Tightening the loop

Recommended methods of perimeter security for seaports

Magal S³, Yehud, Israel

Need for port security

The terror attacks of September 11 raised global awareness about terrorism and its impact on the world economy. The potential to ship weapons, chemical material and 'dirty bombs' into unsuspecting harbors has become a major threat to the global community. Governments around they have realized that the terror organizations – in their attempt to disrupt globalization and modernization – regard trade, open seas and ports as high-value targets. However, due to the complexity of today's trade processes and practices, countries have to come to realize that securing the entry point alone is insufficient; the entire supply chain must be secured – beginning with seaports – as they often represent the weakest point in the chain. In addition, ports face an added level of threat with the continued rise of criminal activity. In light of these risks, combined with the inherent difficulties in securing such facilities, the challenge of port security has become evident.

Inherent vulnerabilities

Mainly due to its topography, ports represent a major challenge in border security. An additional complexity is the large number of interconnected facilities and their operations including bridges, dams, dock infrastructure, hazardous material depots, pipelines, and many other critical assets that may be an enemy target. Furthermore, there is a high volume of foreign vessel, truck and rail traffic to and from these sensitive seaside areas, with significant numbers of passengers passing through on a daily basis.

Terrorism

A decade after 9/11 and amid political instability in many regions, worldwide security measures are being stretched to the limit, with terrorists becoming far more sophisticated in their attempts to penetrate foreign borders. From bombs in sneakers to explosives sewn to animals, terrorists continue to take advantage of any security gap that will allow them to infiltrate and wreak havoc on the global community.

The security vulnerabilities of seaports and maritime operations have not escaped the attention of terrorist groups. The Al-Qaida chief operator – Abd al Rahim al Nashiri – developed a strategy to attack western shipping targets when he was captured in 2002. Furthermore, the possibility of smuggling a 'dirty bomb' via a seaport in order to contaminate a Western city with radioactive material is a real fear. In fact, over the years there have been a number of attempted and successful terror attacks against seaports and maritime operations, as shown in Table 1.

Criminal activity

Organized crime is well-established in many ports. Criminal activity, from smuggling to petty theft, continues undeterred due to the absence of collective supervision and governance. An additional obstacle is the pressure to accelerate the handling of cargo and reduce costs, leading to the omission of various precautions and inevitably compromising port security. These challenges illustrate the critical importance of implementing the appropriate local safety measures in the context of securing global maritime transport.

ISPS code

To address the issue of seaport safety on a global scale, the International Maritime Organiz ation (IMO) – at the behest of the United States – instituted the International Ship and Port Security (ISPS) Code in December 2002. The code is a comprehensive set of measures and requirements aimed at enhancing the security of ships and port facilities around the globe. The ISPS code offers a series of guidelines to governments, port authorities and shipping companies in order to meet these requirements.

The code was quickly adopted by the international convention for the Safety of Life at Sea (SOLAS) as countries and governments realized that secure ports directly benefit their economies.

Need for smart, integrated security

Comprehensive security is comprised of three key elements: technology, human resources and processes. These three components must be tightly integrated through the Concept of Operation (ConOps), allowing for effective and efficient port operation without compromising security.

The core technology of perimeter protection for seaports includes smart fences, access control for all gates and an integrated command and control system. Verification and surveillance cameras are also an important element of the full solution. Ideally, the perimeter should have more than one layer of protection, with additional layers deployed in particularly sensitive areas.

As explained below, the combination of basic fences with simple or smart cameras does not yield an adequate level of security. Moreover, ineffective perimeter protection can create many false alarms, which, in addition to being both time consuming and costly to verify, causes personnel to lose vigilance.

Basic fences only

While physical barriers may deter and delay intruders, they are essentially simple fences without detection capabilities. Due to the

TABLE 1: RECENT MARITIME TERROR ATTACKS

Date	Location	Nature of Attack	Terrorist Group
July 2009	Egypt	Attempted attack against the Suez canal and the adjacent oil pipeline	Egyptian cell of Al-Qaida
March 2005	Indonesia	Discovery of training terrorist operatives in sea-borne guerrilla tactics, including gaining unauthorized access to ships and port facilities in order to plant explosives	Islamic extremist group, Jemaah Islamiya
February 2004	Philippines	Attack on a passenger ferry that killed over 100 people	Abu Sayyaf group
October 2002	Yemen	Attack on French oil tanker Limburg off the harbor of Ash Shahir	Yemenite cell of Al-Qaida
October 2000	Yemen	Attack on the US destroyer USS Cole	Al-Qaida

large area and long perimeters of ports, intruders can easily cut or climb the fence and enter the site without being noticed.

Basic fences and simple cameras

A combined solution of basic fences covered by simple cameras is also inadequate, as it is not feasible to manually monitor the large number of cameras necessary in such a solution. In fact, studies have shown that security personnel tasked with monitoring only nine cameras lose alertness in less than ten minutes.

Basic fences and smart cameras

Although smart cameras can automatically analyze irregular events, a combination of a simple fence with smart cameras will not provide adequate security due to a number of inherent imitations:

- In order to provide complete perimeter intrusion detection, a camera would be required every 60-90 meters, increasing costs significantly.
- Smart cameras with high quality outdoor video motion detection (VMD) – which are capable of performing under extreme changes in lighting and weather conditions – make the solution even more expensive.
- CCTV cameras are limited in poor visibility conditions and thermal cameras, while more robust, are nevertheless inadequate in heavy fog conditions.
- Sophisticated long-range surveillance cameras (IR, CCD, fixed or scanning) may have coverage gaps and suffer from the inherent visibility limitations mentioned above; therefore they are unable to support the required 99% probability of intruder detection.

Perimeter intrusion detection systems (PIDS)

Magal S^3's intrusion detection systems are durable, robust and designed to perform under any seaside condition including salt fog, corrosive materials, water, wind, extreme temperatures, electro-magnetic interference, and vibrations induced by ground traffic.

Several categories of outdoor site protection technologies are available to address a broad range of strategic threats and can be tailored to fit any budget.

- **Taut wire** – A hybrid system of sensors woven into a barbed wire fence. This fence offers guaranteed performance in all-weather conditions. It has demonstrated a high probability of detection (POD) and an almost zero false alarm rate (FAR). It is therefore ideal for high security where deterrence and delay must be achieved on top of uncompromised intrusion detection.
- **MagBar** – A robust grid designed to plug critical holes in perimeter security systems by custom-fitting a specific opening, such as canals, pipes, open tunnels or drains. The grid is fortified with either electro-mechanical or electro-optical sensors threaded within the steel. Any attempt to tamper with the structure will trigger an alarm.
- **Fence-mounted sensors** – These sensors are ideal add-ons to existing fences as an affordable solution. A second security measure, such as CCTV, can be integrated as a further verification layer.

Outdoor perimeter fence-mounted sensors installed at Eilat Port, Israel.

- **Buried cable sensors** – A virtual fence implemented by a smart cable, buried less than one foot underground. The cable creates an invisible electromagnetic field, capable of detecting any intruder entering the narrow virtual corridor. The buried cable sensor is an ideal solution for places where a fence cannot be installed for aesthetic or environmental reasons, such as concrete platforms where movement must be restricted during non-active parts of the day. Although 'ranging' (the ability to detect an intruder's exact presence) is not essential with actual fences because the structure itself can delay a trespasser long enough for apprehension; in the case of virtual fences that do not cause a delay, 'ranging' is critical to effectively intercept intrusions.
- **Decorative fence** – Innocent-looking ornamental fences equipped with internal sensors that will detect climbing, bending or cutting. This fence is ideal for protecting the façade of ports – particularly in passenger or administrative areas.
- **Radar** – Ground protection radars are ideal for a port's open and clear areas, where early warning can significantly reduce the first responders' reaction time.
- **Microwave (μW)** – Another type of virtual fence that creates an invisible electromagnetic beam. This is ideal for virtual gates, where the 'gate' must be open for traffic during the daytime but must be shut down at off-times, such as nights or weekends. It is also well suited for temporary construction when the 'gate' must be easily installed and removed.

ABOUT THE COMPANY

Magal S^3 is a leading international solution provider in security, safety and site management. The company serves a wide range of vertical markets which includes but is not limited to: airports, seaports, railway stations, borders, correctional institutions, municipalities, nuclear and utility facilities. Magal S^3 has developed a unique set of solutions and products optimized for perimeter, outdoor and general security applications. The turnkey solutions are typically integrated and managed by a single, sophisticated modular command and control system.

ENQUIRIES

Magal S^3
17 Altalef Street, PO Box 70
Yehud, 56100, Israel
Tel: +972-3-5391444
Fax: +972-3-5366245
Emails: info@magal-s3.com
sales@magal-s3.com