

Making port security work



Henk van Unnik, *Security expert and former chairman of the Security Development Board at Rotterdam Port, Utrecht, the Netherlands*

Once upon a time commercial ports only had to deal with three key threats on a daily basis - theft, damage to goods and stowaways. The contemporary port is subject to a far wider range of threats including the possibility of terrorist attack, and has to respond accordingly while also managing and responding to a plethora of local, national and international legislative requirements.

This paper outlines the current scenario and explains how a solution to the problem has been developed through the Security Upgrade for PORTs (SUPPORT) research and development project which is part-funded by the European Commission's FP7 Security Research Programme.

With 90 percent of the EU's external trade and 40 percent of internal trade transported by ship, the contemporary sea port is a vital cog in the massive machine that is 21st century commerce. Unsurprisingly, port infrastructure and the 3.5 billion tonnes of freight that flows through EU facilities are vital to maintaining both global and individual countries' economic wellbeing.

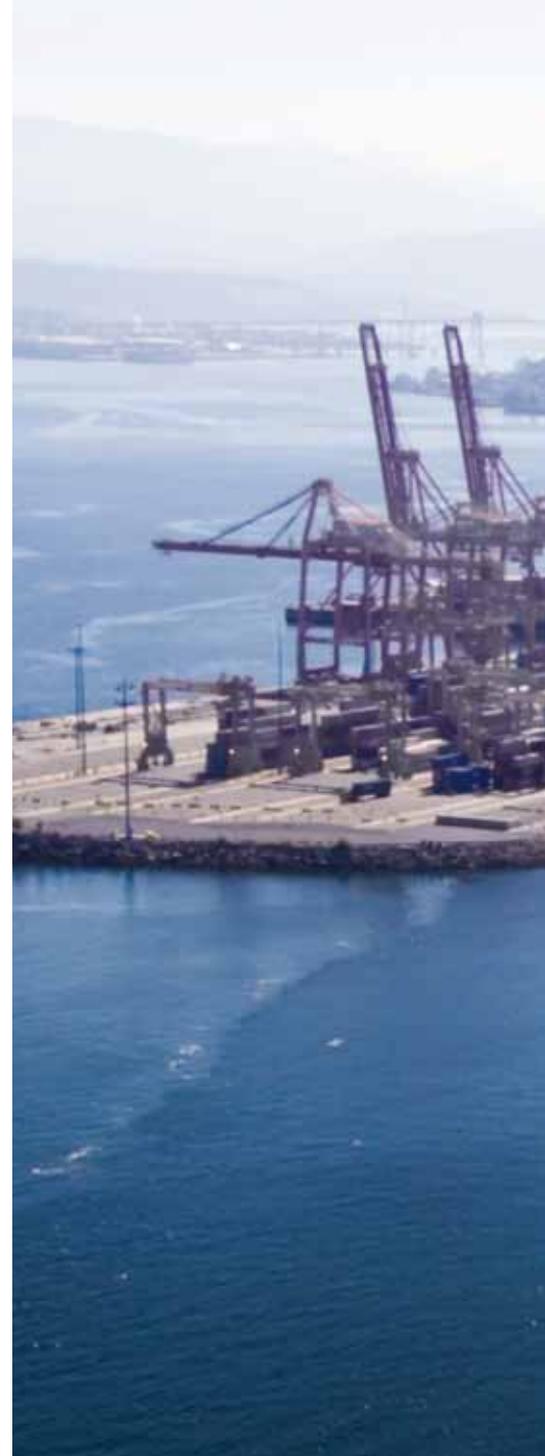
The potential threats to port security come on many different levels from a range of groups and individuals with very different aims and objectives. Theft, fraud, corruption, drugs trafficking and people trafficking are all major issues for port security, especially when their motivation can be traced back to organised crime or terrorist groups. The combination of sophisticated organised crime, the heightened risk of terrorist activity and the ongoing threat of low level crime ensures that ports are under threat 24 hours per day, 365 days per year. Well organised criminal gangs now have access to enough money, knowledge and skills to develop considerably more complex ways of operating. Faced with such innovative and complex criminal activity, port security needs to raise its game.

Current security legislation

Current port security legislation was developed by the International Maritime Organization (IMO) in the aftermath of the September 11th terrorist attacks, with the International Ship and Port facility Security code (ISPS) now regulating security on-board ships, as well as inside ports and terminals which receive seagoing vessels on international voyages. The ISPS code specifies a basic security framework including monitoring and controlling access, monitoring the activities of people and cargo, the preparation of specific ship and Port Facility Security Plans and the appointment of Ship Security Officers and a Port Facility Security Officer (PFSO).

Across the EU, the ISPS code is supported by European Commission Directive 725. While identical to the ISPS code in content and a mandatory piece of pan-European legislation, Directive 725 only requires member states to achieve a particular result without dictating the means of achieving that outcome. Consequently, the ISPS code was implemented by 21 EU countries, each in a different way without any homogenisation of approach or standardisation. Without a pan-European federal agency like the US Department of Homeland Security, the EU has no power to compel member states to work together or to follow prescriptive guidelines, and individual ports work in isolation with commercially-driven secrecy, thwarting the sharing of intelligence or best practice.

Although responsibility rests with a variety of ministries or other government agencies across Europe, the burden of compliance and implementation of the ISPS code has been passed down to the individual terminal operators. This introduces a paradox as commercial companies whose aim is to make a profit are being made responsible for an activity that does not necessarily deliver any business benefit. Enhanced security



beyond that required to protect day to day business operations are often not high on terminal operators' agendas, especially when national authorities do not have the power to force them to invest in such security measures. Consequently the level of security that can be physically implemented will always be a balance between risk and commercial reality. In this context the role of the Port Facility Security Officer (PFSO) is key to ensuring this fine balance is maintained.

EU security upgrade project

Providing a framework to assist the PFSO is a major element of the EU's security upgrade for ports (SUPPORT) project (see www.supportproject.info) which is part-funded by the EC's FP7 Research & Technological Development



Programme. It is a collaboration of 20 European organisations whose focus is to raise the current level of port security. The SUPPORT project's main objectives are to deliver validated generic port security management models (capturing reusable state-of-the-art and best practices) that can be customised for specific ports; and training and open standards-based tools to aid security upgrade in EU ports.

SUPPORT integrates legacy port systems with new surveillance and information management systems. It efficiently supports the complexity of a real port environment through an integrated, holistic approach. This ensures an improved level of security, while reducing the associated administrative burden on the port. Amongst the partners

are a number of ports that represent typical, but different operations. Starting from the perspective of the partner port operations, the project has identified key security gaps and has produced generic models describing measures to maintain or augment the efficient and secure operation of these ports. Communication and decision support tools incorporating semantic technologies have been developed, accessible to all the port security stakeholders.

Providing security solutions

Full scale demonstrators have been organised in representative EU ports (Gothenburg, Lisbon and Piraeus) and augmented with a broader evaluation programme by members of a European ports security forum. SUPPORT solutions

include policy and standardisation proposals and training that can be used by any EU port to efficiently enhance its security level.

One of SUPPORT's key outputs is the Port Security Management System (PSMS). The PSMS is designed to help PFSOs to upgrade their security systems by empowering them with knowledge. It provides information, skills and methodologies that enable them to maintain, evaluate and upgrade their security measures and create security awareness without major investment. The PSMS also delivers outputs in the form of graphics that can be used to reinforce security threats and potential mitigation measures in presentations to managers or boards of directors.

The whole PSMS package comprises



five elements including a maturity module designed to enable security professionals to review and upgrade security plans to address terrorist threats; a corporate security module which addresses crime risks such as loss events, related to corporate processes and procedures; an e-learning education and examination module based on best practices of ISPS related maritime security education including drills and exercises; a sharing and decision support module which enables security professionals to supervise facilities via the internet and to collaborate on a local, national or global scale and an Authorised Economic Operator (AEO) security self-assessment module which provides a system to reach compliancy and submit AEO application.

The pressure of balancing commercial realities and security threats will certainly persist as long as current legislation remains, placing the burden of investment and compliance on terminal operators. However, with access to SUPPORT's Port Security Management System (PSMS), PFSOs now have the tools to assess the situation, advise their management team and make the right decision, whatever the security threat might be.

About the author

Henk van Unnik, managing director of Tosepo, a maritime & logistics security business, and a member of the Executive Committee of SUPPORT (SecurityUPgrade for PORTs) which is part-funded by the EC's FP7 Security Research Programme. SUPPORT is a collaboration of twenty organisations, co-ordinated by the BMT Group, which has been established to help upgrade and enhance security in European Seaports.

Henk is a maritime and logistics security expert whose knowledge and experience has been drawn from an impressive career in senior positions supporting security and maritime organisations all around the world. He started work as a criminal investigator for the Dutch Municipal Police, moving to ever more senior positions in the Rotterdam Seaport Police before being appointed as chairman of the Port Security Development Board Rotterdam and President of the International Association of Airport and Seaport Police (IAASP). He now works as an independent consultant. Henk is one of the architects of the Rotterdam "Reliable Port Concept" and writer of the guide "Security Mainport Rotterdam".

Henk's work has taken him across the globe, auditing and assessing ports and port facilities in Central Asia, South East Asia and North and South America, Africa, Western Europe, the Balkan, Baltic and Mediterranean regions. He has been responsible for developing new regulatory frameworks, new investigation methods and profile analyses to enhance port security and help combat international organised crime, drugs trafficking and terrorism.

Henk is also a certified ISO 28000 (Security management systems for the supply chain) auditor.

Enquiries

Henk van Unnik
Tel: +31 (0) 6 53 12 03 14
Email: h.vanunnik@tosepo.com