



The considerable debate on port security has led to conflicting information in the past. Now though, more structure is falling into place to provide ports with clearer direction. **Steve Cameron** reports.



SCANNING THE HORIZON

In July this year the International Labour Organisation (ILO) produced a draft "Code of Practice on Security in Ports". This was endorsed by a Joint ILO/IMO Working Group and will be presented for adoption by the ILO at a tripartite meeting (governments, employers, workers) this December.

The (currently draft) Code of Practice (COP) establishes the responsibilities of governments to produce a port security policy and ensure a legal framework to:

- promote regional and international co-operation
- encourage stakeholder participation in security policy development
- provide adequate resources to implement and sustain the policy
- identify a designated authority responsible for security in each port
- ensure the establishment of a port security committee involving appropriate employers' and workers' representatives, national and local government agencies, and nominate a port security officer
- ensure a port security assessment is carried out and develop and implement a port security plan.

The objective of the COP on security in ports is to enable governments, employers, workers and other stakeholders to reduce the risk to ports from the threat posed by unlawful acts and provide a guidance framework to develop and implement a port security strategy appropriate to identified threats to security.

The application of security guidelines is to all areas and functions of the port, and those working in, having business with and requiring access to the port or transiting through the port. This includes port workers and other port personnel, seafarers, passengers and passengers' baggage, cargo, material, vehicles and equipment originating from within and outside the port area. Also maximizing the effectiveness of security measures through systematic exercising, testing and audit of security procedures to identify and correct non-compliance, failures and weaknesses.

Some examples of the aim of security measures that may be considered are to:

- Prevent access to the port by persons without a legitimate reason to be there and prevent those persons with legitimate reasons to

be in the port from gaining illegal access to ships or other restricted port areas for the purpose of committing unlawful acts.

- Prevent introduction of unauthorized weapons, dangerous or hazardous substances and devices, into the port or vessels using the port.
- Prevent personnel injury or death, or damage to the port, port facility, ship or port infrastructure by explosive or other devices.
- Prevent tampering with cargo, essential equipment, containers, utilities, protection systems, procedures and communications systems affecting the port.
- Prevent smuggling of contraband, drugs, narcotics, other illegal substances, prohibited material and other criminal activity.

The appropriate security level is determined by member States and the security measures to be adopted appropriate to the security level, should be outlined in the port security plan.

For example:

- Security level 1 may include random personnel, baggage and vehicle screening, and implementation of access and movement control.
- Security level 2 may include increased frequency of screening, more

robust monitoring of the port, and more stringent access and movement control measures.

- Security level 3 may include 100% screening with positive identification check, temporary cessation of certain port activities and/or imposing vessel traffic control measures, restricting access to certain areas, deployment of security personnel to key infrastructure etc.

CONTAINER SCREENING OR SCANNING

With respect to the screening of containers this is taken to be assessment of the risk posed by a particular container or truck. This can be a paper-based assessment process checking that the relevant information is in place and looking for predetermined indicators that suggest particular levels of risk. The process of screening does not necessarily mean container scanning, in fact as things stand at present there is no legislation requiring containers to be scanned but US Customs do expect any port that has cargo bound to or from the USA to have the ability to scan containers. This has stimulated a huge investment by ports in container scanning equipment and in the training necessary for operators to become proficient at using the

range of tools available to identify images that may suggest something is not quite right.

LIGHT AT THE END OF THE TUNNEL

As the world's major container ports wrestle with the new technology there is one location that has been quietly getting on with the process. Although they have now gained significant experience since their operation commenced, they were still surprised to be identified as one of the world leaders in their field. It is not one of the large container terminals as perhaps you might imagine, but the security managers for the Channel Tunnel, Port Maritime Security International (PMSI), who, recognising their accumulated skills, have been spun off as a separate organisation from Eurotunnel plc.

The huge volumes of vehicles and containers that transit through the tunnel every day during the last ten years has given PMSI a considerable amount of accumulated expertise. Today, the demand generated by the traffic volumes is such that there is a freight train through the tunnel every 10 minutes in each direction.

PMSI has worked in partnership with its scanner suppliers Smiths Heinemann. This partnership over the last decade has enabled significant enhancements to be made to the technology and training of the operators.

Certainly the statistics are almost as impressive as the quality of the images they produce. During the last 18 months PMSI has actually scanned half a million units and work on the basis of scanning two 40ft vehicles or containers every 10 minutes.

The images that are produced are extremely clear, the sides of 40 ft trailers become transparent and the 20mm thickness of steel-sided containers present no barrier either. Such is the clarity that parts of the vehicle's chassis, axles and drive train look more like a precise engineering drawing than x-ray.

The scanning equipment is mounted on a gantry inside a suitably lined concrete transit shed. Once the gantry has transited the length of the two units, the system "slices" through the load from one side to the other, section by section.

The more common items that are identified as security threats are knives and handguns in the driver's cab with the latter often concealed in the lining fabric of the vehicle. Even small items such as knuckledusters are clearly detectable. Drugs hidden in the tops of containers of liquid and in the middle of a load of tarmac present no problem to the scanner operators either.

The outline of the human form was another example: the driver's mate left concealed or asleep in the cab or bodies being illegally returned to their final resting place in Europe.

With this level of clarity and expertise it is not surprising that the skills of PMSI are of interest to developed regions where terrorism is a key issue and the less developed regions where smuggled arms are often the precursor to an uprising and a threat to the stability of the country.

In many parts of the world pre- and post-shipment inspections have become a way of life as governments do their best to control banned imports and protect their revenue streams.

Companies such as SGS, Cotena Bureau Veritas and Intertek Testing Services compete vigorously for this business which remains particularly strong in the developing world.

Container scanning is not yet necessarily an alternative to pre- and post-shipment inspection as discovered recently in Ghana where Customs revenues dropped dramatically when container scanning was introduced as an alternative to such inspections and the original processes had to be reinstated!