PacNet
Number 45A

Pacific Forum CSIS
Honolulu, Hawaii

October 15, 2004

Ships and Terrorists – Thinking Beyond Port Security
by Tamara Renee Shie

On Sept. 9 and 10, the U.S. Coast Guard issued two more directives aimed at improving security at the nation's 361 commercial ports. The guidelines call for the additional boarding of vessels from or passing through 17 countries failing to meet the International Maritime Organization's International Ship and Port Facility Security (ISPS) Code requirements.

We should applaud the Coast Guard's efforts to protect U.S. ports from terrorists. They have undertaken a daunting task. However we must ask if drawing the line at our borders and in ports is sufficient to protect the U.S. against a maritime-related terrorist attack at home or abroad.

For many years the intricacies of the international maritime trading system inhibited establishment of viable security measures. With multiple actors based in several countries, the maritime trade sector was largely left to itself.

However, the 2000 terrorist strike on the *USS Cole* and the 2002 attack on the French-flagged *Limburg*, the reports of Osama bin Laden's alleged fleet of ships, and rising concerns over the vulnerability of maritime shipping since Sept. 11, 2001, forced governments and security specialists to focus much overdue attention on sea ports and cargo.

Improving maritime security has become the 2004 security focus. This year two major port and shipping security measures received a great deal of attention – the International Maritime Organization's International Ship and Port Security Facility (ISPS) Code and the U.S. Customs and Border Protection Agency's Container Security Initiative (CSI).

On July 1, 2004 the ISPS Code went into effect. Crafted in late 2002, the ISPS is designed to increase security surrounding seaports and maritime shipping from criminal use or terrorist attacks. In order to receive ISPS Code certification, shipping companies, vessels, port facilities, and contracting governments must meet a specified number of minimum-security requirements.

The CSI stations U.S. Customs officers in participant foreign ports to identify and screen containers that pose a risk for terrorist use. By mid-2004 some 18 of the world's largest ports, handling a majority of the world's cargo, had signed on to the CSI.

Unfortunately, relying on these initiatives alone creates a false sense of security. They are inadequate to deter terrorists from pursuing many maritime targets.

The principal limitation of these two initiatives is their specific focus on the security of major transshipment ports. Though these are essential to international trade, securing only these ports will not protect them or a region from terrorist attacks.

First, the emphasis on upgrading the security of major ports neglects the fact that these represent only a single link in the transportation chain. A shipping container may pass through some 15 physical locations and some two dozen individuals and/or companies while traveling from departure point to destination. Because containers are only searched at the major port, there is no guarantee they cannot be waylaid in route *after* that point.

Second, the CSI conducts security checks only on *U.S.-bound* containers. Therefore even if a tampered container arrives at a major port, if it is destined for a port other than the U.S., it is more likely to escape notice. Containers between the major ports of Singapore and Shenzhen or Pusan and Hong Kong are not subject to CSI requirements. Yet terrorist assaults on U.S. ships or interests can occur outside the U.S.

Third, as major ports increase security, terrorists will look for other maritime targets or other means to target those ports.

Terrorists are increasingly aiming at soft targets. Attacking maritime targets has never been particularly easy, often requiring a greater sophistication in planning, training, and coordination than those aimed at many land-based facilities. This is why maritime terrorism is rather rare, and why terrorists are less likely to attack a more secure major port. Yet in considering maritime terrorist threat scenarios – using a ship to smuggle goods or weapons, sinking a vessel in a major shipping thoroughfare, using a ship as a weapon, or even targeting maritime vessels – none require access to a major port or a shipping container to carry out a strike. There remain numerous small ports and small vessels not covered under the new security initiatives. The ISPS Code for instance only covers ships of 500 tons or more and port facilities that serve large international-bound vessels. The Code would not have protected the *USS Cole*.

How else might terrorists strike?

Piracy in Southeast Asia may provide a clue as to how terrorists will respond to these new measures. In 2002, there were 161 actual and attempted pirate attacks in Southeast Asian waters. Of those, 73 percent occurred within ports. The following year, of the 187 attacks, only 37 percent occurred within ports. Between the two years, the total number of attacks increased by 26. In the first quarter of 2004, of the 41 reported attacks, only one-third were committed in ports. Also between 2002 and 2003 pirate attacks in traditionally targeted ports fell while they rose in ports where few if any attacks were previously reported. Though it may be too soon to definitively tell, it would appear that pirates are adapting to the more stringent security measures in larger ports. If pirates can do it, so can terrorists.

Finally, an attack on a major port does not require terrorists to gain direct access to that port. As pirates are capable of attempting more attacks on vessels at sea, it is not unimaginable that terrorists will commandeer a ship at sea and steer it toward a target. The bomb, biological, chemical or radiological agents, or even nuclear materials, can be loaded onto the ship once seized. Then they head for a port or another ship. The May 2004 collision between two cargo ships off Singapore's Sentosa Island illustrates how easily terrorists could conduct a similar but more disastrous operation.

What can be done?

Other security measures proposed or in their early stages aim at expanding protection of shipping beyond the major ports, such as the Proliferation Security Initiative and the Regional Maritime Security Initiative, but they are mired in legal and political battles. Those also have limitations.

More concrete and enduring measures need to be taken to protect ports and ships from criminal and terrorist exploitation.

First, there needs to be tighter security restrictions for vessels of less than 500 tons and for regional ports not covered under the current ISPS and CSI regulations. Rigorous shipping and port security rules should be firmly established, standardized, and enforced through national and international supervisory organizations. A blind eye has been turned toward the international shipping trade for too long.

Second, greater burden sharing, technology assistance, and intelligence cooperation are essential. The costs of installing the necessary equipment, establishing monitoring centers, and in hiring and training employees to implement new security procedures are immense and beyond the capabilities of some countries. This investment is lost if intelligence is not shared among governments.

Third, the creation and expansion of cooperation between domestic and regional maritime law enforcement units is essential. Often national navies are used for maritime surveillance and pursuit, complicating political cooperation and jurisdiction. Many nations do not have well-established coast guards or marine police and those that do exist are relatively new, small, underfunded, and have poorly defined or overlapping duties with domestic navies. Building up the capacity for regional forces to combat maritime security threats on their own will yield longer-term maritime security beyond the ports.

Tamara Renee Shie was a visiting fellow at the Pacific Forum CSIS. She is also a member of the Pacific Forum's Young Leaders Program. She can be reached at tamara.shie@miis.edu