

## Using technology to combat terrorism

### **The US, as the driving force behind the maritime security measures under discussion at IMO, has been concentrating on its own ports and looking at solutions that will enable security and the efficient flow of goods to work together**

The recent attack on a CMB tanker near Yemen may have signaled the start of another "tanker war", albeit in a world-wide theatre in a new kind of war (unlike the localised scope of the mid-1980s incidents). Security concerns are now looming large, especially concerning tanker operations in the ports of industrialised cargo receiving nations. Industry associations and owners are calling for escort patrols (another feature of the 1980s) in terror prone areas.

Meanwhile, Port States are on alert, vessel crews are increasing their own vigilance, and pending IMO rules will soon institutionalise security-minded operating practices. Ships calling on ports and terminals in the US have been required to submit 96-hour advance arrival notices to the Coast Guard over the past year, along with a declaration of cargo and crew onboard. After recent revisions of the form, the Coast Guard now requires that the vessel charterer be listed. Starting later this year, US Customs will be requiring submission of cargo manifests 24 hours in advance of a US-bound vessel sailing its loadport. Local Coast Guard Port Captains with local authority have established, at their discretion, security zones around tanker anchorages, and around vessels transiting local waters. In some ports, the local Coast Guard have restricted tanker transits to daylight hours, or required Coast Guard personnel to board ships at anchorages and ride the vessels inbound.

But developments in the US are merely harbinger of significant worldwide changes set to impact ships, ports and the interface between the two. Shipping practice will be profoundly affected by decisions taken at the December 2002 meetings of the IMO, representing the culmination of studies and committee recommendations over the past year. It is expected that a Ship and Port Facility Security Code ("the ISPS Code") will be added to Chapter XI of the SOLAS Convention. Procedures at tanker terminals throughout the world would be put under the microscope as port vulnerability assessments are conducted, with solutions and security plans to be developed on a case-by-case basis. It is also expected that ship security plans (eventually to be part of the ISM Code) will be required, along with ship and company security officers. Resulting changes in procedures aboard ships are also under consideration- for example, the Philippines asked the IMO to consider whether the paper intensive security officer role might be combined with that of an electronic maintenance officer, noting the pivotal roles for communications technology in alerting and security generally.

IMO's actions will be broad reaching, mandating tighter access controls to terminals, and creating security standards for access to sensitive areas aboard vessels.

Seafarer identification will also be under discussion, with recommendations promulgated for standardised seafarer credentialing- which could include biometric identification. The question of background checks of mariners, a highly contentious issue, is linked to this dialogue. Also under discussion is the highly elusive area of "transparency of ownership". As the IMO has grappled with definitions of "who is the owner", in addition to "who is onboard", one politically motivated security recommendation is that shipping move back in the direction of national flags, where tighter control could be exerted. Concern about this type of backlash has already caused a number of ship registries to work proactively towards greater transparency. On the communications front, advanced technology will play an integral role in protecting vessels and port states. It is likely that IMO will require that vessels must carry ship alerting hardware, in the form of a panic button that can be accessed from

the bridge which would activate an alarm to be sent to the search and rescue network. IMO had also been looking at instituting mandatory long range tracking, but this requirement may be tabled pending further study. It is likely that the schedule for installing Automatic Identification Systems (AIS), where AIS equipment can be phased in through 2008, will be accelerated.

Other questions abound. Who will pay for security? In the US, proposals floated for a "Security Tax" (budgeted to raise \$3.5 billion) to be levied on shipowners and cargo interests has met with resounding opposition. Schemes for information sharing or feeds to government-operated security databases, get a wary endorsement, subject to the solutions maintaining the confidentiality of commercial information.

Many practical aspects of tanker security still need to be integrated with operational practice and common sense. For example, shouldn't ships making regular port calls (say in a lightering or shuttle trade) be included in a "trusted vessel program" and therefore be able see a fast track into the port amid an increasing maze of inspections? Or, how can Customs requirements for advanced cargo manifests be reconciled with the practice of on-the-water cargo trading? In the US, commercial logicians, academics and government are acknowledging that they need to better understand the flow of bulk cargoes, and how security can be insinuated into decades-old business processes that evolved based on speeding up and optimising the movement of materials.

Indeed, a number of US projects, already funded, will be deconstructing tanker cargo supply chains, i.e. the flow and handoffs of tanker cargo. The "Model Port" project, a subset of Operation Safe Commerce (co-chaired by the Department of Transportation and the Customs Service), focusing on the Port of Boston, will include participation from Irving Oil and Tractebel LNG/Distrigas. Further down the Coast, two groups funded by Port Security grants, Maritrac (with participation from PoleStar) and R.I.S.K. Alert will look at a number of supply chains, including bulk oil and petroleum products moving into the New York Harbour and Delaware Bay/ Delaware River ports respectively. The New York project is likely to have at least one large Jones Act tanker fleet onboard, while the Philadelphia project is expected to see the participation of a major oil company with refining capacity in the region. The tanker industry's stated desire for transparency should help all concerned in their efforts to analyse cargo flows, and build in security, where necessary. A pleasant by-product may be that enhanced information flows actually improve the efficiency of supply chains.