

Tense present: Protecting ports from security threats

Nazery Khalid*

The 9/11 attacks proved that nothing can stop determined terrorists from carrying out their dirty deeds. Despite the phalanx of security measures introduced in the maritime sector after the incident, there is no guarantee that ports are immune to or can withstand attacks. As the adage goes, build a bigger mousetrap and an even bigger mouse will come along.

What then can be done to secure ports from the kind of attacks that can cripple their operations? More realistically, what further measures can be taken to lower the risk of ports from being subjected to the various threats they face in these uncertain times?

To answer the question, it is essential that port operators and players along the maritime supply chain rally behind the set of measures already in place to protect the chain from the threat of attacks. Notwithstanding the complaints that some quarters may have against the inconvenience caused by tighter security measures and more stringent inspections on ships, crew and cargo, it would be counterproductive to give in to the odd opposition against the initiatives in place.

Talks of dismantling programs such as ISPS Code and Container Security Initiative (CSI) at this point in time on grounds of the diminishing threat of terror on ports and the maritime supply chain should not be allowed to gain currency. To let the foot off the proverbial security pedal would be counterproductive to securing ports from the various threats that terrorists are capable of posing. Terrorists can strike anywhere, anytime and via any conceivable means, as seen on September 11, 2001 and on many other occasions.

As it stands, the maritime industry has learned to accept the fact that it is a changed world – arguably for the worse – and the current security matrix requires a more stiff approach towards assessing, anticipating and countering the potential security threats. Port stakeholders have little choice but to live with the security measures in place, despite their criticism against the effect of more strict inspection on ships and cargo on the smooth running of the supply chain.

It is a sad fact that when it comes to strategic infrastructures like ports, even a single major attack would be one attack too many. With ports, the economic price to be paid as a result of lackadaisical attitude toward security could be astronomical and even potentially catastrophic.

As unpopular as some of the post 9/11 measures are – including new ones such as the Secure Freight Initiative (SFI) which requires all US-bound containers to be inspected at their ports of origin – the industry players have little choice but to support the efforts to inspect, monitor or even detect suspect containers and vessels. In these trying times, the concepts of ‘better be safe than sorry’ and ‘prevention is better than cure’ must not be seen as mere clichés and must be adapted into the organizational culture of players in the maritime industry.

Core to the protection of ports and their personnel and assets against threats is intelligence – not the dumb type but solid, reliable intelligence that can be useful in assessing security risk and putting in place appropriate measures to counter real threats. To attain such a level, there must be full cooperation amongst the parties involved – from intelligence agencies to port operators, from security enforcement bodies to port users.

'Smart intelligence' must be collected, analyzed, interpreted, recorded, shared, used and acted upon effectively by maritime security stakeholders. A common, interoperable platform must be put in place to enable the many players involved in port security to cooperate on collecting, analyzing, sharing and disseminating material data and information on which security response can be made. Port operators and other players in the supply chain alike must be convinced that it is in their collective interest to work together within a mutually acceptable organizational framework that can facilitate the sharing and rapid exchange of security-related data and intelligence amongst them.

Adequate resources must also be readied to enable the stakeholders to procure the necessary equipment and systems and also to put in place and train the manpower to secure ports. Help in the form of government grants like the one provided by the US Government via the Department of Homeland Security to boost security at US ports is essential to help assuage the burden of providing extra security on the shoulders of port owners and operators alone. Assistance in cash and in kind should also be extended to ports in developing countries that do not have access to the kind of resources available to ports in developed nations in order to boost their security. Such help would relieve port operators of the need to impose security surcharges on their users to recover security costs and would help facilitate the smooth flow of global trade.

Key to setting up such a platform of cooperation and to undertake the challenging task of monitoring ships, cargo, vehicles and personnel going in and out of ports is the use of technology. Cost-effective and proven technologies already used in activities such as notification of arrival of ships, pre-clearance of cargo before arriving at ports, inspection of cargo, submission and verification of manifest and other documentation, and checking of personnel going in and out of ports must be optimally utilized and enhanced to secure ports from the manifold threats they face.

In the final analysis, it would not be feasible nor possible to inspect all containers and all times. This is where the role of technology and intelligence comes into play to help security agencies to separate the wheat from the chaff and identify and inspect only high risk containers. Technologies such as gamma ray, biometrics, global positioning system (GPS), radio frequency identification (RFID) and long-range identification and tracking (LRIT) systems must be continuously harnessed to develop effective security response based on risk assessment. This stands a better chance to work effectively and to gain widespread acceptance by port users as opposed to a 'needle in the haystack search' approach deployed in security measures such as the SFI.

* Nazery Khalid is a Senior Fellow with the Maritime Institute of Malaysia. The views expressed are those of the author and do not reflect the official policy or position of the Maritime Institute of Malaysia. The Author may be reached at nazery@mima.gov.my / www.mima.gov.my

NATIONAL MARITIME FOUNDATION

Advancing India's Maritime Interests....