difficulty of Tracking Suspect Vessels and Crewmembers

While container ships have their own set of unique vulnerabilities, they also face many of the same security issues as other international seaborne systems. For example, vessels are difficult to track because they "are continually given new fictitious names, repainted or re-registered using invented corporate owners, all while plying the oceans."[40] The crew loading the vessels are often unknown, which brings into question "what cargo is loaded onto ships entering U.S. waters?"[41] Moreover, the individuals on board foreign container ships are often unaccounted for, or may possess false documentation.[42]

---

[36] *See infra* Part III.A.

[37] *See* JOHN F. FRITTELLI, CONGRESSIONAL RESEARCH SERVICE REPORT FOR CONGRESS, MARITIME SECURITY: OVERVIEW OF ISSUES 2 (updated Feb. 24, 2003); *see also* Bruce Stubbs, *The Maritime Component*, SEA POWER 44:32-36 (Aug. 2001).

[38] FRITTELLI, *supra* note 37, at 2; *see* FRITTELLI, *supra* note 3, at 2 (citing Stubbs, *supra* note 37).

[39] Maritime Transportation Security Act of 2002 § 101 (listing congressional findings); *see* Murphy, *supra* note 34, at 588.

[40] Mintz, *supra* note 15.

[41] *Id.*

[42] *See id.*

2. Threats of Piracy in Foreign Ports and During Transit

Although containers are subject to security breaches during the loading phase, they may experience additional potential security breaches while transiting overseas. Maritime container ships run the risk of piracy during transit. The number of reported piracy attacks on cargo ships tripled during the 1990s.[43] Most of the attacks took place when the ships were in port and "in Southeast Asian waters on foreign-flag freighters."[44] Significantly, there may be a link between piracy and terrorism. Experts propose that piracy may be intended to fund or promote terrorist operations.[45] For example, the *Financial Times* reported an incident where pirates boarded a chemical tanker in the south Pacific and steered the vessel at varying speeds for several hours.[46] The purpose behind these maneuvers is unclear, yet they bear an eerie resemblance to the attacks on 9/11, where hijackers had flying experience, but little experience landing aircraft.[47] As we learned from those attacks, terrorists can be creative in choosing their weapons. It is conceivable that terrorists could use a chemical tanker or a container ship carrying flammable components or weapons of mass destruction in a similar fashion—by colliding into a bridge or busy port and causing mass casualties and collateral damage.[48]

C. Unique Threats Posed by Container Ships

The volume and multiple sources providing cargo in maritime containers transported overseas, as well as the potential anonymity of such contents, make containers and container ships easy targets for terrorists. These vulnerabilities make containers and container ships unique security threats. Commissioner Bonner recently described containers as "potential Trojan horses of the 21st century."[49]

---

[43] FRITTELLI, *supra* note 3, at 7 (citing U.S. DOT, Surface Transportation Security: Vulnerabilities and Developing Solutions, n.d., n.p.).
[44] *Id.*
[45] *See id.*
[46] Mansoor Ijaz, *The Maritime Threat from Al Qaeda*, FIN. TIMES, Oct. 20, 2003, *available at* http://www.benadorassociates.com/pf.php?id=636.
[47] HART, *supra* note 2, at 10.
[48] *See* Mintz, *supra* note 15 (presenting a frightening scenario in which terrorists pose as crewmen and "commandeer a freighter carrying dangerous chemicals and slam it into a harbor").
[49] Bonner, *supra* note 2.

1. The Many Sources Providing Goods in Containers

A container ship differs from a common cargo vessel because it transports marine containers laden with a variety of goods.[50] A single container ship may carry more than 3,000, and sometimes upwards of 6000, containers "of which several hundred might be offloaded at a given port."[51] The average container traverses seventeen intermediate points before arriving at its final U.S. destination, and its contents often include goods obtained from several locations even before the container was loaded.[52] As Dr. Stephen E. Flynn, a retired Coast Guard Commander and the preeminent expert on homeland security and border control,[53] explained:

> Nearly 40 percent of all containers shipped to the United States are the maritime transportation equivalent of the back of a UPS van. Intermediaries known as consolidators gather together goods or packages from a variety of customers or even other intermediaries, and load them all into the container. Just like express carriers in the U.S., they only know what their customers tell them about what they are shipping.[54]

The above analogy extends further because any potential container threat arriving in a U.S. port easily can infiltrate into the mainland.

> [Containers are] similar to a truck trailer without wheels; standard sizes are 8x8x20 feet or 8x8x40 feet. Once offloaded from ships, they are transferred to rail cars or tractor-trailers or barges for inland transportation. Over-the-road weight

---

[50] FRITTELLI, *supra* note 3, at 3, 8.

[51] *Id. But see* Justin S.C. Mellor, *Missing the Boat: The Legal and Practical Problems of the Prevention of Maritime Terrorism*, 18 AM. U. INT'L L. REV. 341, 350-51 (2002) (explaining that the current trend seems to be towards enormous container ships with the capacity to accommodate more than 6,000 containers, but acknowledging that such vessels are limited to large "megaports" equipped to handle their size. These megaports become hubs upon which many other ports rely as a centralized distribution point).

[52] *See* FLYNN, *supra* note 1, at 89.

[53] Dr. Stephen E. Flynn is the Jeane J. Kirkpatrick Senior Fellow for National Security Studies at the Council on Foreign Relations and a retired Commander in the U.S. Coast Guard. A copy of Dr. Flynn's biography is *available at* http://www.cfr.org/bios/3301/stephen_e_flynn.html (last visited Sept. 7, 2005).

[54] FLYNN, *supra* note 1, at 89.

> regulations generally limit the cargo load of a 40 foot container to approximately 45,000 pounds.[55]

Although maritime containers only comprise eleven percent of the annual tonnage of cargo carried into U.S. ports each year "containers account for 66% of the total value of U.S. maritime overseas trade."[56] Furthermore, the Bureau of Transportation Statistics estimated that in the year 2001 over six million cargo containers entered U.S. seaports.[57] Currently, this figure is closer to nine million.[58] To illustrate, if the 25,000 containers that enter U.S. ports daily were loaded on a continuous train end-to-end, that train would extend over 189 miles long each day.[59]

Container ships carry cargo from "hundreds of companies" and, often, the containers are loaded at individual company warehouses located away from the port.[60] Typical individual container shipments involve numerous parties and may "generate 30 to 40 documents."[61] The individuals involved in a straight-forward container shipment "usually include the exporter, the importer, a freight forwarder, a customs broker, a customs inspector, inland transportation provider(s) (which may include more than one trucker or railroad), the port operators, possibly a

---

[55] FRITTELLI, *supra* note 3, at 3.

[56] *Id. But see* HOW DID THIS HAPPEN? TERRORISM AND THE NEW WAR 188 (James F. Hoge, Jr. & Gideon Rose eds., New York: Public Affairs 2001) ("It is also important to keep in mind that not all U.S.-bound containers arrive at U.S. ports. Half of the containers discharged at the Port of Montreal, for instance, move by truck or rail for cities in the northeastern or mid-western United States.").

[57] BUREAU OF TRANSP. STAT., U.S. INT'L TRADE AND FREIGHT TRANSP. TRENDS, Executive Summary (2003), *available at* http://www.bts.gov/publications/us_international_trade_and_freight_transportation_trends/2003/html/executive_summary.html [hereinafter TRADE AND FREIGHT TRENDS] (citing statistics from 2001).

[58] *See* U.S. Customs and Border Protection, *Container Security Initiative Expands Beyond the Megaports, Strengthening Anti-Terror* (2003), *at* http://cbp.gov/xp/cgov/newsroom/press_releases/archives/cbp_press_releases/022003/02212003.xml (providing maritime statistics from 2001); *see also* Bonner, *supra* note 2 (stating that 25,000 containers arrive in U.S. ports each day and that nine million containers arrive in U.S. ports annually); TRADE AND FREIGHT TRENDS, *supra* note 57 (noting that approximately 13 million containers arrive by truck or train from Canada and Mexico)

[59] Interview with Commander William Drelling, U.S. Coast Guard, in San Francisco, Cal. (Mar. 15, 2005) (providing the illustration of the annual containers that enter U.S. ports wrapping around the globe approximately three times). Commander Drelling worked as a Coast Guard Regional Examiner in Long Beach, California prior to the attacks on 9/11. *Id.*

[60] FRITTELLI, *supra* note 3, at 8.

[61] *Id.*

feeder ship, and the ocean carrier."[62] As Congress recognizes, "[e]ach transfer of the container from one party to the next is a point of vulnerability in the supply chain. The security of each transfer facility and the trustworthiness of each company [are] therefore critical in the overall security of the shipment."[63]

2. Unreliability of Container Ship Documents

Each container must have a "cargo manifest" specifying the contents of the container. The U.S. Customs and Border Protection is the federal agency with the principal responsibility for reviewing the information contained on the cargo manifest and determining which containers should be more closely scrutinized.[64] After containers arrive in U.S. ports, they may be unloaded or inspected by x-ray or gamma ray machines.[65] Unfortunately, representations contained in cargo manifests may be inherently unreliable for several reasons. First, the manifests are only as reliable as those who provide them. Second, the contents listed on a cargo manifest may not protect the United States from dangerous materials that may be loaded while the carrier is in foreign ports. Third, the manifests may not protect against tampering with the container contents during transit, or at any other time prior to arriving in U.S. ports.

III. The Potential Consequences of a Security Breach in a Container and the Need for a Layered Defense for Container Ship Security

JayEtta Z. Hecker, the Director of Physical Infrastructure for the General Accounting Office, testified before the Subcommittee on National Security, Veterans Affairs, and International Relations in 2002 that terrorist acts

---

[62] *Id.*

[63] *Id.*

[64] *Id.* at 10 (explaining the role of the CBP). United States Customs and Border Protection is the agency within the Department of Homeland Security that manages, controls, and secures U.S. borders; *see* United States Customs and Border Protection, *Mission: Protecting Our Borders Against Terrorism* [hereinafter CBP Mission], http://www.cbp.gov/xp/cgov/toolbox/about/mission/cbp.xml (last visited May 18, 2005); *see also infra* Part V.

[65] *See* Informed Trade International, *The 5 Percent Myth vs. U.S. Customs and Border Protection Reality*, http://www.itintl.com/articles/US_Customs_5_percent_myth.php (last visited Mar. 20, 2005).

> involving chemical, biological, radiological, or nuclear weapons at one of these seaports could result in extensive loss of lives, property, and business; affect the operations of harbors and the transportation infrastructure (bridges, railroads, and highways) within the port limits; cause extensive environmental damage; and disrupt the free flow of trade.[66]

For example, Congress considered the effects of a simple "dirty bomb"[67] arriving via container ship.[68] Congress concluded that an attack with a dirty bomb would be feasible for terrorist groups, but likely would kill or injure only a few people and would not cause great property damage. Congress, however, acknowledged that the use of a dirty bomb in a seaport could cause "panic and might require closing some areas for an undetermined time."[69] Furthermore, the Council on Foreign Relations elaborates that the effects of a dirty bomb in a U.S. port would "snarl a city" and require closure of the area for cleanup which would last at least several months and, possibly, years.[70] The effect of even a simple dirty bomb "could paralyze a local economy and reinforce public fears about being near a radioactive area."[71]

---

[66] PORT SECURITY, *supra* note 7, at 4 (testimony of JayEtta Z. Hecker).

[67] Both dirty bombs and nuclear weapons are weapons of mass destruction. A dirty bomb, however, is a radiological weapon rather than a nuclear weapon and contains both conventional explosives and radioactive materials. A nuclear weapon is much more sophisticated, involves a complex nuclear-fission reaction, and can be thousands of times more destructive than a dirty bomb. For a detailed explanation of the difference between a dirty bomb and a nuclear weapon, visit the website for the Council on Foreign Relations, http://cfrterrorism.org/weapons/dirtybomb.html (last visited Sept. 7, 2005).

[68] *See* FRITTELLI, *supra* note 3, at 6. In addition to the terrorist activities identified as relevant to container ships, Congress recognized other means by which terrorists could attack the United States through the maritime transportation system: terrorists could seize control of a large commercial cargo ship and crash it into a bridge or refinery located on the waterfront; terrorists could block sea traffic by sinking a large commercial cargo ship in a major shipping channel; terrorists could detonate the fuel of a large ship, causing an in-port explosion; terrorists could attack an oil tanker and disrupt the world oil trade and cause large-scale damage to the environment; terrorists could seize control of a ferry or cruise ship and hold the passengers hostage until demands are met; or terrorists could attack U.S. Navy ships and kill U.S. military personnel, destroy military assets, and attempt to cause radiological releases. *Id.* at 5-6.

[69] JONATHAN MEDALIA, CONGRESSIONAL RESEARCH SERVICE REPORT FOR CONGRESS, TERRORIST NUCLEAR ATTACKS ON SEAPORTS: THREAT AND RESPONSE (updated Jan. 24, 2005).

[70] *See* Council on Foreign Rel., *Terrorism: Questions & Answers*, *at* http://www.cnn.com/SPECIALS/2002/cfr/stories/dirty.bomb/ (last visited Sept. 7, 2005).

[71] *Id.*

A. Economic Impact: Domestically and Worldwide

If commerce is the heart of America, ports are the sustaining arteries. Given the vast shipping component of U.S. economy, it follows that disruption of the maritime transportation system could devastate the country's economy. A terrorist attack on U.S. ports or ships entering domestic ports would necessitate closing ports, at least for a period of time, much like the closed aircraft traffic immediately following the attacks on 9/11. Regardless of the breadth or direct consequence of a maritime terrorist attack or infiltration, widespread port closures would be necessary to assess how the attack or infiltration occurred, decipher whether other ports and foreign vessels have been sabotaged, and create a mode for intervening to protect American people and property.

In January 2002, Commissioner Bonner stated in a speech before the Center for Strategic and International Studies that the detonation of a bomb in a container would gridlock container shipments.[72] He explained that such gridlock would have "devastating" consequences for the global economy, and would bring some countries "whose economies are particularly dependent upon robust sea container transit to the edge of economic collapse."[73] While a mere two-week shutdown of international container traffic by sea would cost billions, container transportation would likely stop for a much longer period of time while governments worldwide "figure[d] out how to build a security system that could find the other deadly needles in the massive haystack of global trade."[74]

Considering the tremendous volume and breadth of cargo coming into U.S. ports, it is easy to see the potentially staggering effect that even a short-term shut down would have upon the country's economy. For example, consider the recent closure of ports on the West Coast during a labor dispute. According to one report, the cost of port closures was roughly "$1 billion per day for the first five days, rising exponentially thereafter."[75] The Brookings Institution[76] estimated in 2002 that the

---

[72] Bonner Speech, *supra* note 4.
[73] *Id.*
[74] *Id.*
[75] HART, *supra* note 2, at 17.
[76] The Brookings Institution is an independent and nonpartisan organization devoted to researching, analyzing, and providing the public education while emphasizing economics, foreign policy, governance, and metropolitan policy. More information on the Brookings Institution and its history as "one of Washington's oldest think tanks" is *available at* http://www.brookings.edu/index/about.htm (last visited Sept. 7, 2005).

shipping of a weapon of mass destruction (WMD) via container ship or postal service could result in damages and disruption of the economy costing up to $1 trillion.[77]

Even absent actual port closures due to terrorist attacks, the effect of delaying transportation due to security concerns and screening processes could have a tremendous impact on the U.S. economy. Admiral James M. Loy,[78] the former Deputy Secretary of Homeland Security, asserts that slowing the efficiency of U.S. maritime transportation would be "economically intolerable."[79] Yet, such consequences would be unavoidable. As Congress recognizes, any enhanced security measure would bring with it costs as well.[80]

While terrorists could smuggle a variety of components for a chemical or biological attack—from sarin gas to smallpox—into the United States via container ships, the primary focus has been upon the possibility of terrorists smuggling nuclear weapons into domestic ports on container ships: "[e]xperts are concerned that if a nuclear weapon in a container aboard a ship in port is detonated, it could not only kill tens of thousands of people and cause massive destruction, but could also paralyze the movement of cargo containers globally, thereby shutting down world trade."[81] Currently, the maritime transportation system lacks adequate security measures to protect container shipments.[82] Therefore, it would be relatively easy for a terrorist to smuggle a WMD, or necessary components, into U.S. ports. For instance, if increased protections are placed on small or infrequently sailed vessels, terrorists could "purchase a known exporter with a long and trustworthy shipping record."[83] Apparently, this is a tactic often employed by drug smugglers to bury their contraband among legitimate cargo.[84] Although the Coast Guard and CBP may be familiar with tactics employed in marine transport of illegal drugs, terrorist container threats are unique in method and impact.[85] Drug smugglers often establish patterns that the Coast

---

[77] O'HANLON, *supra* note 5, at 7.
[78] Biography of Admiral James E. Loy, http://www.whitehouse.gov/government/loy-bio.html (last visited Sept. 7, 2005).
[79] *See* Loy & Ross, *supra* note 7.
[80] FRITTELLI, *supra* note 3, at 4.
[81] *Id.* at 8; *see* Bonner Speech, *supra* note 4.
[82] FLYNN, *supra* note 1, at x.
[83] FRITTELLI, *supra* note 3, at 8.
[84] *See id.*
[85] *See id.*

Guard and CBP can track over time. In contrast, terrorists only need to transport a WMD on a single occasion to achieve their goal.[86] In addition, a single WMD may present a substantially greater risk to the American people and economy than mass infiltration of drugs.[87] As Admiral Loy stated during a recent speech before the Maritime and Port Security Summit in Washington D.C., "[t]errorism is a scourge that is not going away; it is the new reality under which we live . . . And in this struggle, we have to be right hundreds of times a day—the terrorists only once."[88]

B. Military Impact

An attack at a major U.S. port could also hinder deployment of military troops. Thirteen of the seventeen U.S. ports identified by the Departments of Defense and Transportation as "strategic because they are necessary for use by DOD in the event of a major military deployment" are "commercial seaports."[89] The maritime transportation system is necessary for the nation's security because it "support[s] the swift mobilization and sustainment [sic] of America's military."[90] To illustrate, the Government Accountability Office noted that "90 percent of all equipment and supplies for Desert Storm were shipped from U.S. strategic ports using our inland and coastal waterways."[91] It follows that a terrorist attack on any of these strategic ports could restrict mobilization of armed forces to flight capabilities and hinder the delivery of supplies and equipment, thereby causing significant delays.[92]

---

[86] *See id*.
[87] *See id*.
[88] James Loy, Former Deputy Secretary of Homeland Security, Remarks at the Maritime and Port Security Summit in Washington, D.C. (Nov. 16, 2004) (transcript), *available at* http://www.cargosecurityinternational.com/channeldetail.asp?cid=4&caid=3759.
[89] U.S. GEN. ACCT. OFF., GAO-03-15, COMBATING TERRORISM, ACTIONS NEEDED TO IMPROVE FORCE PROTECTION FOR DOD DEPLOYMENTS THROUGH SEAPORTS 5 (2002) [hereinafter GAO COMBATING TERRORISM]; *see* ASSESSMENT OF MARINE TRANSPORTATION, *supra* note 33, at 15.
[90] GAO COMBATING TERRORISM, *supra* note 89, at 5; *see* ASSESSMENT OF MARINE TRANSPORTATION, *supra* note 33, at 14-15.
[91] GAO COMBATING TERRORISM, *supra* note 89, at 5; *see* ASSESSMENT OF MARINE TRANSPORTATION, *supra* note 33, at 14.
[92] *See* GAO COMBATING TERRORISM, *supra* note 89, at 1.

C. Current Measures to Address the Threat Posed by Container Ships

Concern over the vulnerability of U.S. ports and, in particular, the potential sabotage of containers by terrorists, is not new. Even before the attacks of 9/11, U.S. ports were identified as potential conduits for terrorist activities. President Clinton established the Interagency Commission on Crime and Security in U.S. Ports on 27 April 1999 to provide a comprehensive study of crime occurring in U.S. ports and the means by which state and local governments are responding.[93] The Commission found widespread criminal exploitation of the security at ports, particularly prevalent in cargo crimes.[94] The Commission also concluded that there are insufficient controls over access to ports and operations within the ports to protect against criminal activity.[95] In fact, many of the ports lacked basic technical necessities, such as security detection equipment, small boats, cameras, x-ray machines, and vessel tracking devices.[96] While the Commission did not identify ports as high threats for terrorist activities, the report noted that the Federal Bureau of investigation (FBI) recognized the "high vulnerability" of ports for such attacks.[97] Congress concluded that "it is in the best interests of the United States to implement new international instruments that establish such a system [of global maritime security]."[98]

Following the attacks on 9/11, concentration on security at U.S. ports was both expanded and focused.[99] In October 2002, an Independent Task Force sponsored by the Council on Foreign Relations reported that U.S. sea and land transportation are more vulnerable to a terrorist attack

---

[93] Maritime Transportation Security Act of 2002, Pub. L. No. 107-295, tit. I, § 101, 116 Stat. 2064, 2066 (codified at 46 U.S.C.S. §§ 70101-117 (LEXIS 2005)) (containing congressional findings rendered as a result of the Commission).

[94] *Id.*; *see* Murphy, *supra* note 34, at 588.

[95] *See* 46 U.S.C.S. § 70101.

[96] *Id.*

[97] *See id.; see also* PORT SECURITY, *supra* note 7, at 4 (testimony of JayEtta Z. Hecker) (finding that U.S. ports are extremely vulnerable to attacks by terrorists due to the vast size and network of ports, the water and land transfers inherent in port activities, and the large quantity of cargo transferred at U.S. ports); HART, *supra* note 2, at 23.

[98] 46 U.S.C.S. § 70101 (containing congressional findings rendered as a result of the Commission). *See* U.S. COMM'N ON NAT'L SEC., HART-RUDMAN COMM'N RELEASE PHASE III ADDENDUM (2001), *available at* http://govinfo.library.unt.edu/nssg/addendum page.htm (finding that terrorism on U.S. soil is the most likely threat Americans face, and the U.S. government is not organized to counter that threat); *see also* FLYNN, *supra* note 1, at 46.

[99] PORT SECURITY, *supra* note 7, at 4 (finding that U.S. ports are opened and extremely vulnerable to attacks).

than aviation.[100] In addition, the 9/11 Commission Report found that the security of transportation is not "allocated to the greatest risks in a cost effective way" and that "[o]pportunities to do harm are as great, or greater, in maritime or surface transportation [than they are in aviation]. Initiatives to secure shipping containers have just begun."[101] Moreover, the 9/11 Commission Report concludes that the need for screening containers is not commensurate with current technology.[102]

D. Layered Security Measures for Container Ships

In response to recommendations of the 9/11 Commission Report and the Commission on Crime and Security in U.S. Ports, recent domestic and international measures have been put into effect to create "a security-oriented approach to container inspection."[103] The domestic laws and initiatives both implement and go beyond the international requirements. Each of these measures creates a layer in security defense by coordinating a variety of detection opportunities throughout the supply chain. A layered defense requires not only an adequate "[s]ystem design," but also "continued system monitoring . . . given that all static systems and technologies are vulnerable to eventual evasion by a sophisticated enemy."[104] Congress recognizes the following:

> [A]n effective solution for securing maritime trade requires creating an international maritime security regime. This regime would rely not on a single solution, such as increasing the number of container inspections, but rather on a layered approach with multiple lines of defense from the beginning to the final destination of a shipment.[105]

In fact, several sources promote a "layered" approach to maritime security, particularly when dealing with container ships.[106] These layers

---

[100] HART, *supra* note 2, at 23.
[101] NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 391 (2004), *available at* http://www.9-11commission.gov/report/911Report.pdf.
[102] *See id.* at 391-92 (concluding that it will take years to develop effective technology to screen containers).
[103] *Id.* at 391.
[104] FLYNN, *supra* note 1, at 105. *See also C-TPAT FAQ*, *supra* note 7.
[105] FRITTELLI, *supra* note 3, at 18.
[106] *See, e.g.*, FLYNN, *supra* note 1, at 69 (promoting "a security-oriented approach to container inspection . . . structured as a 'layered defense'").

involve international cooperation as well as cooperation among many federal agencies. As detailed above, containers are particularly susceptible to sabotage by terrorists during three key phases: while in foreign ports; during non-ocean portions of transit;[107] and after arriving in U.S. ports.

In order to create an effective layered defense to enhance container security, it is necessary to identify the numerous international, federal, state, and local law enforcement players involved, as well as the port authorities, private sector businesses, organized labor and other port employees who play a role in the collective effort.[108] As Congress acknowledges, "[a] major concern for U.S. policymakers is assigning roles and responsibilities for maritime security among federal agencies, among federal, state, and local agencies, and between government agencies and private industry."[109] Without establishing clearly defined roles and responsibilities of each player, there is a risk of overlapping or duplicating efforts. It is crucial for the maritime trade community to understand how federal agencies work in concert. Failure in this organized effort would undermine the Department of Homeland Security's (DHS) goal of forming a "close partnership with industry" to fight terrorism.[110]

> [T]he permissible failure rate for commercial inspection systems falls short of a tolerable threshold for security. . . . By contrast, the consequences of even a single breach of security involving a nuclear weapon could be catastrophic. Therefore, a more sophisticated strategy is required to fulfill the objective of preventing incidents of nuclear terrorism on U.S. territory.

Id. at 105. *See also* CISAC THE STANFORD STUDY GROUP, *supra* note 7, at 5; FRITTELLI, *supra* note 3, at 18; *C-TPAT FAQ*, *supra* note 7; PORT SECURITY, *supra* note 7, at 4 (testimony of JayEtta Z. Hecker).

[107] *See* Flynn E-mail, *supra* note 28 (explaining that the gap between containers on a ship is only 8-12 inches. Therefore, few containers "are accessible once they are stowed"); *see also* E-mail from Lieutenant Commander Michael T. Cunningham, Legal Counsel for the U.S. Coast Guard Port Security Directorate, to author (May 20, 2005) (on file with author) [hereinafter Cunningham E-mail] (explaining that sabotage during transit would be more feasible during the non-ocean portions of the voyage). It is extremely difficult to tamper with containers, or their contents, after they are loaded on a ship. "It's just so much easier to do something with a container when it's landside." *Id*.

[108] *See* PORT SECURITY, *supra* note 7, at 4 (testimony of JayEtta Z. Hecker).

[109] FRITTELLI, *supra* note 3, at 20.

[110] *See id.*

IV. International Players and Initiatives Involved in the Layered Defense of Container Ship Security

The greatest threat presented by containers is during the foreign port phase because containers loaded onto foreign vessels involve a number of unknown variables: they are loaded in ports generally beyond the control of the United States; they are loaded by foreign workers and crew who may not be subject to U.S. regulations;[111] and, their cargo often is a compilation of goods provided by hundreds of different sources. Effective container security must begin by addressing the overseas network of variables. Therefore, it follows that "[t]he first security perimeter in this 'defense in depth' strategy would be at the overseas point of origin."[112] It is necessary to prevent dangerous items from entering the maritime transportation network at the initial phase, because some of these items, in particular WMD, could be detonated before inspectors in a U.S. port find them.[113]

Nine months after the 9/11 attacks, the International Maritime Organization (IMO) and the World Customs Organization (WCO) were identified as the two main institutions to develop global initiatives for improving maritime security.[114] The United States is a contracting government to both the IMO and the WCO. Because neither the IMO nor the WCO is able to enforce the standards and conventions adopted, individual contracting governments have implementation responsibilities.[115] The United States is also a party to the International Labor Organization (ILO), which adopted a convention to document seafarers and assist in maritime security.[116] The United States, however,

---

[111] *But cf.* Cunningham E-mail, *supra* note 107 (noting that the vast majority of foreign workers or foreign mariners "are trustworthy and law abiding" and that the security issue involves the difficulty in "identifying the ones that are untrustworthy, a problem we have just as much as with U.S. workers").

[112] FRITELLI, *supra* note 3, at 18.

[113] *See id.* at 12, 18.

[114] *See id.* at 12.

[115] *See* Int'l Mar. Org., Frequently Asked Questions, http://www.imo.org/home.asp (select the IMO FAQ link) (last visited Sept. 7, 2005) [hereinafter IMO FAQ] (explaining that the IMO adopts legislation but neither implements nor polices compliance); *see also* WORLD CUSTOMS ORG., ABOUT THE WORLD CUSTOMS ORGANIZATION, *available a*t http://www.wcoomd.org/ie/En/AboutUs/aboutus.html.

[116] INT'L LAB. ORG., SEAFARERS' IDENTITY DOCUMENTS CONVENTION (REVISED), 2003 (NO. 185) (2004), *available at* http://www.ilo.org/public/english/dialogue/sector/papers/maritime/sid0002.pdf [SEAFARERS' IDENTITY DOCUMENTS CONVENTION (REVISED)].

has not ratified the convention.[117] Therefore, the main focus of this section will be on the active roles taken by the IMO and WCO, and a minor mention will be given to the ILO's 2003 Convention revising the Seafarers' Identity Documents Convention of 1958.[118]

A. The International Maritime Organization

The IMO and WCO signed a Memorandum of Understanding in July 2002 to coordinate, among other things, examination of security measures for containers loaded onto ships.[119] The IMO[120] is an agency of the United Nations responsible for designing measures to improve the safety and security of international shipping, and to prevent ships from causing marine pollution.[121] Because the IMO was established to adopt legislation only, it has no implementing or policing authority. Therefore, the responsibility for implementing legislation remains with each government that ratifies the conventions to make them part of national law, and to enforce them at the same level as domestic laws.[122] Despite its 164 member governments, the "IMO has plenty of teeth but some of them don't bite."[123]

The IMO adopted a new version of the International Convention for the Safety of Life at Sea (SOLAS) in 1960.[124] The SOLAS Convention is generally regarded as the most important international treaty dealing with maritime safety and the safety of individual merchant ships.[125] It

---

[117] *Id*.

[118] *See id*.; SEAFARERS' IDENTITY DOCUMENTS CONVENTION (REVISED), *supra* note 116; Hartmut Hesse & Nicolaos L. Charalambous, *New Security Measures for the International Shipping Community*, 3 WMU J. MAR. AFF. 123, 128. This article revisits the seafarer identity issue later. *See also infra* Part V.A.3.a-b.

[119] *See* Hesse & Charalambous, *supra* note 118, at 128.

[120] The IMO's original name, "Inter-Governmental Maritime Consultative Organization" (IMCO), was changed to International Maritime Organization (IMO) in 1982. *See* Int'l Mar. Org., *Introduction to IMO*, http://www.imo.org/home.asp (last visited Mar. 20, 2005).

[121] Committees on marine environmental protection, law, technical co-operation, and facilitation, as well as numerous sub-committees, are responsible for the main technical work of the IMO. *See id.*

[122] *See* Hesse & Charalambous, *supra* note 118, at 131.

[123] IMO FAQ, *supra* note 115 (last visited Sept. 7, 2005) (explaining the various components of the IMO).

[124] *See id.*; *see also* SOLAS, *supra* note 9.

[125] *See* Int'l Mar. Org., *Maritime Security on Agenda as USCG Commandant Visits IMO*, Feb. 17, 2005, http://www.imo.org/Newsroom/mainframe.asp?topic_id+1018&doc_id=

has 155 contracting Governments which account for over ninety-eight percent of the world shipping fleet by tonnage.[126] Afterwards, the IMO turned its focus towards facilitating international maritime traffic, and dealing with the carriage of dangerous goods.[127] Because SOLAS was designed to be reviewed and updated periodically, a new Convention was adopted on 1 November 1974 and entered into force on 25 May 1980. The Safety of Life at Sea was amended on numerous occasions and is commonly referred to as "SOLAS 1974 Convention, as amended."[128] Mandatory security measures adopted in December 2002 include a number of amendments to SOLAS. The most far-reaching of these amendments contains the International Ship and Port Facility Security Code (ISPS Code), which details security-related requirements for Governments, port authorities, and shipping companies.[129]

B. The International Ship and Port Facility Security Code

The ISPS Code is a set of measures adopted by the IMO to enhance the security of both port facilities and individual ships involved in international trade.[130] "The ISPS Code requires ships on international voyages and the port facilities that serve them to conduct a security assessment, develop a security plan, designate security officers, perform training and drills, and take appropriate preventive measures against security incidents."[131] The process leading up to the creation of the ISPS Code warrants brief explanation to provide context for the tremendous breadth of the Code.

In an attempt to address port security concerns post-9/11, the IMO and other international organizations began to develop a new maritime security system with the requisite elements for enhancing global

---

4708 [hereinafter *Maritime Security on Agenda*].

126 *Id.*

127 A detailed discussion of the history of SOLAS is *available at* U.S. Coast Guard, *What is "SOLAS"?* (June 12, 2002), http://www.uscg.mil/hq/g-m/mse4/solas.htm.

128 *See* Int'l Mar. Org., *International Convention for the Safety of Life at Sea (SOLAS), 1974*, at http://www.imo.org/Conventions/contents.asp?topic_id=257 &doc_id=647 (last visited Mar. 20, 2005).

129 *See* The ISPS Code, *supra* note 9.

130 *Id.*

131 Subcomm. on Coast Guard and Mar. Transp., *Hearing on Implementation of the Maritime Transportation Security Act, Background*, *available at* http://www.house.gov/transportation/cgmt/06-09-04/06-09-04memo.html [hereinafter *Hearing on Implementation*] (last visited Mar. 20, 2005).

maritime security.[132] In particular, the IMO Assembly met in London in November 2001 to review and update methods for addressing terrorist threats.[133] Following a week-long diplomatic conference in December 2002, the IMO adopted a series of measures designed to strengthen maritime security and, thereby, prevent potential terrorists from targeting the international shipping industry.[134] Although adopted in December 2002, the ISPS Code did not become operative until 1 July 2004 for the 155 contracting parties to SOLAS.[135] Therefore, IMO member governments had until 1 July 2004 to implement the new regulations.[136]

The overarching goals of the ISPS Code are to establish an international framework between governments and the shipping and port industries to prevent security breaches affecting international trade, and to detect such breaches if they occur.[137] The impact of the ISPS Code is expected to affect the international maritime community as well as the world economy, due to the key role of shipping in trade.[138] Because of the tremendous role that container ships play in international trade, implementation of the ISPS Code is critical in addressing the container security issues identified earlier.[139]

---

[132] *See* FRITTELLI, *supra* note 3, at 12-13; *see also* Murphy, *supra* note 34, at 588.

[133] *See* INT'L MAR. ORG., IMO 2004: FOCUS ON MARITIME SECURITY 2, *available at* http://www.imo.org/includes/blastData.asp?doc_id=3808 (containing a message from the Secretary-General of the International Maritime Organization, Mr. Efthimios Mitropoulos, and discussing past efforts to address terrorist threats).

[134] *See* SOLAS, *supra* note 9; *see also* Murphy, *supra* note 34, at 589; Hesse & Charalambous, *supra* note 118, at 125.

[135] *See* Int'l Mar. Org., Summary of Status of Conventions, http://www.imo.org/Conventions/mainframe.asp?topic_id=247 (last visited Mar. 5, 2005) (providing a list of the SOLAS Contracting Governments as of 31 January 2005).

[136] Unlike other Conventions that may require affirmative ratification by participating governments, SOLAS provides for a "tacit acceptance procedure" so that "an amendment shall enter into force on a specified date unless, before that date, objections to the amendment are received from one-third of the parties or from the parties whose combined merchant fleets represent not less than 50 percent of world gross tonnage." SOLAS, *supra* note 9, art. VIII. The International Convention for the Safety of Life at Sea, Chapter XI contains two parts: Chapter XI-1, "Special Measures to Enhance Maritime Safety;" and Chapter XI-2, "Special Measures to Enhance Maritime Security." Chapter XI-2 contains the ISPS Code. *Id.* at XI-2.

[137] *See* The ISPS Code, *supra* note 9; *see also* Hesse & Charalambous, *supra* note 118, at 125-26.

[138] *See* Int'l Mar. Org., FAQ on ISPS Code and Maritime Security, http://www.imo.org/Newsroom/mainframe.asp?topic_id=897 (last visited Mar. 20, 2005) [hereinafter *FAQ on ISPS Code*].

[139] *See supra* Part II.

1. How the ISPS Code Addresses the "Foreign Element" of Container Vulnerability

The rationale behind the ISPS Code is that port security is a risk management function. In order to manage risks, risks must first be identified.[140] Therefore, the ISPS Code imposes duties upon governments, owners, and operators of certain ships and ports involved in international trade.[141] These requirements provide partial protection against the threat of container ships by requiring foreign vessels and ports to identify vulnerabilities and to create and implement security plans to address the vulnerabilities. The more checks and balances in place overseas, the greater the likelihood of enhancing every realm of security. For instance, a container ship that visited ports with excellent security histories and established security plans may pose a low security risk to U.S ports. Container ships with less stellar security plans, or coming from suspect ports may trigger more concern and a need for inspection. The more information available to U.S. ports upfront, the more prepared port authorities will be to determine necessary action in a timely fashion. Thus, high threats, low threats, and necessary security measures will be more readily apparent. Through these measures, the ISPS Code attempts to remove some of the unknown elements involved in the international transportation of container ships.

The ISPS Code contains two sections for ships and port facilities: Part A is mandatory; and Part B is recommended and contains guidance on implementing the Code.[142] Under Part A, certain vessels and ports involved in international voyages must develop extensive security plans, which their government must also approve.[143] Part A also requires the

---

[140] *See* Hesse & Charalambous, *supra* note 118, at 125-26.

[141] *See* The ISPS Code, *supra* note 9, pt. A, §§ 4.1-4.4; pt. B, § 4.1 (setting forth the requirements of contracting governments in performing security assessments). *See also id.* pt. A, §§ 6.1-6.2, 11.1-11.2.13; pt. B, §§ 6.1-6.8, 8, 9, 13 (discussing the obligations of companies as well as the designation and duties of company security officers); *id.* pt. A, §§ 7.1-9.1, 12.1-12.2.10; pt. B, §§ 8, 9, and 13 (detailing requirements and guidance for ensuring ship security as well as the designation and duties of ship security officers); *id.* pt. A, §§ 14.1-14.6; pt. B, §§ 15, 16, 18 (discussing the security of port facilities, in particular, port facility assessments, plans, and officers); *id.* pt. A, §§ 19.1.1-19.1.4, 19.2.1-19.2.4 (explaining the verification and certification issued to complying ships); *id.* pt. B, § 4.20 (detailing ships that are not required to comply with Part A of the ISPS Code).

[142] *See* The ISPS Code, *supra* note 9, pts. A, B.

[143] *See id.* pt. A, §§ 1.2.1, 3.1. Additional requirements that apply to both ship and port facilities under the ISPS Code include measures for monitoring and controlling access to

use of security personnel, including security officers, and appropriate security equipment.[144] The guidance that the ISPS Code provides to ships depends on "the type of ship, its cargoes and/or passengers, its trading pattern and the characteristics of the port facilities visited by the ship."[145] Likewise, the ISPS Code's guidance for port facilities depends upon the types of cargo, passengers, and the trading patterns of vessels that frequent the port.[146] Under the ISPS Code, contracting governments must first assess the risks faced by individual ports and vessels, then owners and operators must identify and undertake appropriate security measures.[147]

a. The ISPS Code Ship Requirements

Under the ISPS Code, certain ships must have a Ship Security Plan (SSP),[148] detailing both the minimum operational and physical security measures that the ship must meet at all times and also the increasingly demanding measures required in case the designated security level escalates.[149] Vessels subject to the ISPS Code include passenger ships and all vessels weighing more than 500 gross tons involved in international trade, including tankers.[150] Company and ship security officers must review the SSP periodically for sufficiency.[151] Each SSP must be approved by the contracting government, or authorized agency, prior to implementation, and any amendment in an SSP requires

---

secure areas, monitoring the activities of people and cargo, and ensuring that readily available security communications are in place. *See* Hesse & Charalambous, *supra* note 118, at 127. This will be addressed later in the analysis of the ILO and the MTSA. *See infra* Part IV.D., Part V.A.

144 *See* The ISPS Code, *supra* note 9, pt. A. §§ 2.1.6-2.1.8, 4.3, 5.4, 6.2.

145 Hesse & Charalambous, *supra* note 118, at 125; *see* The ISPS Code, *supra* note 9, pt. B, § 4.20 (detailing which ships are not required to comply with Part A of the ISPS Code).

146 *See* The ISPS Code, *supra* note 9, pt. A, §§ 14.1-14.6; pt. B, §§ 15, 16, 18 (detailing port facility security requirements and guidance, including port facility security plans and assessments); *see also* Hesse & Charalambous, *supra* note 118, at 125.

147 *See, e.g.*, The ISPS Code, *supra* note 9, pt. A, §§ 14.1-14.6; pt. B, §§ 15, 16, 18 (discussing port facility security). *See also id.* pt. A, §§ 7.1-9.1; pt. B, §§ 8, 9, 13 (discussing ship security).

148 *See* The ISPS Code, *supra* note 9, pt. A, §§ 2.1.4, 9.1-9.8.1; pt. B, §§ 9.1-9.53; *see also* Hesse & Charalambous, *supra* note 118, at 125, 127.

149 *See* The ISPS Code, *supra* note 9, pt. A, §§ 9.1-9.8.1; pt. B, §§ 9.1-9.53; *see also* Hesse & Charalambous, *supra* note 118, at 125, 127.

150 *See* The ISPS Code, *supra* note 9, pt. A, §§ 3.1, 9.1-9.8.1; pt. B, §§ 9.1-9.53.

151 *Id.* pt. B, § 9.5.

resubmission and approval.[152] To support compliance with the ISPS Code, the ship must carry an International Ship Security Certificate (ISSC).[153] A valid ISSC, however, is only indicia of compliance, and may be subject to further verification by a port state.[154]

b. The ISPS Code Port Facility Requirements

Contracting governments are responsible for initially assessing the security of their port and facility plans. The ports and facilities subject to the ISPS Code include mobile offshore drilling units as well as port facilities serving ships involved with international voyages.[155] Individual governments may complete the Port Facility Security Assessments (PFSA), task intergovernmental agencies with the responsibility, or rely upon assessments conducted by a Recognized Security Organization (RSO).[156] The PFSA will factor into the determination of whether a Port Facility Security Officer (PFSO) is needed.[157] The PFSA, like the SSP, states the minimum security requirements that each facility and port needs in place at each security threat level.[158] Using the PFSA, port facility owners and operators must implement an approved Port Facility Security Plan (PFSP).[159]

c. The ISPS Code's "White Lists"

The IMO is responsible for publishing a list of ports that have approved PFSPs.[160] In addition, the IMO is responsible for publishing a

---

[152] Hesse & Charalambous, *supra* note 118, at 125, 127.

[153] *See* ISPS Code, *supra* note 9, pt. A, §§ 19.1-19.2; *see also* Hesse & Charalambous, *supra* note 118, at 127.

[154] *See* Cunningham E-mail, *supra* note 107.

[155] The ISPS Code, *supra* note 9, pt. A, § 3.1.1.3, 3.1.2.

[156] *Id.* pt. A, §§ 15.1-15.7; pt. B, §§ 4.3, 15.1-15.16.12.

[157] *See id.* pt. A, §§ 17.1-17.3; pt. B, §§ 17.1-17.2; *see also* Hesse & Charalambous, *supra* note 118, at 128.

[158] Hesse & Charalambous, *supra* note 118, at 128.

[159] *Id.* at 26; The ISPS Code, *supra* note 9, pt. A, §§ 16.1-16.8; pt. B, §§ 16.1-16.63.

[160] *See FAQ on ISPS Code*, *supra* note 138 (providing a link to "Status of Compliance with the maritime security provisions of SOLAS chapter XI-2 and the ISPS Code"); *see also* The ISPS Code, *supra* note 9, pt. B, § 4.33 (providing examples of "possible clear grounds" that a ship may not be in compliance with the ISPS Code).

list of vessels that have ISSCs issued by authorized shipping societies.[161] Any ship subject to the ISPS Code that lacks a valid ISSC violates the ISPS Code.[162] Likewise, when a vessel scheduled to arrive from a port is not on the IMO "white list," "the government responsible for a 'white list' port may use this as 'clear grounds' that the ship may not be in compliance with the ISPS Code."[163]

To illustrate the ISPS Code's usefulness, CBP officials will know if a container ship and the ports visited by the ship comply with the ISPS Code even before the vessel departs for U.S. ports. If a foreign container ship fails to comply with the ISPS Code, the U.S. port authority has the discretion to impose compliance as a condition for entering domestic ports.[164] United States authorities may choose to inspect ships while in foreign ports to ensure that they meet IMO standards before they enter U.S. territorial waters.[165] The U.S. Coast Guard, however, always retains discretion to deny entry of a container ship, or any other vessel, arriving from a port that is not on the "white list."[166]

2. Limits of the ISPS Code in Addressing the Unique Threat of Containers

When the ISPS Code became operational on 1 July 2004, IMO reported that eighty-six percent of ships and sixty-nine percent of port

---

[161] *See* Murphy, *supra* note 34, at 589; *see also* The ISPS Code, *supra* note 9, pt. B, §§ 4.3-4.4 (discussing the use of Recognized Security Organizations by contracting governments to fulfill their responsibilities under the ISPS Code). Details on domestic or foreign port or facility compliance are available to the public. *See* Int'l Mar. Org., IMO Global Integrated Shipping Information System (GISIS): Status of Compliance with the Maritime Security Provisions of SOLAS Chapter XI-2 and the ISPS Code, http://www2.imo.org/ISPSCode/ISPSInformation.aspx.

[162] *See* The ISPS Code, *supra* note 9, pt. B, §§ 1.13, 4.32; Murphy, *supra* note 34, at 589.

[163] Murphy, *supra* note 34, at 589.

[164] *See id.* at 589.

[165] *See* FRITTELLI, *supra* note 3, at 10; *but see* Cunningham E-mail *supra* note 107 (explaining that the U.S. Coast Guard does not have the unilateral ability to board foreign vessels, but may require the permission of the port state or the vessel's flag state).

[166] *See* Cunningham E-mail, *supra* note 107 (noting that the U.S. Coast Guard has the prerogative to deny a foreign vessel entry into a domestic port due to the vessel's failure to comply with the ISPS Code). *See also* The ISPS Code, *supra* note 9, pt. B, § 4.33 (listing examples of "clear grounds" for ISPS Code violations, warranting denial of port entry); *id*. pt. A, § 4 (setting forth the responsibilities of Contracting Governments and listing some of the conditions that each Contracting Government may impose upon foreign vessels seeking port entry).

facilities had approved security plans in place.[167] Those figures have substantially increased, and currently nearly ninety-seven percent of the more than 9600 declared port facilities have approved PFSPs in place.[168] Likewise, "well beyond" ninety percent of ships have approved security plans in effect.[169]

Despite these promising statistics, even 100% compliance with the ISPS Code provisions is insufficient to address the security threats containers pose to U.S. ports. As identified earlier, the primary vulnerability of container ships is the inherently unknown element of containers arriving from foreign ports.[170] The ISPS Code attempts to remove some of these unknown variables by both exposing weaknesses and addressing security measures in place to prevent security breaches. These measures are useful, but leave the following enormous gaps in container ship security: (1) the ISPS Code does not protect against goods loaded into containers during or before the containers were loaded onto ships; (2) ports and vessels may have difficulty complying with the ISPS Code, thereby excluding them from the benefits of maritime commerce; and (3) the ISPS Code may expand the threats posed by containers by introducing a largely unregulated privatization element that lacks oversight.

a. The ISPS Code Does Not Protect Against Goods Loaded into Container Ships

Despite the clear informational advantages of the ISPS Code, it was not designed to address a number of key foreign threats that container ships present to U.S. ports.[171] In particular, the ISPS Code does not protect against goods loaded into containers that are then loaded onto container ships. Notably, the ISPS Code does not provide any protection

---

[167] Hesse & Charalambous, *supra* note 118, at 132.

[168] *Maritime Security on Agenda*, *supra* note 125.

[169] Hesse & Charalambous, *supra* note 118, at 132. The IMO and the United States have been very active in providing training in maritime security measures. *Id.* at 133.

[170] *See supra* Part II.B.

[171] While the ISPS Code was not designed to address container ship security, container security issues are an inherent element of the ISPS Code's objective to provide an "international framework involving co-operation between Contracting Governments, Government agencies, local administrations and the shipping and port industries to detect security threats and take preventive measures against security incidents affecting ships or port facilities used in international trade." The ISPS Code, *supra* note 9, pt. A, § 1.2 (stating the objectives of the ISPS Code).

against a WMD being loaded onto a container scheduled to enter a U.S. port.

The contents of a typical single container shipment may include goods from various sources and involve thirty to forty documents.[172] The sources providing the container contents, however, are cloaked in anonymity. While cargo manifests should list the contents of each container, even by a conservative estimate, it is possible that the listed contents of a single container ship carrying 3,000 containers may require good faith reliance upon representations from more than 90,000 sources.[173] The 25,000 containers[174] that arrive in U.S. ports each day present continuing threats. The arrival of this enormous volume of containers translates to daily good faith reliance upon the representations of over 750,000 providers of goods entering U.S. ports.[175] The ISPS Code alone is insufficient to address these threats.

b. The ISPS Code Does Not Protect Against Container Ships Arriving from Countries that Lack the Financial Means or Political Incentive to Comply with ISPS Code Requirements

While the percentage of ports and vessels complying with the ISPS Code is extremely high, there remain regional areas where compliance has been difficult to achieve. The numbers suggest that the ISPS Code strikes a good balance between security and feasibility for most countries. As Scott J. Glover, a retired Captain with the U.S. Coast Guard, recently explained, although reports indicate a large percentage of ISPS Code compliance in foreign ports and with foreign vessels, trips to these ports suggest that the ISPS Code is not actually in compliance with U.S. standards; "a cursory examination of some ports may make you wonder."[176] In addition, "Africa is falling behind other continents in

---

[172] *See* FRITTELLI, *supra* note 3, at 8.

[173] This figure is calculated by multiplying the number of containers on a large container ship (i.e. 3,000) by a conservative estimate of the number of documents connected to and listing the purported cargo of each container (i.e. thirty).

[174] *See* Bonner, *supra* note 2 (stating that 25,000 containers arrive in U.S. ports each day and that nine million containers arrive in U.S. ports annually).

[175] This figure is calculated by multiplying the average number of containers that arrive in U.S. ports each day (i.e. 25,000) by a conservative estimate of the number of documents connected to and listing the purported cargo of each container (i.e. thirty).

[176] Scott J. Glover, Director of Maritime Security, HPA, LLC, Speech at the 4th Annual International Conference on Public Safety: Technology & Counterterrorism (Mar. 15,

complying with the new regulations" and "[c]ountries in the former Soviet Union and Eastern Europe have also been slow to implement the measures."[177]

There are two implementation problems identified by the IMO. First, member countries may lack the necessary expertise, experience, and resources to implement the ISPS Code.[178] Second, member countries may place a low priority on implementation.[179]

While wealthy countries that can afford to comply with the ISPS Code will likely enjoy priority as importers to the United States, poorer countries that lack the financial means to comply with the ISPS Code may find that they are internationally boycotted.[180] The IMO does not generate a "black list" of non-conforming countries, and specifically states that "[l]ack of inclusion in the database should not be construed automatically as failure to comply with the requirements in SOLAS."[181] As discussed above, however, if a vessel scheduled to arrive from a port is not on the IMO "white list," "the government responsible for a 'white list' port may use this as 'clear grounds' that the ship may not be in compliance with the ISPS Code."[182] It is easy to see that the "white list" implies a "black list" by negative inference.

Anticipating the plight of poorer countries, the IMO initiated a $2.5 million Global Program on Maritime and Port Security in January 2002.[183] The program includes worldwide activities, such as seminars and workshops at regional and national levels to help countries comply with SOLAS and the ISPS Code.[184] Thus far, the program has trained

---

2005) (stating that progress is being made in ISPS Code compliance, but "we're still not there").

[177] Int'l Mar. Org., Security Compliance Shows Continued Improvement (Aug. 6, 2004), http://www.imo.org/Newsroom/mainframe.asp?topic_id=892&doc_id=3760 [hereinafter Security Compliance].

[178] *Id*.

[179] *See id*; *see also* Hesse & Charalambous, *supra* note 118, at 133.

[180] *See* Flynn E-mail, *supra* note 28 (noting that a ship may be delayed if it visited a non-compliant port during the past ten port calls).

[181] *FAQ on ISPS Code*, *supra* note 138.

[182] *See* Lloyd's Register, Maritime Security - Frequently Asked Questions and Answers, http://www.lr.org/market_sector/marine/maritime-security/faqs.htm; *see also* The ISPS Code, *supra* note 9, pt. B, § 4.33 (providing examples of "possible clear grounds" that a ship may not be in compliance with the ISPS Code).

[183] *See* Security Compliance, *supra* note 177.

[184] *See id.*

more than 3,200 people in developing regions.[185] As the current IMO figures suggest, however, parts of Africa, the former Soviet Union, and Eastern Europe still have not implemented the ISPS Code measures.[186] While compliance by ninety-seven percent of ports may sound high, because over 9,600 ports are involved in international trade, approximately 300 ports still are not in compliance. Therefore, the United States may face either an effective boycott of goods from these ports, or risk the potentially dangerous consequences of accepting goods from their ports.

c. Privatization Problems in Determining the Reliability of Information

By implementing international criteria for vessels and ports, the intent of the ISPS Code is that other participating countries will be able to rely on measures executed abroad to protect against the threat of people or goods harming their country.[187] Government approved security assessments and plans may provide a level of justified reliance. Unregulated private businesses, however, play a significant role in meeting the ISPS Code requirements and, due to lack of oversight, may be unreliable. While the ISPS Code removes some of the unknown variables faced by the United States in dealing with foreign containers, it also creates additional unknown variables.

The ISPS Code permits governments and owners to have security assessments of vessels and port facilities conducted by an RSO.[188] The ISPS Code defines an RSO as "an organization with appropriate expertise in security matters and with appropriate knowledge of ships

---

[185] *Id.*
[186] *Id*.
[187] *See* The ISPS Code, *supra* note 9, pt. A, § 1.2 (stating objectives of the ISPS Code).
[188] *See* SOLAS, *supra* note 9, ch. 1, reg. 6.

> All ships must be surveyed in order to be issued certificates which establish their seaworthiness, type of ship, and so on and this is the responsibility of the flag State of the vessel . . . [h]owever, the flag State ("Administration") [may] entrust the inspections and surveys either to surveyors nominated for that purpose or to organizations recognized by it.

Id. See also ISPS Code, *supra* note 9, pt. A, §§ 15.1-15.7; pt. B, §§ 15.1-15.16.12.

authorized by the Administration to approve the SSP, carry out audits and issue on its behalf International Ship Security Certificates."[189] In addition, RSOs often are an international association of classification societies, or certain non-Governmental organizations that were granted consultative status with the IMO in 1969.[190]

Due to implementation and time constraints imposed by the ISPS Code, privatization is necessary for countries to comply with the multi-layered requirements in a timely fashion. Without oversight requirements, however, this privatization creates a new layer of unknowns and, consequently, another security threat. After all, regulations for RSOs may vary among countries, and there are no international certification requirements or formal training requirements for RSO inspectors.[191] The inherent problem with the existing scenario is that SSPs and ISSCs may only create the appearance that a foreign ship or port facility is in compliance. This appearance, however, may be more of an illusion than a reality, because the lack of RSO oversight or guidelines may render verification of the approval process virtually impossible. Furthermore, it is conceivable that unscrupulous RSOs could generate rubber-stamped SSP and ISSC approvals, which the United States may have difficulty controlling or discovering.[192]

According to the U.S. Coast Guard website, once an organization is certified as an RSO, its conduct is only policed by the Coast Guard if it is involved in "ISPS-related detention, expulsion, or denial of entry."[193]

---

[189] *See* ISPS Code, *supra* note 9, pt. A, §§ 15.1-15.7; pt. B, §§ 15.1-15.16.12; *see also* U.S. Coast Guard, 2004 List of Targeted Recognized Security Organizations (July 19, 2005), http://www.uscg.mil/hq/g-m/pscweb/RSO.htm (explaining what targeted RSOs are, and providing the same definition of RSO contained in the ISPS Code) [hereinafter List of RSOs – 2004].

[190] *See* INT'L MAR. ORG., MSC/CIRC.1074, MEASURES TO ENHANCE MARITIME SECURITY: INTERIM GUIDELINES FOR THE AUTHORIZATION OF RECOGNIZED SECURITY ORGANIZATIONS ACTING ON BEHALF OF THE ADMINISTRATION AND/OR DESIGNATED AUTHORITY OF A CONTRACTING GOVERNMENT (2003), *available at* http://www.imo.org/includes/blastData.asp/doc_id=3008/1074.pdf (explaining the role of RSOs in ISPS compliance).

[191] *See* Flynn E-mail, *supra* note 28 (noting that the lack of certified formal training for inspectors "raises obvious questions about the qualifications of those who are conducting these security checks").

[192] *But see* Cunningham E-mail, *supra* note 107 (arguing that "[w]hile an unscrupulous RSO may pencil whip an ISSC, we [the Coast Guard] most definitely will discover it via our very aggressive port state control activity"). *See infra* Part V.A.1.c. (discussing the U.S. Coast Guard's Port State Control Program).

[193] *See* List of RSOs – 2004, *supra* note 189 (containing the same definition for RSO as The ISPS Code and SOLAS). *But see* Cunningham E-mail, *supra* note 107 (noting that

The U.S. Coast Guard "determines whether the actions or inaction of the RSO contributed to the control action. If so, the Coast Guard attributes the control action to the RSO."[194] "[Recognized Security Organizations] will be targeted based on their total number of related major control actions accumulated during the previous 12-month period as determined by [Coast Guard Head Quarters]."[195]

In efforts to compensate for the inherent unknowns of RSOs, the Coast Guard scrutinizes activities of RSOs, uses Port State Control actions, [196] and constantly revamps assessments of RSOs based on new information.[197] The lack of RSO oversight or regulations, however, may lead to retroactive rather than preventive security measures.[198] Furthermore, while a foreign vessel's ISSC is available for the Coast Guard to review, the underlying plans reviewed by RSOs (or other foreign officials) in issuing the ISSC may not be available to the Coast Guard. Inspection officers designated by a Contracting Government have no authority to inspect SSPs except in very limited circumstances, as specified in section 9.8.1 of the ISPS Code.

RSOs can be targeted in various ways: e.g. "[i]f too many vessels issued an ISSC by an RSO have control actions, even control actions not directly attributable to the RSO, vessels using the RSO will be targeted and face increased scrutiny").

[194] *See* List of RSOs – 2004, *supra* note 189. *But see* Cunningham E-mail, *supra* note 107 (stating that port state control provides a very good method for verification and identifying unscrupulous RSOs).

[195] *See* List of RSOs – 2004, *supra* note 189 ("The list of targeted RSOs . . . will be updated and posted on a monthly basis. RSO's have the ability to appeal the determination made by USCG HQ concerning their association with a major control action.").

[196] *See infra* Part V.A.1.c. (discussing the U.S. Coast Guard's Port State Control Program).

[197] *See* Cunningham E-mail, *supra* note 107 (discussing various means by which an RSO may be targeted (e.g. "[i]f many vessels issued an ISSC by an RSO have control actions, even control actions not directly attributable to the RSO, vessels using the RSO will be targeted and face increased scrutiny")). While there may be a preventive aspect to this method of targeting, it is based upon past detection of other vessels that were subject to control actions rather than purely preventative methods.

[198] *Cf Addressing the Shortcomings of the Customs-Trade Partnership Against Terrorism (C-TPAT) and the Container Security Initiative Before the Permanent Sub-Committee on Investigations, Committee on Homeland Security and Governmental Affairs, United States Senate*, 109th Cong. (testimony of Stephen E. Flynn, Ph.d) (May 26, 2005) [hereinafter *Addressing the Shortcomings of the Customs-Trade Partnership Against Terrorism (C-TPAT) and the Container Security Initiativ*] (stating that the C-TPAT approach to deterring terrorist activity is problematic "because private security is inherently reactive; i.e., companies cannot punish violators of their rules until there is some evidence that those rules have been broken.").

> If the officers duly authorized by a Contracting Government have clear grounds to believe that the ship is not in compliance . . . and the only means to verify or rectify the non-compliance is to review the relevant requirements of the ship security plan, limited access to the specific sections of the plan relating to the non-compliance is exceptionally allowed, but only with the consent of the Contracting Government, or the master of the ship concerned. [Certain] provisions in the plan . . . are considered as confidential information, and cannot be subject to inspection unless otherwise agreed by the Contracting Governments concerned. [199]

The lack of international regulations or certification of RSOs limits the ability of the United States to control or verify RSOs overseas.[200] These impediments pose security risks that may persist until RSOs are subject to oversight, international standards, and verifiable criteria.

C. The World Customs Organization

Although the ISPS Code does not deal with the possible threat posed by goods loaded on a container ship, the WCO compiled a set of elements to identify high-risk goods which can be applied to container ships.[201] The WCO is an international institution based in Brussels, Belgium that works "towards simplifying and harmonizing customs procedures to improve the efficiency of cross-border trade."[202] Current

---

[199] *See* The ISPS Code, *supra* note 9, pt. A, § 9.8; *see also* Cunningham E-mail, *supra* note 107 (noting that while the United States inspects all vessels subject to SOLAS and the ISPS Code at least annually, there remain information stumbling blocks: "a port state does not have access to a vessel's security plan before an inspection," "[s]ome parts of the security plan may not be viewed by a port state unless the flag state gives permission," and "we must have clear grounds for seeing even parts of the plan").

[200] *See* U.S. COAST GUARD, NAVIGATION AND VESSEL INSPECTION CIR. NO. 04-03, CHANGE 1 TO GUIDANCE FOR VERIFICATION OF VESSEL SECURITY PLANS ON DOMESTIC VESSELS IN ACCORDANCE WITH THE MARITIME TRANSPORTATION SECURITY ACT (MTSA) REGULATIONS AND INTERNATIONAL SHIP & PORT FACILITY SECURITY (ISPS) CODE, COMDTPUB 16700.4, Enclosure 3, 3 (May 21, 2004), *available at* http://www.uscg.mil/hq/g-m/nvic/03/NVIC_04-03_CH-1.pdf (noting that although the ISPS Code permits RSOs, 33 C.F.R. pt. 104 does not and, therefore, the U.S. Coast Guard has not designated any RSOs).

[201] FRITTELLI, *supra* note 3, at 13.

[202] *Id.*

members of the WCO include 168 countries, including the United States, which account for ninety-eight percent of world trade.[203]

In June 2003, a WCO task force, consisting of representatives from fifty countries and twenty-five organizations, created a Resolution on Security and Facilitation of the International Supply Chain.[204] The task force generated a set of data elements for identifying high risk cargo. These elements were incorporated into the WCO's Framework of Standards to Secure and Facilitate Global Trade in June 2005.[205] In addition to identifying high risk cargo, the elements and subsequent framework provide a consistent method for exchanging information "on inbound, outbound and transit shipments," and a "consistent risk management approach to address security threats."[206] The objective of the task force was "to secure and protect the international trade supply chain from being used for acts of terrorism or other criminal activity while insuring continued improvements in trade facilitation without unnecessarily increasing costs."[207] As part of an effort to achieve this objective, the framework contains an Appendix entitled, "Seal Integrity Programme for Secure Container Shipments."[208]

Similarly, the Group of Eight, or G8,[209] began working with the WCO to develop joint standards and guidelines for electronic

---

[203] *See* WORLD CUSTOMS ORG., WCO FACT SHEET: THE WORLD CUSTOMS ORGANIZATION, *available at* http://www.wcoomd.org/ie/en/AboutUs/aboutus.html (last visited Sept. 6, 2005); *see also* Kunio Mikuriya, Deputy Secretary General, WCO, The Challenges of Facilitating the Flow of Commerce in a Heightened Security Environment, Speech at the UNECE International Forum on Trade Facilitation (May 29-30, 2002), *available at* http://www.unece.org/trade/forums/forum02/presentations/session_i/kmikuriya.pdf (explaining that the members of the WCO account for 97% of world trade).

[204] PRAVIN GORDHAN, RESOLUTION OF THE CUSTOMS CO-OPERATION COUNCIL ON SECURITY AND FACILITATION OF THE INTERNATIONAL TRADE SUPPLY CHAIN (2002), http://www.wcoomd.org/ie/En/Press/Resolution%20Final%20Council%20June%202002%20-%20E.PDF [hereinafter Resolution of the Customs Co-operation].

[205] WORLD CUSTOMS ORG., FRAMEWORK OF STANDARDS TO SECURE AND FACILITATE GLOBAL TRADE (2005), *available at* http://www.wcoomd.org/ie/En/Press/Cadre%20de%20normes%20GB_Version%20Juin%202005.pdf [hereinafter FRAMEWORK OF STANDARDS].

[206] *Id.* at 1.3, 1.2.2.

[207] Resolution of the Customs Co-operation, *supra* note 204.

[208] FRAMEWORK OF STANDARDS, *supra* note 205, at Appendix to Annex 1.

[209] *See* Fed'n of Am. Scientists, *G-8 to Take Further Steps to Enhance Transportation Security*, June 2, 2003, *available at* http://www.fas.org/asmp/campaigns/MANPADS/G8evianmtg_DoSsummary.htm. The Group of Eight—G8—is a grouping of eight of the world's leading industrialized, democratic nations (Canada, Germany, France, Italy, Japan, Russia, the United Kingdom, and the United States). *See id.*

transmission of customs data for cargo, and a standardized set of data elements to identify high-risk cargo.[210] The WCO and the G8 aspire to combine security needs with trade facilitation.

This article is limited in addressing the elements used to identify high-risk cargo because the lists and criteria are classified. Those familiar with the maritime trade industry, however, could likely manipulate the system. For example, cargo manifests and other representations of goods could be crafted to avoid suspicion. The classified criteria could be deciphered by following which patterns of cargo or shipments trigger enhanced scrutiny. Once the criteria are identified, the methods of reporting or otherwise providing ascertainable characteristics of a vessel and its goods could be altered to avoid further scrutiny. Furthermore, while the WCO "resolves" to do a variety of things, measures to achieve such goals are incomplete and not yet ratified.

D. The International Labor Organization and Documentation of Seafarers' Identity

Currently, there is no reliable seafarer document that verifies the identity of crewmembers on container ships and port facility workers. Containers are a source by which terrorists could smuggle themselves into U.S. ports.[211] Moreover, terrorist crewmembers or stowaways on container ships may sabotage the containers during transit or steer a container ship into a bridge or port. Therefore, the identity of those who have access to containers and container ships is an important security layer.

As a result of the 9/11 attacks, the international community recognized the need to update seafarer identification documents. The ISPS Code requires ships and port facilities to create measures for monitoring and controlling access to secure areas, for monitoring the activities of people and cargo, and for ensuring that readily available security communications are in place.[212] These requirements must be

---

[210] *See id.*

[211] *See supra* Part II; *see also* Bonner, *supra* note 2 ("Shipments may contain terrorist operatives or terrorists themselves.").

[212] *See* The ISPS Code, *supra* note 9, pt. A, §§ 9.1-9.8.1, 14.1-14.6; pt. B, §§ 9.1-9.53, 15, 16, 18.

considered jointly with the efforts of the International Labor Organization (ILO).

The ILO revised the 1958 Convention Dealing with Documentation of Seafarers' Identity, effective 9 February 2005.[213] The new Convention provides rigorous procedures for seafarer identification to enhance security against infiltration of terrorists and to "ensur[e] that the world's 1.2 million seafarers will be given the freedom of movement necessary for their well-being and for their professional activities and, in general, to facilitate international commerce."[214]

Although the United States is a contracting government to the ILO, the United States has not ratified the revised Convention. In fact, only four countries—France, Hungary, Jordan and Nigeria—ratified the revised Convention.[215] Therefore, the ILO's attempt to provide another layer of security has achieved marginal success, at best. Nonetheless, the detailed discussion of the MTSA below addresses domestic attempts to resolve the identification issue.[216]

V. Domestic Players and Initiatives Involved in the Layered Defense of Container Ship Security

On 25 November 2002, Congress enacted the Homeland Security Act of 2002, which established the Department of Homeland Security as an executive department of the United States.[217] In addition to the creation of DHS, the U.S. Customs Service was reorganized and renamed as the Bureau of U.S. Customs and Border Protection on 1 March 2003 under the Customs Co-Operation and Mutual Assistance in

---

[213] *See* SEAFARERS' IDENTITY DOCUMENTS (REVISED), *supra* note 116.

[214] Press Release, Int'l Lab. Org., 91st Annual Conference of the ILO Concludes Its Work: Delegates Debate Action To End Poverty Through Work, Adopt Convention On Seafarers Security Measures (June 19, 2004), *available at* http://www.ilo.org/public/english/bureau/inf/pr/2003/35.htm. *See* SEAFARERS' IDENTITY DOCUMENTS (REVISED), *supra* note 116.

[215] The International Labor Organization website contains a list of the countries that have ratified the SEAFARERS' IDENTITY DOCUMENTS (REVISED), *supra* note 116. *See* Int'l Lab. Org., Convention No. C185 Was Ratified by Four Countries, http://www/o;p/prg/ilolex/cgi-lex/ratifce.pl?C185 (last visited Sept. 21, 2005).

[216] *See infra* Part V.A.3.a-b (discussing §§ 70105, 70111 of the MTSA).

[217] *See* The Homeland Security Act of 2002, Pub. L. No. 107-296, § 101, 116 Stat. 2135 (2002).

Customs Matters. Furthermore, the U.S. Coast Guard was transferred from the Department of Transportation to DHS.[218]

The Coast Guard is the principal maritime law enforcement authority in the United States, as well as the lead DHS agency for maritime security, including port security.[219] The Coast Guard is the logical choice based on its equipment, training, connections to civilian federal law-enforcement agencies, and "because of its dual status as both an armed service and a law enforcement agency."[220] Coast Guard responsibilities include evaluating, boarding, and inspecting commercial ships as they approach U.S. waters.[221] In addition to numerous other duties, the Coast Guard assesses and counters terrorist threats in U.S. ports, as well as protects U.S. Navy ships while in U.S. ports.[222] Under both the Ports and Waterways Safety Act of 1972,[223] and the recently enacted Maritime Transportation Security Act of 2002, discussed in detail below,[224] the Coast Guard is responsible for protecting vessels and harbors from terrorists, or otherwise subversive acts.[225]

The U.S. Customs and Border Protection (CBP) has the principal and initial responsibility to inspect cargo.[226] This duty includes inspecting

---

[218] *See id.* United States Customs and Border Protection is the agency within the Department of Homeland Security that manages, controls, and secures U.S. borders. *See* CBP Mission, *supra* note 64.

[219] *See Hearing on Implementation*, *supra* note 131; *see also* U.S. Coast Guard, Welcome to the Office of Law Enforcement Home Page (last updated Jan. 24, 2005), http://www.uscg.mil/hq/g-o/g-opl/Welcome.htm. *See also* 14 U.S.C.S. 2 (authorizing the Coast Guard Law Enforcement mission; "[t]he Coast Guard shall enforce or assist in the enforcement of all applicable laws on, under and over the high seas and waters subject to the jurisdiction of the United States"); 14 U.S.C.S. 89 (authorizing U.S. Coast Guard active duty commissioned, warrant, and petty officers to enforce applicable U.S. laws, and federal laws, on waters subject to U.S. jurisdiction, and in certain instances in international waters).

[220] O'ROURKE, *supra* note 15, at 1.

[221] *See id.*; *see also* FRITTELLI, *supra* note 3, at 9-11; Rear Admiral Kevin J. Eldridge, U.S. Coast Guard Commander of District 11, Speech at the 4th Annual International Conference on Public Safety: Technology & Counterterrorism (Mar. 15, 2005) (explaining that surveillance technology allows the U.S. Coast Guard to know if a vessel encounters problems during transit, which warrant interdiction on the high seas).

[222] *See* FRITTELLI, *supra* note 3, at 9-10; *see also* RONALD O'ROURKE, CONGRESSIONAL RESEARCH SERVICE REPORT FOR CONGRESS, HOMELAND SECURITY: COAST GUARD OPERATIONS BACKGROUND AND ISSUES FOR CONGRESS 1-2 (updated June 30, 2005).

[223] Ports and Waterways Safety Act of 1972, 33 U.S.C. S. §§ 1221-1236 (1994).

[224] *See infra* Part V.A.

[225] FRITTELLI, *supra* note 3, at 10.

[226] *Id.*

cargo containers that foreign ships bring into U.S. ports, as well as examining and inspecting the crew members and passengers on ships arriving in U.S. ports from foreign ports.[227]

The Transportation Security Administration (TSA) is yet another agency involved in domestic maritime security. The TSA was created by the Aviation and Transportation Security Act of 2001.[228] Initially, it focused on the security of air transportation, but then the TSA expanded to include all modes of transportation, including maritime transportation.[229]

In order to understand how the various players contribute layers to the domestic security of containers and container ships, it is necessary to look at the key national measures implemented post-9/11. While a number of federal agencies have implemented a variety of measures, the seminal sources that deal with container security threats in maritime transportation are the Maritime Transportation Security Act, the Container Security Initiative, and the Customs-Trade Partnership Against Terrorism.

A. The Maritime Transportation Security Act of 2002

On 25 November 2002, President George W. Bush signed into law the Maritime Transportation Security Act of 2002 (MTSA) in an attempt to improve port security standards.[230] The central function of the MTSA

---

[227] *Id.* ("Prior to the establishment of the CBP, customs and immigration functions at U.S. borders were conducted separately by the Department of the Treasury's U.S. Customs Service and the Department of Justice's Immigration and Naturalization Service.").

[228] Aviation and Transportation Security Act of 2001, Pub. L. No. 107-71, 115 Stat. 597. *See* FRITTELLI, *supra* note 3, at 10, 12 (explaining the role of TSA).

[229] Aviation and Transportation Security Act of 2001, Pub. L. No. 107-71, 115 Stat. 597; FRITTELLI, *supra* note 3, at 11.

[230] *See* The Maritime Transportation Security Act of 2002, Pub. L. 107-295, tit. I, § 101, 116 Stat. 2064, 2066 (codified at 46 U.S.C.S. §§ 70101-117 (LEXIS 2005)); *see also* FRITTELLI, *supra* note 3, at 2. The Coast Guard and Maritime Transportation Act of 2004 was signed into law on 9 August 2004. Title VIII of the 2004 Act clarifies provisions of the MTSA and imposes specific deadlines for designated actions. For instance, the 2004 Act requires the Secretary to investigate and examine sensors that are able to track marine containers throughout their supply chain and detect hazardous and radioactive materials within the containers. *See* Coast Guard and Maritime Transportation Act of 2004, Pub. L. No. 108-293, 118 Stat. 1028; *see also* Maritime Transportation Security Act of 2002, 46 U.S.C.S. § 70115 (imposing AIS requirements).

is to "increase security at United States ports" by securing entry points and other areas of port facilities, and examining or inspecting containers.[231] The MTSA was implemented, in part, to comply with the requirements in the ISPS Code.[232] Therefore, much of the MTSA aligns with the ISPS Code. The MTSA, however, creates additional layers of protection against the container ship security threat facing U.S. ports by regulating domestic as well as foreign vessels and facilities.[233] Unfortunately, the MTSA leaves remaining gaps in container ship security, which necessitate additional measures.

The MTSA tasks agencies and individuals with a variety of responsibilities designed to deter a "transportation security incident" to the greatest extent practicable.[234] The MTSA addresses foreign maritime threats as well as domestic threats, recognizing that the central threat presented by container ships departing for the United States takes place during the foreign port phase. In attempts to resolve these outstanding threats, the MTSA strives to achieve the following: (1) to identify and track vessels;[235] (2) to assess the level of security preparation of particular vessels and port facilities;[236] (3) to limit access to secure areas;[237] (4) to develop an automatic identification system allowing port officials to identify and position vessels in U.S. waters;[238] and (5) to require foreign and domestic owners or operators of vessels operating in U.S. waters to prepare and submit a "vessel security plan" for approval to

---

[231] *See* Maritime Transportation Security Act of 2002 § 101 (listing congressional findings).

[232] *See supra* Part IV.A. (explaining that the ISPS Code is an amendment to SOLAS). The ISPS Code enacted new regulations in Chapter V of SOLAS as well as a new Chapter, XI-2 which makes the ISPS Code mandatory. *See also* Cunningham E-mail, *supra* note 107 (noting that the MTSA and the ISPS Code "intentionally mirror each other. At the same time we (the Coast Guard) [were] providing drafting assistance to Congress on MTSA we were in London proposing the same text for ISPS").

[233] *See generally* The MTSA, 46 U.S.C.S. §§ 70101-117; Vessel Security, 33 C.F.R. Part 104 (LEXIS 2005) (implementing the MTSA, and requiring foreign SOLAS government members to submit vessel security plans in accordance with the ISPS Code to designated agencies).

[234] 46 U.S.C.S. § 70101.

[235] *Id.* § 70114.

[236] *Id.* §§ 70102-03; *see* Maritime Security, 33 C.F.R. pt. 101 (defining a facility as any structure located in, on, under, or adjacent to any waters and subject to the jurisdiction of the United States, regardless of whether it is operated, used, or maintained by public or private entities, and including any contiguous or adjoining property that is under common operation or ownership).

[237] 46 U.S.C.S. §§ 70105, 70111.

[238] *Id.* § 70114.

the Secretary of Homeland Security.[239] While the MTSA applies to a variety of ships, the following analysis focuses on the security layers it provides against the threat posed by container ships.

1. Role of the U.S. Coast Guard in Securing U.S. Vessels and Port Facilities Under the MTSA

The MTSA creates a system to enhance U.S. maritime security by requiring federal agencies, ports, and vessel owners to take numerous steps to upgrade security. In particular, the MTSA requires the Secretary[240] of the department in which the Coast Guard is operating to develop national and regional Area Maritime Transportation Security Plans.[241] The DHS further delegated the responsibility and authority for security plans to the Coast Guard.[242] These plans evaluate security risks and delegate the duties and responsibilities among federal, state, and local government agencies.[243] The MTSA also requires ports, waterfront terminals, and certain types of vessels to develop their own security and incident response plans.[244] These plans must receive Coast Guard approval.[245]

The Coast Guard published six final rules to implement the MTSA: Implementation of National Maritime Security Initiatives[246]; Area Maritime Security[247]; Vessel Security[248]; Facility Security[249]; Outer Continental Shelf (OCS) Facility Security[250]; and Automated Identification Systems.[251] While the requirements set forth in the MTSA

---

[239] *Id.* §§ 70103(c)(1)-(3), 70108.
[240] *Id.* § 70101(5) (defining the term "Secretary").
[241] *Id.* § 70103(a).
[242] U.S. GEN. ACCT. OFF., GAO-04-838, MARITIME SECURITY: SUBSTANTIAL WORK REMAINS TO TRANSLATE NEW PLANNING REQUIREMENTS INTO EFFECTIVE PORT SECURITY 7 (2004).
[243] 46 U.S.C.S. § 70103(a).
[244] *Id.*
[245] *Id.* § 70104(a).
[246] Maritime Security, 33 C.F.R. pt. 101 (2005).
[247] Area Maritime Security, 33 C.F.R. pt. 103 (2005).
[248] Vessel Security, 33 C.F.R. pt. 104 (2005).
[249] Facility Security, 33 C.F.R. pt. 105 (2005).
[250] Outer Continental Shelf Facilities, 33 C.F.R. pt. 106 (2005).
[251] Automated Identification Systems Vessel Traffic Service, 33 C.F.R. pts. 26, 161, 164, and 165. In addition to these rules, on 21 October 2002, the Coast Guard issued a Navigation and Vessel Inspection Circular (NVIC) entitled "Security Guidelines for Vessels." This NVIC was revised on 6 August 2004, retains the same title, and instructs

apply broadly to U.S. ports and different categories of vessels, the requirements also increase the security of containers and container ships.

a. The Coast Guard's Duty to Identify Threats Faced by Ships and Ports

The MTSA requires the Coast Guard to conduct initial facility and vessel vulnerability assessments to identify the vessel types, ports, and port facilities "that pose a high risk of being involved in a transportation security incident."[252] The Coast Guard must then conduct a detailed vulnerability assessment of those vessels and facilities identified.[253] The detailed vulnerability assessment identifies all critical assets and infrastructures, threats to those assets and structures, and weaknesses in physical security, passenger and cargo security, structural integrity, and protection systems.[254] To protect against the foreign element, the MTSA also requires the Coast Guard to perform "antiterrorism assessments of certain foreign ports."[255]

b. The Coast Guard's Duty to Address Threats Faced by Ships and Ports

Using detailed vulnerability assessments, the Coast Guard must develop national and regional Maritime Transportation Security Plans for deterring and responding to a transportation security incident.[256] Like the assessments, the plans must identify critical assets, infrastructure, and potential threats and weaknesses in the security of the maritime

---

vessel operators and owners on how to comply with IMO requirements. The revised NVIC also instructs on how to appoint company and ship security officers, conduct security assessments, designate protective measures, prepare vessel security plans, and coordinate security provisions with port facilities, in satisfaction of §§ 70102-70104 of the MTSA. *See* U.S. COAST GUARD, NAVIGATION AND VESSEL INSPECTION CIR. NO. 10-02, SECURITY GUIDELINES FOR VESSELS (Oct. 21, 2002), *available at* http://www/uscg/mil/hq/g-m/nvic/02/10-02.pdf; *see also* U.S. COAST GUARD, NAVIGATION AND VESSEL INSPECTION CIR. NO. 10-02, CHANGE 1, SECURITY GUIDELINES FOR VESSELS (Aug. 6, 2004), *available at* http://www.uscg.mil/hq/g-m/nvic/02/NVIC%2010-02%CHANGE%201.pdf.

[252] 46 U.S.C.S. § 70102.

[253] *See id.*

[254] *See id.*

[255] *See Hearing on Implementation*, *supra* note 131, at 3.

[256] 46 U.S.C.S. § 70103.

transportation system.[257] These plans are necessary both to help prevent breaches in security and, equally as important, to put into effect a plan for dealing with such breaches should they occur.

c. The Coast Guard's Port State Control Program

The Coast Guard developed a formal Port State Control Program in 1994 to "closely scrutinize foreign-flagged freight ships."[258] Following 9/11, the Coast Guard significantly enhanced security procedures as part of the Port State Control Program.[259] In particular, Subpart C of Title 33 of the Code of Federal Regulations, Part 160, which implements[260] the Ports and Waterways Safety Act,[261] requires certain foreign vessels to provide a Notice of Arrival (NOA) to the National Vessel Movement Center (NVMC) prior to entering the United States.[262] The Coast Guard then prescreens those vessels before they arrive in a U.S. port using three "Risk-Based Decision Making" (RBDM) tools.[263] The purpose of these RBDM tools is to determine the level of threat that each vessel poses to the United States.[264] The RBDM tools consist of three "Compliance Verification Examination Matrices," which the Coast Guard uses to prioritize vessel boardings.[265] The first of the three matrices is the "Foreign Vessel Port Security Targeting Matrix."[266] The classified components of this matrix are used to evaluate the security risk of certain foreign vessels entering a U.S. port.[267] The second matrix is the "ISPS/MTSA Compliance Targeting Matrix"[268] which evaluates compliance with security standards, rather than the actual security of the vessel. The third matrix is the "Port State Control (PSC) Safety and

---

[257] *See id.*

[258] U.S. COAST GUARD, PORT STATE CONTROL IN THE UNITED STATES: ANNUAL REPORT 2004, *available at* https://www.piersystem.com/external/index.cfm?cid=786&fuseaction=EXTERNAL.docview&documentID=76068.

[259] *See id*.

[260] 33 C.F.R. § 160.1(a) (2005).

[261] 33 U.S.C.S. 1221.

[262] 33 C.F.R. § 160.206 (setting forth the information that an NOA must contain).

[263] U.S. Coast Guard, ISPS/MTSA Compliance Targeting Matrix, *available at* http://www.uscg.mil/hq/g-m/pscweb/ISPS-MTSA.htm [hereinafter Targeting Matrix].

[264] *Id*.

[265] *Id.*

[266] *Id*.

[267] *Id*.

[268] *See* U.S. Coast Guard, ISPS/MTSA Compliance Targeting Matrix (PDF), *available at* http://www.uscg.mil/hq/g-m/pscweb/SecurityMatrix.pdf

Environmental Protection Compliance Targeting Matrix"[269] (formerly known as the "Foreign Vessel Targeting Matrix"), which evaluates the foreign vessel's compliance with both safety and environmental standards.

The objective of both the ISPS/MTSA Compliance Targeting Matrix and the PSC Safety and Environmental Protection Compliance Targeting Matrix is to help Captains of the Port or Officers-in-Charge, Marine Inspection identify which foreign vessels pose the greatest risk to U.S. ports.[270] "When applied consistently, the targeting regime will identify the appropriate risk level and corresponding boarding frequency for each vessel, ensuring that vessels posing a higher risk for noncompliance are boarded more frequently than vessels posing a lower risk."[271]

2. Role of Owners and Operators of Vessels and Port Facilities in Securing Container Ships Under the MTSA

Owners and operators of vessels, ports, and facilities must create comprehensive, Coast Guard-approved Security Plans and Incident Response Plans that incorporate the detailed vulnerability assessments and security recommendations issued by the Coast Guard.[272] The Security Plans must designate a qualified individual to implement security actions, and must be updated every five years.[273] The Response Plans must provide "a comprehensive response to an emergency, including [procedures for] notifying and coordinating with local, state, and federal authorities."[274] Following Coast Guard approval, the ports, waterfront facilities and vessels must operate in accordance with the Security and Response Plans.

In addition to domestic vessels, these requirements apply to certain foreign vessels. Although the MTSA is vague about the requirements of foreign vessels, the Area Maritime Security Regulations put forth by the

---

[269] *See* U.S. Coast Guard, Port State Control Safety and Environmental Protection Compliance Targeting Matrix, *available at* http://www.uscg.mil/hq/g-m/pscweb/SafetyTargetingMatrix.htm.
[270] Targeting Matrix, *supra* note 263.
[271] *Id*.
[272] *See* 46 U.S.C.S. § 70103(c)(3); *see also* Facility Security, 33 C.F.R. pt. 105; Vessel Security, 33 C.F.R. pt. 104.
[273] 46 U.S.C.S. § 70103(c)(3).
[274] *Id.* § 70104(b).

Coast Guard provide clarification.[275] Pursuant to the regulations, foreign vessels from SOLAS member states need not submit Security Plans to the U.S. government for approval.[276] Non-SOLAS foreign vessels,[277] however, must either have and comply with a Coast Guard-approved Security Plan, or comply with an alternative security plan or specific measures contained in a bilateral or multilateral agreement.[278]

3. Limited Ability to Secure Access and Identify Legitimate Seafarers Under the MTSA

In an attempt to remove some of the unknown elements involved in the international maritime transportation system and, thereby, protect the integrity of U.S. ports, the MTSA imposes restrictions on access to secure areas on vessels and in port facilities.[279] The MTSA also requires foreign crew to carry and present valid documentation while in U.S. jurisdiction, which includes U.S. territorial seas.[280]

a. Limited Access to Secure Areas

The MTSA regulates access to secure areas on vessels, in ports, and in waterfront facilities.[281] By limiting access to secure areas used to load, unload, and store containers and container ships, the MTSA ostensibly reduces the risk of sabotage in these areas.

Specifically, the MTSA requires DHS to develop a transportation security card for port workers to limit access to secure areas.[282] The Security Plan shall identify the areas covered by the cards. Although the MTSA designates who should receive transportation security cards, guidance is more inclusive than exclusive, and proscribes issuance of

---

[275] *See, e.g.*, Facility Security, 33 C.F.R. pt. 105; Vessel Security, 33 C.F.R. pt. 104.
[276] *See* Vessel Security, 33 C.F.R. pt. 104.
[277] A list of the SOLAS Contracting Governments as of 31 July 2005 is available online. *See* Int'l Mar. Org., Summary of Status of Conventions (31 July 2005), http://www.imo.org/Conventions/mainframe.asp?topic_id=247.
[278] *See* Area Maritime Security, 33 C.F.R. pt. 103.
[279] *See* 46 U.S.C.S. § 70105.
[280] *See id.*
[281] *See id.*
[282] *See id.*

cards unless an individual "poses a security risk . . . warranting denial of the card."[283]

The Transportation Security Administration is in the process of developing a Transportation Worker Identification Credential (TWIC) Program to meet the requirements of a transportation security card.[284] Under TWIC, background checks will be conducted but not released to the public.[285]

b. Seafarer Identification Requirements

Both the ISPS Code and the ILO discussed above[286] require methods for identifying legitimate seafarers and for preventing security breaches. The MTSA imposes similar requirements:

> The Secretary of the department in which the Coast Guard is operating is encouraged to negotiate an international agreement, or an amendment to an international agreement, that provides for a uniform, comprehensive, international system of identification for seafarers that will enable the United States and another country to establish authoritatively the identity of any seafarer aboard a vessel within the jurisdiction, including the territorial waters, of the United States or such other country.[287]

These requirements provide a necessary layer of protection against the unknown element of foreign crew arriving in U.S. ports. As discussed earlier, there is a threat that terrorists posing or legitimately working as crewmembers may tamper with containers or redirect container ships during transit, or may gain access to the United States via containers.[288] The MTSA enhances crewmember identification

---

[283] *Id.* § 70105(b)(1).
[284] *See* Trans. Security Admin., Industry Partners: TSA Pilots & Programs: Transportation Worker Identification Credential (TWIC) Program, http://www.tsa.gov/public/interapp/editorial/editorial_multi_image_with_table_0218.xml.
[285] *See supra* Part IV.D.
[286] *Id*.
[287] 46 U.S.C.S. § 70111.
[288] *See supra* Part II.B.

requirements for "vessels calling at United States ports."[289] All foreign crew must carry and present on demand "any identification that the Secretary [of DHS] decides is necessary."[290]

4. Protections Against the Many Unknown Sources Providing Goods in Containers Under the MTSA

Possible security breaches in container ships may take place when a container ship stops at multiple foreign ports before arriving at U.S. ports.[291] Although it is relatively difficult to tamper with containers that already have been loaded on ships due to limited space and access,[292] terrorists may seek an opportunity to sabotage a shipment while loading additional containers during stops. To address this concern, the MTSA permits the United States to limit what comes into its ports and, in effect, to boycott goods coming from high risk foreign ports. In addition, the MTSA attempts to provide U.S. port authorities with greater insight into the possible contents lurking within containers.

a. Antiterrorism Measures at Foreign Ports

Under the MTSA, the Coast Guard must determine if antiterrorism measures maintained at foreign ports are effective.[293] The Coast Guard also must notify government officials of a foreign country if it determines that the port fails to maintain effective antiterrorism measures.[294] Although CBP Officials are present at foreign ports under CSI,[295] the level of coordination between CBP and the Coast Guard to combine efforts in foreign ports is questionable.[296]

---

[289] 46 U.S.C.S. § 70111.
[290] *Id.* § 70111(a).
[291] *See supra* Part II.B-C.
[292] Flynn E-mail, *supra* note 28 (explaining that the gap between containers on a ship is only 8-12 inches. Therefore, few containers "are accessible once they are stowed").
[293] *See* 46 U.S.C.S. § 70108(a)(1); *see also* The Maritime Transportation Antiterrorism Act, H.R. 3983 (June 4, 2002) (tasking the Coast Guard with assessing security systems in certain foreign ports and denying entry to vessels from ports that fail to maintain effective security measures).
[294] 46 U.S.C.S. § 70108.
[295] *See infra* Part V.B.
[296] *See* Glover, *supra* note 176 (explaining that there are discussions between CBP and the U.S. Coast Guard to coordinate efforts but noting that "CBP and the Coast Guard are not bumping into each other"). *But see* Cunningham E-mail, *supra* note 107 (challenging

b. Uncertain Contents in Containers

The MTSA authorizes the CBP to require incoming foreign vessels to provide cargo manifests twenty-four hours before the cargo is laden on a vessel bound for a U.S. port.[297] These manifests contain explicit information on the claimed contents of the vessel.[298] Information on inbound or outbound shipments must be provided to the CBP electronically prior to the arrival or departure of the cargo.[299] This information may then "be shared with other appropriate federal agencies."[300]

As discussed earlier, the information contained on cargo manifests is only as reliable as those who provide it. [301] It is important, however, for federal agencies to have these manifests upfront, well before a container ship arrives in U.S. ports. Cargo manifests provided in advance of arrival allow federal agencies to consider the represented contents along with the history of ports visited in determining the risk level of the container ship.

To address the unreliability of cargo manifests, the MTSA attempts to "evaluate and certify secure systems of international intermodal transportation"[302] by setting standards and procedures to screen and assess cargo before it is loaded on a vessel in a foreign port bound for the United States. The MTSA also sets standards and procedures for securing cargo and monitoring security measures while the vessel is in transit.[303] Likewise, the MTSA calls for standards to increase the

---

this assertion and noting that "[a] number of country visits have been done jointly with not only CBP, but TSA and DOD," and "the Coast Guard is on every CSI country visit, and CBP has been on a number of USCG foreign assessments").

[297] *See* FRITTELLI, *supra* note 3, at 13. *See also* Area Maritime Security, 33 C.F.R. pt. 103 (LEXIS 2004); 19 U.S.C.S. § 1431; Presentation of Vessel Cargo Declaration to Customs Before Cargo is Laden Aboard Vessel at Foreign Ports for Transport to the United States, 67 Fed. Reg. 66,318 (Oct. 31, 2002) (to be codified at 19 C.F.R. pts. 4, 113, and 178).

[298] In addition, section 343 of the Trade Act of 2002, which was signed into law on 6 August 2002, provides CBP with the authority to issue regulations that require the electronic transmission of cargo information to CBP prior to the shipments' exportation or importation into the United States. The Trade Act of 2002, Pub. L. No. 107-210, 116 Stat. 933 (2002).

[299] FRITTELLI, *supra* note 3, at 13.

[300] *Id*.

[301] *See supra* Part II.C.2.

[302] 46 U.S.C.S. § 70116 (LEXIS 2005).

[303] *See id.*

physical security of containers, including the types of seals and locks used to prevent tampering.[304] The MTSA mandates creation of regulations that provide the United States with means to confirm and validate compliance with such procedures and standards.[305]

5. Addressing Container Ship Security Threats During Transit Under the MTSA

The MTSA protects against sabotage of container ships during transit by requiring seafarer identification and limiting access to secure areas on vessels and in port facilities.[306] By legitimizing those on container ships through affirmative methods of identification, containers loaded on foreign ships at foreign ports are less likely to be tampered with before or during transit, or upon arrival at U.S. ports. The MTSA provides for additional protection against security risks during transit by mandating domestic and foreign deployment of Automatic Identification Systems (AIS) for certain types of vessels.[307] Automatic Identification Systems consist of a VHF maritime radio for vessels and specific shore stations that broadcasts unique identifiers and safety information about a vessel.[308] Vessels required to have AIS include self-propelled commercial vessels sixty-five feet or longer, vessels that carry a particular number of passengers for hire (as specified by DHS), towing vessels longer than twenty-six feet and with 600 horsepower, and any other vessel DHS deems necessary for safe navigation.[309]

The Coast Guard implemented this specification of the MTSA by adopting certain AIS carriage and operational requirements for certain classes of U.S. flag vessels and foreign commercial vessels, including container ships.[310] In addition to providing mariners with accurate information on a vessel, AIS provides information on the type of cargo, as well as the vessel's destination and estimated time of arrival.[311] With

---

304 *See id.*
305 *See id.*
306 46 U.S.C.S. § 70111.
307 *See id.* § 70114.
308 *See id.* §§ 70114, 70116.
309 *See id.*
310 *See, e.g.*, 33 C.F.R. pt. 164.46 (LEXIS 2005). *See also* Automated Identification Systems, 33 C.F.R. pts. 26, 161, 164 (LEXIS 2005).
311 *See* Automated Identification Systems, 33 C.F.R. pts. 26, 161, 164, 165 (LEXIS 2005).

AIS devices in place on foreign container ships, the Coast Guard is able to identify the vessel, its position, and a variety of other factors that may not be available through traditional radio or radar methods. If the AIS information is inconsistent with the cargo manifests, the history of foreign ports visited, or the GPS position of the vessel, U.S. authorities may be put on alert before a suspect vessel arrives in a domestic port. Therefore, if fully implemented and monitored, AIS has the potential to be one of the more creative and effective layers in container ship security.

6. Coordination and Exchange of Information Under the MTSA

The exchange of information, particularly intelligence information about sources scheduled to arrive in U.S. ports, must be broadly disseminated to federal and local agencies in order to avoid security breaches. Naturally, a system of gathering information is only useful if that information is disseminated to the proper authority equipped to respond to potential threats.

The MTSA provides for such exchange of information by setting up local port security committees to coordinate efforts of federal, state, local, and private law enforcement agencies and to advise on Security Plans.[312] The agencies include the FBI, the CBP, and the Coast Guard. Maritime intelligence systems collect and analyze information concerning vessels operating in U.S. waters, as well as their crew, passengers, and cargo. Thus, under the MTSA, agencies will collaborate and exchange their intelligence under a maritime intelligence regime.[313]

7. Security Layers Provided by the MTSA Fail to Protect U.S. Ports

As noted above, many of the MTSA requirements directly implement the international security requirements adopted by the IMO in the ISPS Code.[314] Therefore, the MTSA contains many of the same

---

[312] *See* 46 U.S.C.S. § 70112. The Coast Guard implemented the MTSA requirement for Maritime Security Advisory Committees. *See* 33 C.F.R. pts. 103.300, 103.305, 103.310 (LEXIS 2005).

[313] 46 U.S.C.S. § 70112; *see also* 33 C.F.R. pts. 103.300, 103.305, 103.310 (LEXIS 2005).

[314] *See supra* Part V.A.

weaknesses as the ISPS Code. Specifically, the MTSA does not adequately address the nature of goods loaded in foreign ports.[315] While the MTSA imposes additional requirements upon domestic and foreign vessels and facilities that the ISPS Code lacks, the MTSA also leaves many gaps in the security of container ships by failing to recognize the nature of modern-day terrorists.[316]

Identification requirements for seafarers, and limited access to secure areas on ships, ports, and, facilities may deter unsophisticated terrorists or saboteurs. These measures, however, do not contemplate the complicated terrorist threat that the United States faces today, particularly the patient and persistent threats presented by al Qaeda. The MTSA's identification cards will likely be inadequate to counter this threat. The cards will be generated based on presentation of mariner documents, but these documents can be counterfeited or forged by today's sophisticated terrorists. Furthermore, the greater concern is that today's recruited terrorists may obtain valid identification cards without triggering security concerns because they do not have a suspect past.[317] Just as there are concerns that terrorists may be involved in the flight industry,[318] terrorists already may be involved in the shipping industry. While identification cards may be a meaningful way to identify known terrorists, they will neither protect U.S. ports from sophisticated terrorists with counterfeit or forged identification cards, nor will they protect U.S. ports from terrorist recruits who lack a remarkable or known past. The MTSA and the ISPS Code's identification recommendations and mandates are a reasonable security layer, but they still leave U.S. ports exposed. In addition, the identification systems may provide a false sense of security and lead officials to ignore otherwise obvious actual or potential security breaches.

---

[315] The author does not imply that the MTSA was specifically designed to address the nature of goods loaded in foreign ports, but simply points out that the MTSA does not provide adequate safeguards to address such security risks.

[316] Historically, the terms "terrorism" and "terrorist" are not well or consistently defined. This article uses the term "terrorist" interchangeably with "member of al Qaeda" in light of the 9/11 attacks.

[317] George Jonas, *Biometrics Won't Catch Disposable Terrorists*, NAT'L POST, Jan. 19, 2004, *available at* http://www.hspig.org/ipw-web/bulletin/bb/viewtopic.php?t=555.

[318] *Id*.

a. Identification Cards are Subject to Forgery or Counterfeiting

Recent events demonstrate the technological sophistication of terrorists. For example, individuals linked to al Qaeda operatives maintain that "'[i]f you have the right connection, you can get anything.'"[319] A former member of a terrorist cell in Detroit, Youssef Hmimssa, found it simple to obtain birth certificates, social security cards, driver's licenses, and U.S. passports.[320] According to Hmimssa, he easily purchased passports and social security cards on the black market.[321] Using a home computer and readily available "special" ink for government documents, he was able to forge identification documents for other members of his terrorist cell.[322] Although Hmimssa's fraud took place in 1994, similar means for breaching security measures may still exist today.

As part of an investigation, members of the Office of Special Investigations (OSI) in the Inspector General's (IG) office at the Government Accountability Office (GAO) obtained driver's licenses using forged documents in each of the eight states they visited.[323] The forged documents included licenses from other states created with inexpensive computer programs. Using these fake identification cards, the investigators drove a truck into a Justice Department courtyard.[324]

If social security cards, driver's licenses, and passports are readily available to terrorists, it follows that counterfeit mariner documents and, subsequently, seafarer identification cards will also be attainable, and that valid identification cards will be available for misuse and forgery. "[H]omeland security is vulnerable to identity fraud and, unless action is taken, individuals who intend to cause harm can easily exploit these vulnerabilities."[325]

---

[319] *Fake U.S. IDs Easy for Terrorists*, CBS NEWS, Sept. 9, 2003, *available at* http://www.cbsnews.com/stories/2003/09/09/attack/main572405.shtml (quoting Youssef Hmimssa, former member of a terrorist cell).

[320] *See id.*

[321] *See* Jeff Johnson, *Federal Agents, Illegal Aliens Say IDs Easy to Forge*, THE NATION, Sept. 10, 2003, *available at* http://www.cnsnews.com/National/archive/200309/NAT20030909/NAT20030910a.html.

[322] *See Fake U.S. IDs Easy for Terrorists*, *supra* note 319.

[323] *See id.*; *see also* Johnson, *supra* note 321.

[324] *See Fake U.S. IDs Easy for Terrorists*, *supra* note 319.

[325] Johnson, *supra* note 321 (quoting Robert Cramer, the managing director of the GAO's IG-OSI).

b. Biometric Identification Systems Fail to Protect Against Today's Terrorists

There are ongoing efforts to improve identification systems by using biometric markers, including fingerprints. While identification containing biometric markers may be less susceptible to forgery or counterfeiting, it is questionable whether these technologically advanced forms of identification would address the threat of today's terrorists. First, a functional biometric system of identification may be years away.[326] Biometric identification "is a technology that has been thrust ahead of its growth curve."[327] Technology is "moving so fast that before it has a chance to be in front of a legislative panel . . . the technology has already been breeched."[328] Second, while biometric identification systems may prevent attacks by known or suspected terrorists, these security measures may be ineffective against threats in the post-9/11 world.[329] "Biometrics are yesterday's solution for today's problem."[330]

---

[326] *See* FRITTELLI, *supra* note 3, at 21; *but see* Carol DiBattiste, Deputy Administrator for the Transportation Security Administrator, U.S. Department of Homeland Security, Speech at the 4th Annual International Conference on Public Safety: Technology & Counterterrorism (Mar. 14, 2005) (explaining that a prototype of the TWIC identification card for aviation should be complete by May 2005, but that combined efforts with the U.S. Coast Guard to create an identification card for maritime workers may be coordinated "next year").

[327] *See* Raj Nanavati, Partner with International Biometric Group, Speech at the 4th Annual International Conference on Public Safety: Technology & Counterterrorism (Mar. 15, 2005).

[328] *Cf.* R. David Henze, Business Development Executive, IBM Global Services, Speech at the 4th Annual International Conference on Public Safety: Technology & Counterterrorism (Mar. 14, 2005) (discussing cyber-terrorism). While Mr. Henze's statement referred to cyber-terrorism, the underlying premise—that terrorists are sophisticated and creative enough to circumvent advances in technological security measures—applies equally to biometric identification systems. *Id. See* Jacques Duchesneau, President and Chief Executive Officer of Canadian Air Transportation Security Authority, Speech at the 4th Annual International Conference on Public Safety: Technology & Counterterrorism (Mar. 14, 2005) (stating that a growing dependence upon computer technology is not foolproof and pointing out that "our enemy [al Qaeda] has the same tools that we do").

[329] *See* Jonas, *supra* note 317.

[330] *Id. See* NATO PARLIAMENTARY ASSEMBLY, SUB-COMMITTEE ON THE PROLIFERATION OF MILITARY TECHNOLOGY, TECHNOLOGY AND TERRORISM (2001), *available at* http://www.tbmm.gov.tr/natopa/raporlar/bilim%200ve%20teknoloji/AU%20121%20STC% (discussing threats of WMDs or computer attacks by terrorists due to the changing nature and means of terrorists).

"If you know the enemy and know yourself, you need not fear the result of 100 battles."[331] This sage advice was provided 2500 years ago by Sun Tsu in *The Art of War*, and it still rings true today. Existing security measures fail to counter what the United States knows of the enemy. Unfortunately, the means by which the United States will learn more about the enemy facing it today will likely be through more attacks or breaches in existing security measures. Pre-9/11 terrorists often participated in multiple missions, while post-9/11 terrorists are characterized as "disposable."[332] Disposable terrorists, including suicidal militants recruited by al Qaeda, have no future, "but more importantly, they're without a past."[333] Consequently, if al Qaeda recruits members for suicide missions who have no past records, they will not trigger security alerts even assuming that the most advanced system of biometric identification is in place.

As an example, the "shoe bomber," Richard Reid, was traveling with a valid British passport under the Visa Waiver Program when he was discovered trying to ignite plastic explosives hidden in his shoes during a flight.[334] No form of biometric identification will protect against these disposable terrorists because they do not match any profiles contained in maintained database systems. "The most sophisticated scanning device is useless if it functions by comparing the present with the past."[335] Failure to acknowledge the limited usefulness of biometric identification may foster a false sense of security which is likely to be compounded as biometric systems advance in order to justify the expense and time devoted to developing them. "Like bees, disposable terrorists die as they sting—but unlike bees, they cannot be recognized for what they are until they've stung."[336] This illustrates the weakness in relying too heavily upon biometric identification cards as a layer in container ship security.

---

[331] SUN TZU, THE ART OF WAR 37 (Lionel Giles trans. 1963) (circa 500 b.c.).
[332] Jonas, *supra* note 317.
[333] *See Oversight Hearing on "Should Congress Extend the October 2004 Statutory Deadline for Requiring Foreign Visitors to Present Biometric Passports?" Before the House Judiciary Committee* (2004) (testimony of Secretary Powell) (stating that it was his understanding that Richard Reid had a legitimate French or British passport issued under the Visa Waiver Program).
[334] Lucy Sherriff, *U.S. Extends Biometric Passports Deadline*, REG. (U.K.), June 17, 2004, *available at* http://www.theregister.co.uk/2004/06/17/biometric_delayed/.
[335] Jonas, *supra* note 317 ("The more sophisticated the high-tech side becomes, the more it exposes itself to an end-run by the low-tech side.").
[336] *Id.*

Furthermore, reliance on a biometric system of identification may actually protect otherwise known terrorists. Biometric identification cards link a person to physical characteristics, e.g. fingerprints, retina, or iris patterns.[337] The identity of a person who obtains a TWIC identification card, however, will be based on other forms of identification presented at the time the biometric information is entered into the database.[338] Consider a terrorist whose name and picture are on a watch list, but who has no pre-existing biometric information entered into a governmental system. If he easily attains false documents linking him to a different identity, his biometric information will tie him to the name on the false documents rather than to his true identity. Carol DiBattiste, the Deputy Administrator of TSA, emphasizes that utilizing biometric identification and automated systems to screen passengers decreases the rate of human error and "reduces in half the number of passengers selected for pre-screening."[339] Focusing on technology to detect potential terrorists, however, may prove disastrous.

Not only does biometric focus promote reliance on a system that may not detect many of today's terrorists, but it also overlooks the necessary tool of a screener's gut instincts. Consider Jose Melendez-Perez, an immigration inspector at Orlando's International Airport, who denied airline access to al-Qahtani, the twentieth would-be hijacker in the 9/11 attacks.[340] As Mr. Melendez-Perez explains, "[t]he bottom line is: he gave me the creeps."[341] Emphasis on terrorist identification through biometric systems may have allowed al-Qahtani to slip through the cracks.

B. The Customs-Trade Partnership Against Terrorism and the Container Security Initiative

The C-TPAT and the CSI are creative initiatives involving the CBP, foreign ports, and businesses. The mission of both initiatives is to create a system of agreements among those interested in securing the integrity

---

337 *See* Carol DiBattiste, *supra* note 326.
338 *Id*.
339 *See id*.
340 *Id*.
341 Seventh Public Hearing of the National Commission on Terrorist Attacks Upon the United States, Jan. 26, 2004 (statement of Jose E. Melendez-Perez), *available at* http://www.9-11commission.gov/hearings/hearing7/witness_melendez.htm.

of maritime trade, to avoid security breaches.[342] The C-TPAT and the CSI involve the active participation of the shipping community, but they still leave gaps in container ship security that could prove fatal and economically devastating if exploited by terrorists.

1. The Customs-Trade Partnership Against Terrorism

The C-TPAT, announced by Commission Bonner in November 2001 and initiated in April 2002, is a series of agreements between private businesses and governments designed to strengthen the maritime transportation system by improving the integrity of the supply chain.[343] The agreements focus on cargo security rather than vessels, ports, and facilities, by encouraging those engaged in carrying goods to share information about the supply chain and to become involved in efforts to assess the security risks.[344] The C-TPAT recognizes that the CBP is in a position to provide a high level of security only in concert with the individuals involved in the supply chain: "importers, carriers, brokers, warehouse operators and manufacturers."[345]

In order to participate, businesses sign an agreement to do the following: (1) assess their current supply chain security measures by applying guidelines developed by the trade community and the CBP; (2) provide the CBP with a completed supply chain security profile questionnaire; (3) create and implement a program to increase security throughout the supply chain and consistent with C-TPAT guidelines; and (4) inform other companies in the supply chain of the C-TPAT security guidelines in hopes of incorporating such guidelines into the working relationship with these companies.[346]

Currently, more than 9,000 companies participate in the C-TPAT program.[347] It is anticipated that business participants will contribute to

---

[342] *See C-TPAT FAQ*, *supra* note 7; FRITTELLI, *supra* note 3, at 11.

[343] *See C-TPAT FAQ*, *supra* note 7.

[344] Robert G. Clyne, *Symposium: Admiralty Law Institute: Confused Seas: Admiralty Law in the Wake of Terrorism: Terrorism and Port/Cargo Security: Developments and Implications for Marine Cargo Recoveries*, 77 TUL. L REV. 1183, 1197 (2003).

[345] *C-TPAT FAQ*, *supra* note 7.

[346] *See id.* Irvin Lim Fang Jau, *Not Yet All Aboard . . . But Already All at Sea Over the Container Security Initiative*, J. HOMELAND SECURITY 11 (Nov. 2002), *available at* http://www.homelandsecurity.org/journal/articles/jau.html.

[347] Robert C. Bonner, Commissioner of the U.S. Customs and Border Protection Remarks to the Kansas City Chamber of Commerce in Kansas City, Missouri (May 16,

a collective effort to secure the supply chain worldwide, thereby leading to a more secure transaction for the business's employees, suppliers, and customers.[348] As an added incentive, the CBP will provide participating businesses with other benefits, including access to a list of other C-TPAT members and a reduction in the number of inspections, which, consequently, results in less time spent at borders.[349] "The material benefit to membership in C-TPAT is that less verification by U.S. Customs should be necessary because more self-policing is expected to occur. This, in turn, should lead theoretically to fewer inspections and an attendant decrease in expense and delay in the C-TPAT member's commercial undertakings."[350] It is anticipated that the emphasis on self-policing rather than CBP inspections may appeal to many businesses.[351]

2. The Container Security Initiative

The CSI is an initiative that the CBP began in late 2002 to protect against the use of global trade containers for terrorist acts, including transportation of WMD.[352] CSI partnerships involve foreign governments that allow CBP agents in their ports to identify high-risk containers bound for the United States.[353] Currently, the CSI is operating at thirty-seven[354] ports in Europe, Asia, Africa, and North America, which "represent the world's major seaports."[355]

2005), *available at* http://www.customs.gov/xp/cgov/newsroom/commissioner/speeches_statements/05162005_kansas.xml.

348 *Id*.

349 *Id*.

350 Clyne, *supra* note 344, at 1199.

351 *See C-TPAT FAQ*, *supra* note 7.

352 *See id*; *see also* Presentation of Vessel Cargo Declaration to Customs Before Cargo is Laden Aboard Vessel at Foreign Ports for Transport to the United States, 67 Fed. Reg. 66,318 (Oct. 31, 2002) (to be codified at 19 C.F.R. pts. 4, 113, and 178).

353 FRITTELLI, *supra* note 3, at 11.

354 U.S. Customs and Border Protection, CBP's Container Security Initiative Provides Roadmap to International Trade Accord, U.S. CUSTOMS AND BORDER PROTECTION TODAY (July/Aug 2005), *available at* http://www.customs.gov/xp/CustomsToday/2005/Jul_Aug/csi.xml (stating that CSI is "operational at 37 ports around the world").

355 Bonner, *supra* note 2 (stating that CSI is operational in thirty-five of the largest ports); *see also* Press Release, U.S. Customs and Border Protection, U.S. Customs and Border Protection Achieves Container Security Initiative (CSI) Milestone of 25 Operational Ports (Aug. 25, 2004), *available at* http://www.customs.gov/xp/cgov/newsroom/press_releases/archives/2004_press_releases/08302004/08252004.xml (quoting Commissioner Bonner).

The CSI complements the C-TPAT and contains four major components: (1) to transmit automated information to identify and target containers that pose a high security risk; (2) to pre-screen high-risk containers before they arrive in U.S. ports; (3) to use cutting-edge technology to quickly assess and pre-screen high-risk containers; and (4) to develop "smart" tamper-resistant containers.[356]

To help target high risk containers and meet the first component, all CSI and non-CSI ports must submit cargo manifests twenty-four hours before loading containers on ships bound for U.S. ports.[357] When CBP receives electronic transmission of advance cargo manifests, the National Targeting Center considers the information in conjunction with data, intelligence, and the ship's history to target potentially high-risk cargo.[358] Under the theory of the CSI, pre-screened containers will be processed faster.[359] As part of this process, the CSI is designed to identify and process low-risk containers easily and quickly. By weeding out the low-risk containers, the CSI process of elimination helps define which containers may be high-risk, thereby accomplishing the CSI's second component.[360] Cutting-edge technology involving large x-ray and gamma ray machines, as well as radiation detection devices, are currently in use to meet the third component of the CSI—to quickly assess and pre-screen high-risk containers before they depart for the United States. These pre-screening methods only take ninety seconds.[361] Research into the fourth component of CSI, calling for "smart" and tamper-resistant

---

[356] Bonner Speech, *supra* note 4 (announcing CSI).

[357] Advanced notice of arrival requirement differs from advanced submissions of cargo manifests. Notice of arrival must be submitted ninety-six hours before the vessel departs, or twenty-four hours before the vessel departs if the voyage will be less than ninety-six hours. Advanced cargo manifests must be submitted twenty-four hours before the containers are loaded onto a container ship. *See* 67 Fed. Reg. 66,318, 66,319-21. *See also* J. Ashley Roach, Container and Port Security: A Bilateral Perspective, Address to the Symposium on Interference with Navigation: Modern Challenges, International Tribunal for the Law of the Sea in Hamburg, F.R.G. 19 (Mar. 15, 2003) (explaining the ninety-six hour advanced notice requirement); U.S. Customs and Border Protection, Frequently Asked Questions: 24-Hour Advance Vessel Manifest Rule (Apr. 16, 2004), *available at* http://www.customs.gov/linkhandler/cgov/import/carrier/24hour_rule/cbp_24hr.ctt/cbp_24hr.doc.

[358] *See* Tom Ridge, Former Secretary of Homeland Security, Remarks at Port of Los Angeles (June 21, 2004), *available at* http://www.dhs.gov/dhspublic/display?theme=44&content=3728&print=true.

[359] *See* Roach, *supra* note 357, at 5, 6 (explaining how inspections done while containers are in storage will save time).

[360] *See id.* at 4.

[361] *See id.* at 6.

containers, is already underway. In particular, there has already been progress in designing tamper-resistant electronic seals.[362]

As with C-TPAT business participants, ports that join the CSI will enjoy certain benefits, including reduced transportation times and fast-lane access.[363] In trade, time is most certainly money, so any reduction in the length of time it takes to get goods to their final destination provides tremendous incentives for businesses. The mere presence of U.S. customs inspectors in foreign and domestic ports should expedite the processing of containers. Although most containers remain in a terminal for several days prior to being loaded onto a ship, U.S. Customs inspectors will be able to screen containers while they are sitting in the terminal during "down time."[364] Shipments from CSI ports will enjoy expedited inspections while in foreign ports and will be processed immediately.[365] In fact, "CSI-screened container[s] should be released immediately by U.S. Customs, which could shave hours, if not days, off of the shipping cycle. In this manner, the CSI should increase the speed and predictability for the movement of cargo containers shipped to the U.S."[366] CBP will not inspect containers sealed under CSI when they arrive in U.S. ports, absent "additional information affecting [the container's] risk analysis."[367]

3. The C-TPAT and the CSI Fail to Remedy Security Threats Presented by Containers

The C-TPAT and the CSI initiatives address many of the security gaps for container ships left by the ISPS Code and the MTSA. As Dr.

---

[362] *See id*.

[363] *See* Fang Jau, *supra* note 346, at 11. However, the fast-lane or "green lane" access for C-TPAT and CSI businesses and ports is not yet in effect and is not anticipated to go into effect until the end of 2005. *See also* Ned Ahearn, Partner with North American Supply Chain Management, Unisys Corporation, Speech at the 4th Annual International Conference on Public Safety: Technology & Counterterrorism (Mar. 14, 2005).

[364] Roach, *supra* note 357, at 16 (stating that screening containers during "down time" will expedite the inspection process). *See* Presentation of Vessel Cargo Declaration to Customs Before Cargo is Laden Aboard Vessel at Foreign Ports for Transport to the United States, 67 Fed. Reg. 66,318, 66,319 (Oct. 31, 2002).

[365] *See* Flynn E-mail, *supra* note 28.

[366] 67 Fed. Reg. at 66,319. *See* Roach, *supra* note 357, at 16 (noting that CSI compliance will speed up the flow of trade, and explaining that pre-screened and sealed containers will not need further inspection when they reach U.S. ports).

[367] 67 Fed. Reg. at 66,319.

Flynn astutely points out, however, "none of these programs address [sic] the core cargo security imperative of confirming that the goods loaded into a container from the start are indeed legitimate and that the container has not been intercepted and compromised once it is moving within the transportation system."[368] In addition, while incentive for foreign ports and companies to agree to participate in the C-TPAT and the CSI is high, actual compliance with the initiatives is not subject to oversight or enforcement. "When everyone's responsible, there's a question of who's accountable."[369] Therefore, actual compliance remains a serious issue.

a. The C-TPAT Initiative Lacks Adequate Enforcement and Oversight

One of the problems with the C-TPAT is that it is not subject to governmental enforcement or oversight. Essentially, the agreement is self-policed. An additional problem with the C-TPAT is that it does little to fill gaps regarding the legitimacy of shipped cargo and, instead, creates yet another level of unjustified reliance on businesses based solely on their agreement to participate in the program.

Because C-TPAT is self-policed, enforcement and compliance are questionable. As discussed, the United States relies in large part on the cargo manifests and other documents that accompany container shipments.[370] These documents include statements by shippers, sellers, and port authorities, each of whom may have incentives to misrepresent the contents of their shipments. While C-TPAT businesses agree to participate voluntarily, they may also have an incentive to feign compliance. Furthermore, there is no enforcement mechanism against those who fail to abide by their agreements. It appears that the only leverage against C-TPAT participants who fail to honor their agreement is removal of their priority status upon discovery of noncompliance. It is unlikely that noncompliant businesses will be exposed until a security violation has already taken place, however, because no oversight of the C-TPAT program is in effect. Those ports and businesses who have agreed to comply with the C-TPAT may "prefer to adopt an

---

[368] FLYNN, *supra* note 1, at 107.
[369] Edgar A. MacLeod, President of Canadian Association of Chiefs of Police, Speech at the 4th Annual International Conference on Public Safety: Technology & Counterterrorism (Mar. 14, 2005).
[370] *See supra* Part II.C.2.

incrementalist wait-and-watch approach in actual implementation," to defer expense and inconvenience.[371] "The carrot of facilitation that comes from participating in these programs is not matched by a credible stick."[372]

Enticing private businesses with promises of efficiency is a creative approach to maritime security. However, it introduces another level of reliance and another level of unknowns, which further complicate, rather than strengthen, security of container ships. As the Stanford Study Group recognized in their Container Security Report, "measures adopted voluntarily by commercial operators are, in general, not adequate to the task of ensuring reliable detection of smuggled nuclear weapons and SNMs [Special Nuclear Material]."[373] The C-TPAT security layer functions according to a misplaced belief that there is sufficient market incentive for the public to protect itself.[374]

b. The CSI's Inadequate Implementation and Enforcement Mechanisms

Like the C-TPAT, the CSI is also difficult, if not impossible, to adequately implement or enforce, because CBP inspectors have no enforcement powers overseas.[375] Similarly, the CBP "lacks the manpower and resources to adequately staff the Container Security Initiative, to review the applications of companies who wish to participate in C-TPAT, and to move away from error-prone cargo manifests that remain the cornerstone of its targeting system."[376] Although CSI is operational in thirty-seven ports, the physical burden placed upon CBP agents to pre-screen containers does not address the

---

[371] Fang Jau, *supra* note 346, at 5.

[372] FLYNN, *supra* note 1, at 107.

[373] CISAC THE STANFORD STUDY GROUP, *supra* note 7, at 5 (recognizing that "the permissible failure rate for commercial inspection systems falls short of a tolerable threshold for security . . . . [and] a more sophisticated strategy is required to fulfill the objective of preventing incidents of nuclear terrorism on U.S. territory."). *See* FLYNN, *supra* note 1, at 130 ("Relying on best practices and industry self-policing was acceptable for meeting our pre-9/11 regulatory needs, but they are simply inadequate in the post-9/11 security world.").

[374] *See* Stephen E. Flynn, Homeland Security Expert and Former U.S. Coast Guard Commander, Speech at the 4th Annual International Conference on Public Safety: Technology & Counterterrorism (Mar. 15, 2005).

[375] *See* Roach, *supra* note 357, at 7.

[376] FLYNN, *supra* note 1, at 107.

central threat. Assuming that it is possible to prescreen a substantial portion of the containers at CSI ports, failure to catch just one dangerous item contained in an otherwise low risk container could have the devastating consequences anticipated in Part III.[377]

c. Neither the C-TPAT nor the CSI Meets the Functional Objective of Keeping Ports Opened When There is a Breach in Security

Authorities maintain that the C-TPAT and CSI initiatives will help return the necessary flow of maritime commerce if an attack were to occur using a container.[378]

> [The CBP] believes the CSI network of ports will be able to remain operational because those ports will already have an effective security system in place—one that will deter and prevent terrorists from using them. Without such a network, the damage to global trade caused by a terrorist attack involving international shipping would be staggering.[379]

This argument, however, is counter-intuitive. An attack via container would prove either that the security measures relied upon were not in place, or that they were inadequate. Therefore, it would be necessary to close ports—and at least temporarily halt maritime transportation—to conduct a full review and determine which of the layers in the system failed. "When bad things happen, communications aren't there anymore."[380] Thus, the security measures implemented by the C-TPAT and CSI tend to create a false sense of security and, even in conjunction with the ISPS Code and the MTSA, do not provide a reliable security layer for container ships.

VI. Conclusion and Recommendations

The layers of container ship security must protect U.S. ports throughout the supply chain. Security measures must protect against the

---

[377] *See* Fang Jau, *supra* note 346, at 8.
[378] 67 Fed. Reg. 66,318, 66,319-20.
[379] *Id.* Roach, *supra* note 357, at 16.
[380] Ahearn, *supra* note 363.

following: loading a container with illegitimate cargo while overseas; fraudulent reporting of cargo to the CBP; and tampering with or redirecting a container during transit.[381] The existing layered defense provides some protection, however, it does not resolve the blind faith reliance placed on the container ship supply chain. Instead, existing measures provide a number of additional levels of reliance upon statements made by foreign ports, individuals, and businesses who stand to gain substantially from their representations. There is no accountability or enforcement mechanism, however, to assure the reliability of these statements.

Existing security layers also fail to acknowledge today's terrorists. Today's terrorists may travel using their own names with valid documentation on container ships. They may travel on ships and through ports that comply with the ISPS Code and the MTSA. They may travel on container ships carrying goods loaded in foreign ports where CBP officials are stationed in accordance with the CSI. They also may travel on ships carrying goods from businesses that participate in the C-TPAT. Layered security defenses, however, may not detect or prevent the transportation of a WMD via container ship. The MTSA, ISPS Code, CSI, and C-TPAT promote a false sense of security in existing protections of U.S. ports, because they easily may be circumvented. In order to protect the integrity of container ships, authorities must recognize the nature of terrorist threats and acknowledge that security measures will be breached.[382] "[W]e need to plan for the eventuality that our security measures will be imperfect."[383] While maintaining existing security layers, authorities must now focus on and dedicate substantial resources to detection devices that keep the transportation system moving at an economically feasible rate. "Adopting smart and secure containers becomes the only way to stay competitive."[384]

The importance of smart containers with imbedded devices to detect certain contents, including nuclear and biological material, has been

---

[381] FRITTELLI, *supra* note 3, at 17.

[382] *See* HART, *supra* note 2, at 18 ("If an explosive device were loaded in a container and set off in a port, it would almost automatically raise concern about the integrity of the 21,000 containers that arrive in U.S. ports each day and the many thousands more that arrive by truck and rail across U.S. land borders."); *see also* Bonner, *supra* note 2 (stating that 25,000 containers arrive in U.S. ports each day and that nine million containers arrive in U.S. ports annually).

[383] FLYNN, *supra* note 1, at 78.

[384] *Id.* at 104.

acknowledged.[385] Unfortunately, efforts have concentrated predominantly on creating tamper-resistant containers. For instance, the TSA and CBP are conducting the Operation Safe Commerce (OSC) pilot project.[386] OSC funds business initiatives to help "analyze security in the commercial supply chain and test solutions to close security gaps."[387] DHS awarded the private sector fifty-eight million dollars in grants since its inception, and awarded another seventeen million dollars during the summer of 2004.[388] Despite the fact that imbedded detection devices clearly fall within the realm of OSC, the project has focused on tamper-resistant containers and GPS tracking capabilities.[389]

Similarly, the MTSA authorizes ninety million dollars in grants devoted to research and develop improvements in cargo inspection, nuclear material detection devices, and improvements in the physical security of containers.[390] However, it appears that these grants also have been devoted to funding research on tamper-resistant container seals.[391]

While tamper-resistant containers provide a necessary layer in securing the supply chain, imbedded detection devices may be equally important. A partial solution to the missing layer of defense may already be well underway in both the public and private sectors. In fact, a wide array of anti-terrorism detection devices are currently being researched and developed.[392] Some of the most promising devices have multi-

---

[385] *See, e.g.*, U.S. DEPARTMENT OF HOMELAND SECURITY: OFFICE OF STATE AND LOCAL GOVERNMENT COORDINATION AND PREPAREDNESS, OFFICE FOR DOMESTIC PREPAREDNESS, OPERATION SAFE COMMERCE PHASE III: PROGRAM AND APPLICATION GUIDELINES, *available at* http://www.ojp.usdoj.gov/odp/docs/FY05_OSC_revised.pdf [hereinafter DHS: COORDINATION AND PREPAREDNESS] (last visited Mar. 20, 2005) (providing grant funds for pilot projects involving the three largest container load centers in the U.S.: the Ports of Seattle and Tacoma; the Port Authority of New York and New Jersey; and the Ports of Los Angeles and Long Beach); *see also* FLYNN, *supra* note 1, at xv.

[386] *See* DHS: COORDINATION AND PREPAREDNESS, *supra* note 385.

[387] U.S. DEPARTMENT OF HOMELAND SECURITY, SECURE SEAS, OPEN PORTS: KEEPING OUR WATERS SAFE, SECURE AND OPEN FOR BUSINESS 5 (2004), *available at* http://www.dhs.gov/ interweb/assetlibrary/DHSPortSecurityFactSheet-062104.pdf.

[388] *See id. But see* FLYNN, *supra* note 1, at 108 (explaining that OSC is managed by TSA but has not received any 2005 fiscal year funding despite the fact that three of the largest US ports (NY, Seattle, and LA) are operating under OSC and adopting tests to fine-tune it).

[389] *See* FLYNN, *supra* note 1, at 108 (discussing the Smart Box Initiative designed to produce tamper-evident containers).

[390] *See* FRITTELLI, *supra* note 3, at 13.

[391] *See id.*; *see also* 46 U.S.C.S. § 70107 (2000).

[392] *See* Dep't of Energy, National Nuclear Security Administration Terrorism Technologies, http://www.au.af.mil/au/awc/awcgate/doe/nnsa_terrorism_tech_v.htm (last

sensor chemical and radiation detection monitors, as well as network capabilities for DHS.[393] While current funding may be insufficient to fine-tune these devices, such devices are necessary to provide a key missing layer in protecting U.S. ports from the threats presented by container ships.

In addition to imbedded detection devices, extensive and efficient radiological screening devices may provide a necessary layer to protect against the eventual breach of existing security defenses. Although CBP officers "already use[] scanning technology at hundreds of American ports as well as many land border crossings" and have "hand held radiation scanners . . . at every major U.S. port," these scans are used only on high risk containers. [394] Existing U.S. scanning techniques are considered "an alternative or precursor to physical inspections, and the scan images are never stored."[395]

In contrast, a pilot project in Hong Kong[396] provides an example of how expansive container scanning could work in the United States. The Container Terminal Operators Association of Hong Kong[397] sponsors a security regime project which scans each container arriving at "two of the busiest marine terminals in the world" with a "gamma ray machine, a radiation portal, and optical character recognition cameras which record the container number."[398] The startup equipment for such a screening

---

visited Mar. 22, 2005) (explaining various devices being developed to detect nuclear, chemical, and biological agents).

[393] *See, e.g.*, RAE SYSTEMS INC., SECURING THE SUPPLY CHAIN: CONTAINER SECURITY AND SEA TRIAL DEMONSTRATION RESULTS (2005), http://www.raesystems.com/~raedocs/Securing_the_Supply_Chain_011205.pdf. Rae Systems is a leading global developer and manufacturer of container security devices that were tested at sea during October and November, 2004. *Id.*

[394] Alex Ortolani & Robert Block, *Hong Kong Port Project Hardens Container Security*, WALL ST. J., July 29, 2005, *available at* http://www.post-gazette.com/pg/05210/545822.stm.

[395] *Id*.

[396] *See Addressing the Shortcomings of the Customs-Trade Partnership Against Terrorism (C-TPAT) and the Container Security Initiative*, *supra* note 198, at 7.

[397] *See* Ortolani & Block, *supra* note 394 (noting that "the Hong Kong Terminal Operators Association . . . includes several private companies that manage the world's second-busiest port after Singapore").

[398] *Id*. *See* U.S. GOV'T ACCT. OFF., GAO-05-557, CONTAINER SECURITY: A FLEXIBLE STAFFING MODEL AND MINIMUM EQUIPMENT REQUIREMENTS WOULD IMPROVE OVERSEAS TARGETING AND INSPECTION EFFORTS (2005) (stating "nonintrusive inspection equipment at CSI ports, to include imaging and radiation detection devices, that help ensure that all equipment used can detect WMD"). *See also* Ortolani & Block, *supra* note 394 (explaining that "[t]rucks that haul the port's containers pass through two of the giant

system is costly, but the system is efficient and the estimated cost of ten dollars per container to run and maintain the screening procedure is nominal.[399]

The scanning system likely would increase the efficiency of CBP officials domestically and at foreign ports by allowing them to review the computer files and identify suspect cargo immediately, "before [the container] gets loaded onto a ship, or at any point along its journey."[400] Balancing costs and benefits of the system clearly weighs in favor of the screening system. Because the scanning process provides a potential method of detecting radiological devices or components, the process would likely deter terrorists.[401] Furthermore, if officials receive intelligence on a particular container or distributor, officials may virtually inspect the contents of that container, as well as containers loaded with goods from the same distributor, without having to remove the container(s) from a ship for landside inspection.[402] As an added benefit, "if an incident can be quickly isolated to a single supply chain[,] then there will be no need for a port-wide shut down."[403]

As discussed throughout this paper, the ramifications of a prospective security breach, and resulting gridlock, may present the largest threat to our maritime transportation system. The screening techniques employed in Hong Kong could reduce these potentially devastating consequences. Moreover, U.S. implementation of a similar scanning program could provide maritime security benefits domestically and abroad.

Admittedly, even wide-spread use of technological advances in the form of imbedded detection devices and scanning equipment will not provide a completely secure maritime transportation system. A comprehensive security regime is neither feasible nor the objective

---

scanners. One checks for nuclear radiation, while the other uses gamma rays to seek out any dense, suspicious object made of steel or lead inside the containers that could shield a bomb from the nuclear detector").

[399] *See Addressing the Shortcomings of the Customs-Trade Partnership Against Terrorism (C-TPAT) and the Container Security Initiative*, *supra* note 198, at 7 (estimating a $6.50 cost for containers scanned in Hong Kong and a $10 cost for containers scanned in the U.S. with similar equipment).

[400] Ortolani & Block, *supra* note 394.

[401] *See Addressing the Shortcomings of the Customs-Trade Partnership Against Terrorism (C-TPAT) and the Container Security Initiative*, *supra* note 198, at 7.

[402] *Id*.

[403] *Id*.

behind protecting U.S. ports with layered security measures for container ships. Comprehensive security is impossible, and a system that tries to achieve it would compromise the essential flow of maritime commerce. The layers of maritime security must be flexible enough to evolve along with changing technology and to provide sufficient deterrents to prospective terrorists. While there are additional feasible methods to help resolve current weaknesses in container ship security, the effectiveness of the existing layered security defense still remains to be seen.