American Shipper
INTERNATIONAL TRADE & LOGISTICS

Trade lane strategy on steroids

By Eric Kulisch
9/29/2010

In an interview, Michael Barrett gave a qualified endorsement to border security expert Stephen Flynn's concept for protecting against the nuke-in-a-box threat.

Barrett is a former naval intelligence officer and director of strategy for the White House Homeland Security Council who specialized in antiterrorism and now is a principal at Diligent Innovations, an Arlington, Va.-based consulting firm that does work for the Homeland Security and Defense departments and private firms. In 2007, he co-authored a book with Rosalyn Wilson and Luke Ritter, *Securing Global Transportation Networks*.

Flynn, now president of the Center for National Policy, advocates a privatized, for-profit, inspection model in which marine terminals take responsibility for scanning every box that enters their facilities, and hire third-party information technology firms to manage the entire data collection and analysis process. Governments would be the recipients of the information and oversee the process rather than operating all the inspection equipment itself and combing through the readouts. The goal is to create a process that is integrated into normal port activity without disrupting container transportation schedules, and can be implemented worldwide for all traffic not just that bound for the United States.

Flynn's model goes too far and Customs and Border Protection's trade lane strategy doesn't go far enough, Barrett said.

"I think the Flynn model is right, but if you try to do 100 percent everywhere, you blow out the cost models. It's almost impossible to do everywhere" without enormous costs, much like trying to rollout broadband connections to the last 20 percent of the United States with a dispersed population is too expensive, he said.

"But, if you said you want 100 percent inspections of the 70 to 80 percent of container trade that comes through the main ports using the main shippers, then you'd have a certain segment of the system that's fairly secure.

"I think ultimately you're going to get a better bang for your buck than if you're relying on risk-based targeting. And the reason for that is that the terrorist is not a habitual shipper. They might just ship one time. So your risk-based models that look at historical patterns are not reliable."

That means CBP has to hope the intelligence community tips it off to a terrorist plan to smuggle a device through the global supply chain to thwart an attack, he elaborated at the Heritage Foundation symposium in Washington.

"Picking specific secure corridors where industry has the most to gain from assured security is more effective than essentially random targeting," he told *American Shipper*.

"There are a lot of the political issues with CSI (Container Security Initiative), such as whether the host country wants to play," he added, alluding to the tiny amount of sea boxes (about 0.1 percent) that undergo non-intrusive inspections overseas.

"You're talking miniscule volumes with the CBP trade lane corridor approach. I'm talking about protecting the major economic patterns," he added.

Barrett also said government ultimately will have to develop a more collaborative information-sharing approach to tap the trade transaction data already generated by shippers as a way of better identifying supply chain threats because industry can't completely self-regulate its security. Smaller companies don't have as much at risk if a container gets destroyed by a terrorist and may not invest as much as larger companies to forestall a loss, while the government is not in a good position to manage trade data and plug the knowledge gaps, he explained in his presentation.

Harkening back to the information clearinghouse espoused by former DHS Deputy Secretary Michael Jackson (without naming him), he said a trusted third-party such as a certified and regulated non-profit or industry association could collect trade data, standardize the data-mining process and make portions of it available to governments under specific criteria, thereby alleviating privacy concerns associated with turning over wholesale data.

The ability to know the status of each container could also prevent port closures in the event of an attack associated with the ocean freight transportation system, because it would allow authorities to quickly investigate whether there are other containers that having been compromised without having to manually inspect all cargo, he argued

Industry is justifiably concerned that security measures can wreak havoc with efficiency, but needs to view an effective security regime in a broader context, Barrett said.

"Efficiency is important over time. It's kind of like having car insurance. The cheapest thing you can do everyday is not have car insurance. But the day that you wreck your car you wish that you had car insurance. So, there's going to be some inefficiency on a day-to-day basis on a micro level, but it creates macro efficiency because when something bad happens the system continues to function."