



Tel 352 692 5493  
Fax 352 692 5494

**Dennis L. Bryant**

Bryant's Maritime Consulting  
4845 SW 91<sup>st</sup> Way  
Gainesville, FL 32608-8135

February 2010

## **The fallacy of technology-based security**

**Dennis L. Bryant**

The recent failed terrorist attack on the airliner traveling from the Netherlands to the United States highlights once again the faulty assumption that we can leave our security to technological devices. The US Government knew that the individual involved had become radicalized. It knew that he had traveled to Yemen, a growing center for al-Qaeda linked extremists. It knew that al-Qaeda had recruited a Nigerian to conduct a suicide attack. It knew that al-Qaeda was planning an attack on Christmas Day. Rather than take all possible steps to keep this individual from entering the United States, our intelligence community and homeland security professionals relied on the technology at foreign airports to scan potential passengers and detect weapons and explosives. They failed to take into consideration that the terrorists are familiar with the technology and with the usual scanning protocols. The terrorists took steps to minimize the likelihood that the explosives would be detected – and they were successful in this regard. The only thing that failed, from the terrorists' perspective, was that the individual was unable to properly mix and detonate the explosive material. If he had been a little better trained, or a little luckier, the airplane would probably have suffered a catastrophic explosion and a large loss of life.

What does this have to do with the maritime industry?

Security in the maritime sector suffers from the same faulty assumptions as those so recently visible in the aviation sector. Much data is collected (possibly too much), but inordinate emphasis is placed on technology-based security. Congress, in particular, keeps pushing for 100% scanning of containers prior to their being loaded on ships bound for US ports. The belief is that such scanning will keep our country safe and that, without 100% scanning, our country is at high risk of attack through use of a weapon of mass destruction (WMD).

The problem with scanning being used as a primary maritime cargo security system revolves around technology. The current generation of cargo scanners does not do a very good job of detecting nuclear devices or radiological material. The next generation of such scanners has been in testing for several years now and has multiple problems. Even if those problems are eventually solved, it will be fiscally expensive, physically difficult, and politically knotty to deploy the new scanners at all foreign ports from which containers are dispatched to America. Even then, the government will only have addressed (albeit poorly) one mode of maritime cargo

**E-mail**  
**Internet**

[dennis.l.bryant@gmail.com](mailto:dennis.l.bryant@gmail.com)  
<http://brymar-consulting.com/>

transport to the United States. The scanning program under development would not address bulk cargoes or break-bulk cargoes. And this assumes that maritime transport is the best method for deploying a WMD in the United States.

The 9-11 Commission recognized this wrong-headed approach and counseled against it. Rather, the Commission recommended the use of better intelligence to identify suspicious shipments and the close examination of such cargoes once identified. In other words, 100% screening should be followed by scanning and physical examination as appropriate.

While such an approach does not have the sex appeal of 100% scanning, it is more effective and cost-efficient. Terrorists have demonstrated the ability to evade technologies soon after a new technology is deployed. It is more difficult for terrorists to evade screening protocols, which are subject to regular updating and are not widely disseminated in the first place.

I am not advocating the abandonment of technology-based security systems. They serve a valuable role. I am saying, though, that technology (for all of its superficial attractiveness) has serious limitations. Unless we recognize and take account of those limitations, we will be playing into the hands of terrorists and others who wish to do us harm, while lulling ourselves into a false sense of security. In the 1930's, the French thought that they could both keep the Germans at bay and reduce the size of their army by building the then-sophisticated Maginot Line. In 1940, the United States thought that it could deter Japanese aggression by forward deploying the Pacific Fleet from San Diego to Pearl Harbor. In both instances, the technological approach failed because it was not preceded by an in-depth analysis of the situation. One should not decide on a solution until there is a full understanding of the problem. One should also not rely primarily on only one approach to address a multifaceted threat.