

MARITIME AND PORT SECURITY

WHITE PAPER

BY

CHARLES GOSLIN

“Charles Goslin, Vice President of International Operations for Duos Technologies, Inc., is an international expert in security threat and risk assessment. He developed his extensive security experience as a veteran operations officer for 27 years with the Central Intelligence Agency. He is skilled in developing and executing programs targeting terrorism, espionage, weapons proliferation, and other select U.S. national security objective. He brings a unique, ground-level perspective to security challenges that can only come from a lifetime spent mitigating risk, in all its forms, while living and working abroad.

His most recent assignment, before joining Duos, was as a senior advisor to the Regional Joint Terrorism Task Forces (JTTF) in the U.S. In addition to Mr. Goslin’s current work with international clients, he has authored professional articles and undertaken public speaking engagements regarding the evolution of physical security in the 21st century, and how it can better secure critical infrastructure for public and private enterprise.”

THIS PAGE INTENTIONALLY LEFT BLANK

INTRODUCTION

Worldwide Port and Maritime operations and their associated facilities and infrastructure collectively represent one of the single greatest unaddressed challenges to the security of nations and the global economy today. The reason that ports and shipping activity are so difficult to secure lies primarily in their topography. Ports are typically large, asymmetrical activities dispersed over hundreds of acres of land and water so that they can simultaneously accommodate ship, truck and rail traffic, petroleum product/liquid offload, storage or piping, and container storage. The movement of freight, cargo (solid or liquid), and transport through a port is generally on a “queuing” system, meaning that any delay snarls all operations¹. Whether or not delays are related to security, security generally falls by the wayside in the interest of time management or convenience.

Globally, there are very few uniform standards for point-to-point control of security on containers, cargoes, vessels or crews - a port’s security in one nation remains very much at the mercy of a port’s security, or lack thereof, in another nation. Organized crime is entrenched in many ports², and a large majority of them still do not require background checks on dock workers, crane operators or warehouse employees. Most ports lease large portions of their facility to private terminal operating companies, who are responsible for their own security. The result of this is a “balkanized”, uneven system of port security and operations management as a whole.

In spite of awareness by public policymakers that ports remain critically vulnerable³, funding and government-led efforts to harden port facilities worldwide is moving at a glacial pace. Terrorists, in particular, are aware of this unaddressed vulnerability. As outlined below, the threats to the maritime industry are very real. Unfortunately, the question of whether terrorists will act to exploit the weaknesses in port facilities is, unfortunately, not a matter of “if” they will, but “when” they will.



Troops alone cannot protect a seaport

THE THREAT: Terrorism

Global trade is dependent mainly on maritime transport. It is estimated that more than 46,000 vessels and 4,000 ports make up the world’s maritime transportation system. The United Nations Conference on Trade and Development (UNCTAD)

¹ Extracted from GAO report dated 17 May 2005 entitled “Maritime Security: Enhancements Made, But Implementation and Sustainability Remain Key Challenges”

² President’s Commission on Crime and Seaport Security, recently estimated \$30-\$50 billion loss worldwide, per year, through cargo theft activity alone. CanWest News Service, on 23 March 2007, reported that Canada’s ports were “riddled” with organized crime.

³ “Our Vulnerable Seaport Security”, by Senator Dianne Feinstein, 7 April 2003, op-ed column in the San Francisco Chronicle.

estimated in 2001 that 5.8 billion tons of goods were traded by sea in 2001; more than 80 percent of the world's trade⁴. This fact alone makes maritime networks an attractive target of terrorists. Although it has been some time since Usama bin Laden has been seen, it is ominous that in one of his last video appearances in October 2004 he confirmed that his agenda remained primarily economic⁵. While terrorists have in the past targeted land or aviation assets, experts believe that this could soon change to include shipping, port, coastal facilities, and container/container yards are increasingly vulnerable because secondary emphasis has been placed on hardening these assets due to the urgent need to address threats to aviation facilities and transportation⁶. The following trends in terrorist threat reporting underscore increased concern for the maritime industry:

- When captured in November 2002, Abd al-Rahim al-Nashiri, Al Qaida's operations chief in the Persian Gulf had developed a four-pronged strategy to attack Western shipping targets:
 - Ramming vulnerable vessels at sea
 - Blowing up medium-sized vessels at ports
 - Attacking vulnerable, large cargo ships such as super tankers from the air by using explosive-laden small aircraft
 - Underwater attacks by divers or suicide demolition teams, using limpet mines

Al-Nashiri was an explosives expert, specializing in naval demolition sabotage⁷.

- Al Qaida operative Saud Hamid al-Utaibi who replaced al-Nashiri, took an active role in the operation that targeted the bombing of the USS Cole in 2000, and the French tanker Limburg in 2002. Following al-Utaibi's appointment, the threat to maritime targets involving chemical agents was elevated⁸.
- Operatives belonging to the Islamic Extremist group Jemaah Islamiah (JI), which is affiliated with Al Qaida, have been trained in sea-borne guerrilla tactics. A key element to their strategy is to gain unauthorized access to ships and port facilities in order to place explosives⁹.



Vulnerability from the air and the sea

⁴ www.unctad.org/en/docs/rmt2003_en.pdf

⁵ On October 29, 2004, Osama Bin Laden appeared on the Al Jazeera network, and spoke of his desire to "bankrupt" the U.S. *"(we)...have experience in using guerilla warfare and the war of attrition to fight tyrannical superpowers, as we, alongside the mujahidin, bled Russia for 10 years, until it went bankrupt and was forced to withdraw in defeat."*

⁶ "Port Problems Said to Dwarf New Fears," Paul Blustein and Walter Pincus, Washington Post, 24 February 2006, para 16.

⁷ The Threat of Maritime Terrorism: Defense Update, by David Eshel, 10 December 2005

⁸ The Maritime Threat, by Ophir Falk and Yaron Schwartz, 25 April 2005

⁹ David Eshel, *ibid.*

- At least one Al Qaida operative is known to have been in the process of obtaining an international seaman's license that would allow him into any port in the world without a visa¹⁰.
- In 2003, 35 heavily armed terrorists boarded a chemical tanker off the coast of Sumatra. However, unlike pirates who operate in the region and routinely rob the crew and loot the vessel, these boarders simply demanded that the ship's captain teach them how to "drive" the large ship. Like the 9/11 hijackers, who only wanted to learn to fly an airliner, these boarders were not interested in learning how to dock the vessel.¹¹
- Intelligence officials have identified cargo freighters they believe are controlled by Al Qaida, which could be used by the terrorist network or its affiliates to ferry operatives, explosive components, cash or commodities on the high seas.¹² One example is a well-dressed middle-eastern man discovered by Italian police who had hidden himself in a cargo container destined for the U.S. He was equipped with a bed, toilet, water supply, satellite phone, laptop computer, cameras and maps. He also had security passes to various airports in the U.S.¹³

Port of Gioia Tauro, Italy



THE THREAT: Organized Crime and Piracy

The threat of piracy on the high seas has grown over the past 10 years, and there is a very credible concern that terrorists and pirates will find common cause¹⁴. The regions of highest concern for shipping are waters off Indonesia, Bangladesh, Malaysia, Somalia and Nigeria¹⁵. Coincidentally, Islamic Extremist terrorist organizations to include Abu Sayyaf, Jemaah Islamiah (JI), and Al Qaida also operate in these areas and could ally themselves with pirates to hijack vessels, or infiltrate vulnerable port facilities in third world countries. Consider the following:

¹⁰ "Qaeda Suspect Was Taking Flight Training Last Month," Patrick E. Tyler, New York Times, December 22, 2002

¹¹ "The Maritime Threat from Al Qaeda," *Financial Times*, October 20, 2003

¹² "Fifteen Freighters Believed to Be Linked to Al Qaeda," *Washington Post*, Dec 31, 2002, p. A1, also "Terrorism – Bin Laden Group Shipping Interests Probed," *Lloyd's List*, Sept. 28, 2001.

¹³ "Italian Court Frees Canadian Suspect," *Toronto Star*, 16 November 2002

¹⁴ "The Maritime Threat From Al Qaeda", *Financial Times*, October 20, 2003

¹⁵ UN Piracy Report

- On 5 November 2005, the cruise liner “Seabourn Spirit” was attacked by machine gun fire and rocket-propelled grenades about 160 kilometers off the coast of Somalia. The assailants were believed to be pirates, although Somalia was and continues to wage a bloody civil war with Taliban-style Islamic extremists. The pirates attacked in a small boat, which was directed from a “mother ship” nearby.¹⁶
- In a recent six-month period there were at least 44 reported pirate attacks in the waters off of Indonesia, and nine more in the nearby Straits of Molucca.¹⁷
- It is estimated that piracy and organized criminal groups who target both cargo ships/bulk carriers at anchor and on the open sea cost over \$450 million per year.¹⁸
- Canada and many other western governments have admitted that their ports and associated facilities are “riddled” with organized crime. There is a real concern that terrorists could take advantage of this security weakness, to infiltrate or exfiltrate a facility, thereby circumventing border control and customs authorities.¹⁹



Armed boats attack a cruise ship off the coast of Somalia

VULNERABILITIES

Ports and shipping remain attractive targets for criminals and organized crime because of the centralized aggregation of both containerized and warehoused goods that often have not yet been subjected to end-user accounting and valuation. This has always, sadly, been known.

More ominously, the maritime industry as a whole is an increasingly important target for both transnational terrorist organizations such as Al Qai'da and its affiliates, and state-sponsored terrorist organizations such as Hizbollah. Terrorists are increasingly aware of the fact that the maritime industry represents an exploitable soft target in terms of smuggling in arms, personnel, or lethal WMD components and as a point of attack. They understand the fact that a strike on a large port facility could cripple a nation's economy, significantly impact world stock markets and cause significant casualties and potential long-term environmental damage. Following are key vulnerable assets in the maritime system:

- **Ports:** Drawbridges and their operation, locks, dams, navigational aids, dock infrastructure (cranes, mooring facilities), pilot boats, multimodal connections (oil and gas



Seaport with HAZMAT terminal facilities

¹⁶ David Eshel, *ibid.*

¹⁷ David Eshel, *ibid.*

¹⁸ U.S. Coast Guard

¹⁹ CanWest News Service, *ibid.*

pipelines, rail access, roads), power and water distribution systems, utilities, communications systems, fuel and HAZMAT depots, and terminal facilities (containers and container yards).

- **Bridges:** Approximately 1.7 million rail cars carrying Hazardous Materials (HAZMAT) move annually through the United States and Canada, alone. Shipments of HAZMAT, which includes ordinance, are a very attractive target to terrorists. The consequences of an attack in a port facility where many drawbridges are located and often in densely populated urban centers would be catastrophic. Bridges are particularly vulnerable to attack by explosives, or explosives tied to chemical/biological agents. Al Qaida has been known to have targeted the Brooklyn Bridge in New York City and the Golden Gate Bridge in San Francisco, among others.



Rail cars carrying hazardous material exploded on bridge

- **Ships:** Cruise liners (vulnerable both from a media perspective if attacked, and as an easy infiltration/exfiltration method), supertankers (vulnerable due to slow speed, particularly when navigating straits or canals), and warships (demonstrated vulnerability to low-tech sea borne attack, a la USS Cole).



Terrorists attack the USS Cole, October of 2000



SOLUTIONS

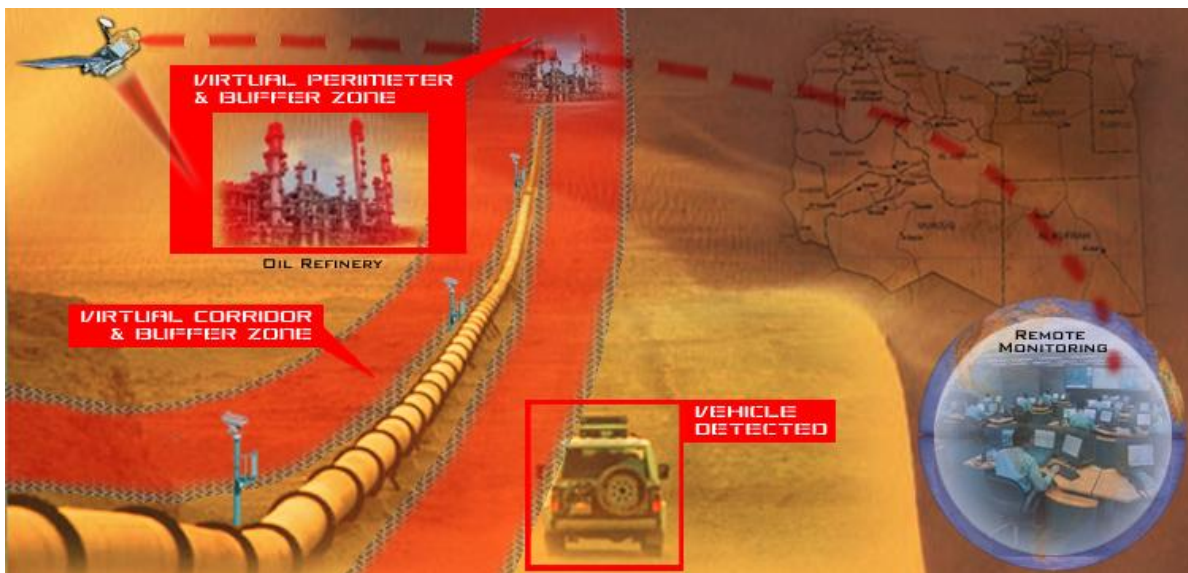
No single security countermeasure such as the container security initiative (CSI) or the terrorist watch list, can adequately address port or maritime security and safety concerns. Technology alone cannot secure ports and shipping, nor can adding additional security procedures, physical barriers, or additional manpower fully mitigate the risk. What will work is an integrated, carefully planned approach that incorporates the best elements of technical, physical, procedural and information security disciplines into a comprehensive strategy.

Duos Technologies and our partners can provide a comprehensive range of sophisticated solutions that address every facet of a customer's security requirements. Working in close consultation with Duos, a full range of countermeasures to security challenges can be developed that mitigate risk to an acceptable level.

TECHNICAL SECURITY COUNTERMEASURES

Duos Technologies provides a broad range of sophisticated, turn-key technology based systems for wide area security, automated surveillance and instrument controls for the private sector and for governments. Duos designs and deploys customized, artificial intelligence-driven digital security systems integrated with actionable video-based surveillance intelligence. Proven Duos technical solutions with potential to be tailored for the maritime industry include:

SECURITY CORRIDOR SYSTEMS (the Virtual Fence): The **Virtual Fence** was developed and is being deployed to harden long, isolated stretches of critical infrastructure such as rail tracks and pipelines. This system could easily be adapted to isolated fence line perimeters as well as pipeline and rail lines entering and exiting port facilities both overland and also across water. The Virtual Fence is based on Duos proprietary digital video recorders (**rvspro™**) driven by the innovative **PRAESIDIUM®** intelligent sensor detection suite which integrates fixed and pan/tilt/zoom (PTZ) high resolution, color, day/night cameras, RF/ID (Radio Frequency Identification) active scanners and other sensor types (chemical/hazardous material, radiation detectors), positioned at strategic locations along the line of the asset whether it is a perimeter, pipeline, or rail line. The system establishes virtual fence lines within the field of view of each of the cameras. Live streaming video is interpreted to deliver low false alarm, real-time, 24/7/365 vigilance for common behaviors that can indicate a security breach. Data is encrypted and transmitted using wired or wireless TCP/IP-based communication either via a chain of WiFi radio transmitters, satellite, and fiber optic or hard-wire connectivity to local and remotely located command and control centers. The Security Corridor System is fully integrated with all other system components to provide centralized command unity.



Oil Refinery Virtual Fence

The **Virtual Fence** performs the following functions:

- Detects moving objects within buffer zones and/or areas declared “off limits”
- Detects objects left behind or removed
- Detects loitering activity
- Detects fence line, pipeline vibration – multiple vibration sensors on the perimeter send signals to the central processor to verify normal vibration patterns (such as from wind/weather, gate closures/opening, other pre-defined “normal” activity), detect tampering, tapping, and to obtain measures of any leaks present in the pipeline network, or unauthorized tampering of switches/points on the rail network.

REMOTE BRIDGE MONITORING AND CONTROL SYSTEM: To address the critical vulnerability posed to shipping and urban areas by drawbridge operations in and adjacent to port facilities, Duos developed the remote Bridge Security System, which is currently being used to monitor and control various critical bridge operations throughout the U.S.

Control and monitoring is effected using a dedicated control console (DCC) or a remote control terminal (RCT). This system incorporates intelligent video, radar, sonar, and audio technologies as well as redundant Programmable Logic Controllers (PLCs), and Safety PLCs. The system automatically detects intruders and suspicious objects left behind (or removed) within a user defined video security zone atop the bridge. The bridge control system, operated from a remote location, raises and lowers the bridge by means of controlling all discreet devices and commands motor operations using Variable Frequency Drive (VFD). A permissive function, whereby the bridge cannot be raised unless permission is granted from the signaling department, is included. Video monitors all river/sea traffic to, from and under the bridge to visually verify bridge conditions before and during lift or lowering operations. In addition, the system transmits audio data to the RCT for determining river/sea traffic and other audio events. A marine grade radar system detects shipping traffic, and seismographic sensors provide bridge impact detection. Events are also automatically digitally recorded, time stamped, and stored for later retrieval. A powerful video search engine (searched by several criteria including time, date, camera number, location) allows for easy retrieval of stored video files.

Upon perimeter breach, strobe lights flash and a multi-language audio annunciation demands that the intruder immediately leave the restricted area.



Remote Bridge Monitoring and Control



Remote Bridge Monitoring and Control

Alarms and live video are broadcast simultaneously to remote monitoring stations. Port Authority enforcement police are enabled to speak over the amplifier in real time (utilizing VOIP via the data highway) to address the subject of the perimeter violation.

SMART Yard Management/Dispatch/Operations/Intelligent Digital Video Surveillance System:

As previously noted, port facilities are typically large, asymmetrical activities dispersed over hundreds of acres of land and water so that they can simultaneously accommodate ship, truck and rail traffic, petroleum product/liquid offload, storage or piping, and container storage. Like a rail yard, they are crowded, and with huge stacks of containers, warehouses and cranes, and often have limited visibility.

Installation of a turn-key **SMART Yard Digital Management Solution** in the port area provides robust, fully scalable live video with real-time, intelligent video capability. This enables the central port authority to coordinate the activities of its personnel and assets day-to-day by monitoring critical road or rail transit areas, checkpoints, or container offload/stack locations. Unprotected crossings can be monitored and critical navigational assets can be monitored for operation or critical change.

SMART Yard was originally designed and deployed for a crowded rail yard activity in the United States deemed part of our nation's critical infrastructure. It lends itself to easy adaptation to port operations, both in large or medium-sized facilities. Using an IP-based architecture as a foundation, **SMART Yard** employs a network of fixed and Pan-Tilt Zoom (PTZ) digital video cameras connected to Duos **rvspro™** digital video servers. Each **rvspro™** includes the rule-based **PRAESIDIUM®** intelligent vision suite to automatically deploy audio and visual alarms, process live video feed and create a video digital archive. The cameras also function as intrusion detectors providing live streaming video of vulnerable security areas and potential threats to vulnerable areas within the facility viewed on a customized, intuitive Graphical User Interface (GUI). The GUI shows intrusion points and critical port locations so that port authority controllers can simultaneously view and control cameras positioned throughout the facility to analyze incoming video and sensor feeds, and thus maintain a real time situational awareness of container operations, rail and/or truck transport on-load/off-load activity, crane operation, warehouse security, and shipping movement in and out of the port facility and adjacent areas.



SMART Yard Management / Dispatch / Operations / Intelligent Digital Video Surveillance System

In addition to remote real-time viewing of events, images are also automatically digitally recorded, time stamped, and stored for later retrieval. A powerful video search engine (searched by several criteria including time, date, camera number, location) allows for easy retrieval of stored video files.

INTERMODAL CONTAINER EXIT SYSTEM (ICES[®]): As previously noted port security and operations are particularly vulnerable to theft, smuggling and vandalism. Terrorism is also an increasingly significant concern, particularly with respect to the movement and identification of containers and contents. Approximately 13 million containers a year move through the U.S., for example, and yet only 2 or 3 percent of these are physically inspected. While it is a daunting challenge to inspect every container, Duos Technologies has developed a system that can identify and track containers and link them to transport companies, drivers and specific vehicles. The system gives law enforcement a significant tool to track containers of concern, and at the same time allows port authorities to keep their operations running smoothly.



Intermodal Security

ICES[®] is a completely automated application for tracking and recording intermodal containers exiting, or entering, a container yard. The core technology of the system is the **Video Optical Character Reader (VOCR)**. The system takes video imagery from moving containers, extracts relevant data (user defined) and populates a database with the extracted data. **ICES[®]** will capture and store the following information in a simple user interface:

- Container numbers
- Trailer numbers
- Front and rear license plates
- Driver's license data
- Video of vehicle and container
- Video and audio of driver and guard interaction at the port
- Biometric capture of fingerprints



ICES[®] is an ideal application for intermodal container yards, rail yards, and port authority checkpoints and weigh stations.

HAZMAT Storage/Fuel Tank Storage Security System: Fuel storage tanks for shipping are of necessity located in or adjacent to port facilities, and typically hold about 60,000 gallons of fuel each. Even if it is diesel fuel, which is not particularly volatile, the addition of an accelerant makes

it quite dangerous. Hazardous chemicals such as chlorine or natural gas are also often stored within port facilities and are an obvious danger, and hence a target, for terrorists. These “tank farms” are considered a part of a nation’s critical infrastructure, and must be secured.

Duos’ role in protecting these assets is the design and installation of turn-key remote viewing and sensor security systems that incorporate audio and visual alarms, process live video feed and create a video digital archive. Systems are defined to simultaneously detect multiple events and process each event in accordance with user-defined parameter settings. PRAESIDIUM® provides multi-sensor support to include chemical (including chemical/petroleum fumes or spill), radiological, nuclear, explosive, GPS, RFID, Biometrics, Radar, Optical Character Recognition, biological, meteorological, trip wire, IR break beam, passive infrared, magnetic, seismic/geophone, and hydrophone.



HAZMAT Storage / Fuel Tank Storage Security System

VIRTUAL GATES: Virtual gates are installed in conjunction with the Virtual Fence application. These are installed at a pre-determined distance from the actual port/marine facility entry point, thus creating a buffer zone. The Virtual Gate serves as a remote controlled advance checkpoint for inbound traffic. Gates include vehicle presence sensors, PTZ cameras, chemical detection sensors, radiation detection sensors, and I/O controllers. Vehicles and personnel approaching the Virtual Gates are detected and the real time video together with potential rule breaches are presented and routed simultaneously to the command and control center and other locations where operators can view live, streaming video images and alarm events in real time.

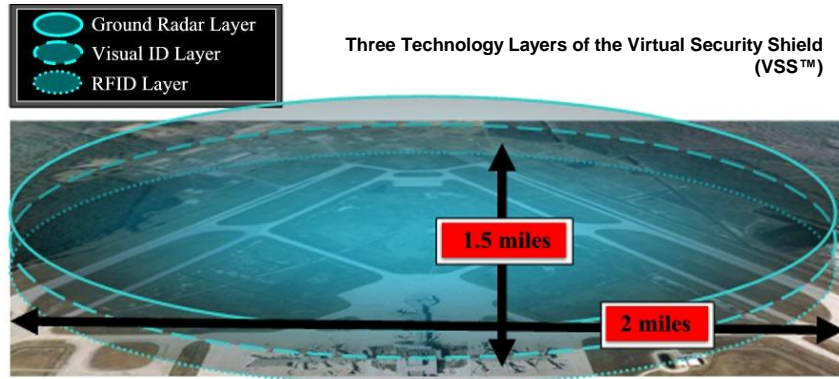
Friend or Foe Detection System (FFDS): This system component is achieved and can be incorporated into a Port Authority’s overall security plan by adding an RFID technology layer. It can be an especially important element of protection of critical infrastructure and hazardous material (HAZMAT) or fuel dump depots and pipeline off-load, or loading points within the port. All personnel and visitors authorized to access the facility would receive an active RFID tag, which is constantly scanned by an array of scanners installed throughout the facility. Tag geo-spatial information (achieved through scanner triangulation) is displayed on the GUI, thus revealing the location of each person at any time. If the Virtual Fence is breached, the



Friend or Foe Detection System (FFDS)

Friend or Foe Detection System (FFDS) automatically validates approaching “authorized” personnel to prevent false alarms.

Virtual Security Shield (VSS™): Port facilities are considered critical infrastructure, and are vulnerable to terrorist attack. Given their value, they should be protected by early detection capabilities. A technology layer is added consisting of ground/buoy-based radar that monitors any activity within a set radius (0.5 – 10 miles). The ground radar data will be stitched and layered to provide a unified multi-layered system. All data from the various layers and sources is fused into a three-dimensional, immersive security tool that provides a tight virtual security shield covering the entire port facility area.



VSS™ includes the following features:

- Detects unauthorized personnel entering the port facility
- Detects unauthorized vehicles approaching or operating in a facility
- Monitors large, specific areas
- Warning of threats towards objects, suspicious activity, or perimeter breaches
- Tracks and classifies people, vehicles, and low flying aircraft
- Signals are layered into a PPI display with multiple dynamic fluctuating tracking plots overlaid into an aerial image of the facility



Live 360 degree panoramic views

- Live-360 degree panoramic views of the facility
- Provides security personnel a window for measured response
- Historical data and imagery is archived and organized in an intuitively accessible database for forensics and post-event analysis
- Open architecture (existing camera infrastructure can be integrated), scalable solution
- Audible and visual alarms alert security personnel
- Extremely low false alarm rate
- Systems can include audible announcements, strobes, or any other required deterrent devices

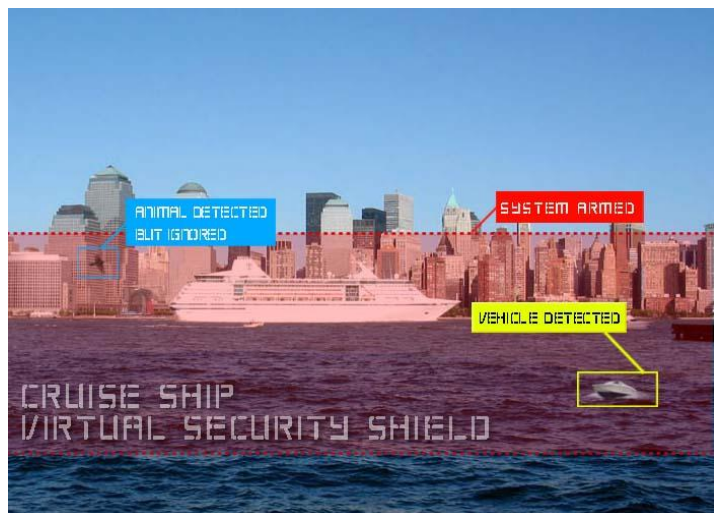
SHIP SECURITY/SAFETY MEASURES

Cruise Ship Virtual Security Shield (CSVSS™): As illustrated previously, the threat of an attack by heavily armed pirates or terrorists from unsecured waters represents the single greatest vulnerability to cruise ships today. Existing warning systems, such as that used by the “Seabourn Spirit” off the coast of Somalia, only provide a single layer of protection from a determined, inbound threat.



“Seabourn Spirit” off the coast of Somalia

Duos Technologies has developed the concept of **CSVSS™**, an enhanced effective coverage system encompassing a 100-yard security zone, a 300-yard no-float zone, and sensitive areas on and in proximity to the vessel. **CSVSS™** enables early detection of any real threat potential through a multi-layered security application to facilitate early detection, classification, and electronic as well as visual verification of objects entering the security zones. The system identifies authorized private craft, crew and passengers, and automatically tracks and classifies as friend or foe entering craft and persons. More specifically, the system facilitates:



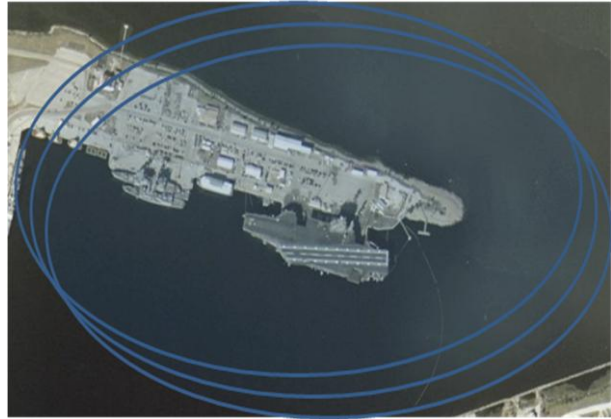
Cruise Ship Virtual Security Shield (CSVSS™)

- Early detection of all vessels, aircraft, and objects approaching from the land, air, and above or below the surface of the water
- Simultaneous tracking of multiple objects/threats
- Early identification, classification and verification of any threat potential
- Security zone-wide traffic verification
- Security zone-wide personnel authentication
- Real-time craft and personnel tracking
- Archiving of all events and responses for forensics and post-event analysis
- Man-overboard alarming and tracking

Naval Ship Virtual Security Shield (NSVSS™): The tragic attack on the USS Cole in October 2004 demonstrated the vulnerability of warships to a low-tech suicide bomber attack at close range

during fueling operations in a port facility. This kind of attack still represents a significant vulnerability to naval vessels, and force protection requires that solutions be developed.

In an effort to prevent these kinds of attacks, Duos Technologies has developed the concept of **Navy Ship Virtual Security Shield (NSVSS™)**, an enhanced, effective coverage system encompassing the standoff area and missile engagement zone in proximity to Navy Ships. **NSVSS™** enables early detection of any threat potential through a multi-layered security application to facilitate early detection, classification, and electronic as well as visual verification of objects entering the standoff area and missile engagement zone. The system identifies authorized vehicles/vessels, and automatically tracks and classifies as friend or foe entering vehicles or vessels. More specifically, the system facilitates:

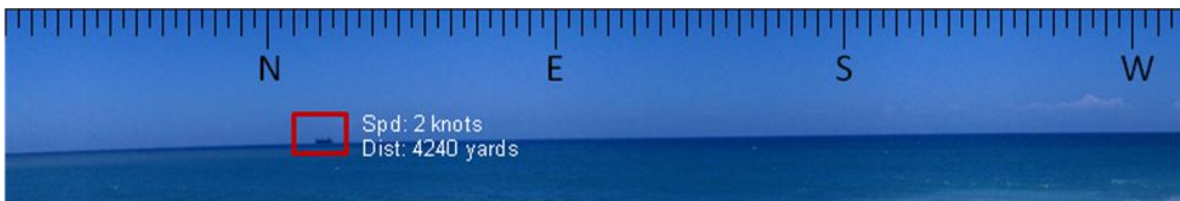


Navy Ship Virtual Security Shield (NSVSS™)

- Early detection of all vessels, aircraft, and objects approaching from the land, air, and above or below the surface of the water
- Simultaneous tracking of multiple objects/threats
- Early identification, classification and verification of any threat potential
- Standoff area-wide traffic verification
- Standoff-wide personnel authentication
- Real-time craft, vehicle and personnel tracking
- Archiving of all events and responses for forensics and post-event analysis
- Man-overboard alarming and tracking



Navy Ship Virtual Security Shield (NSVSS™)



The heart of **NSVSS™** is an exceedingly powerful operator interface in which security information from all sources is fused into one analytical application that compares layers and analyzes data to provide a robust early warning and defense system against intrusions. Today's U.S. Navy, for example, includes 276 active service vessels, all of which are capable of utilizing **NSVSS™**.

PROCEDURAL, PHYSICAL AND INFORMATION SECURITY SOLUTIONS

Duos Technologies, with its rich, insightful in-house counterterrorism experience and expertise in risk and threat analysis and wide area security, continually tracks the rapidly evolving government and commercial enterprise security environment of today, critical due in large part to sustained threats from trans-national terrorism and organized crime.

Our strong ties with partners in both the government and commercial sectors who specialize in procedural, physical and information security help Duos with confidence provide full spectrum tailored vulnerability client asset risk assessment and deliver solutions that comprehensively address complex, multi-faceted security issues. Our technology applications are scalable, and can be infinitely adjusted to anticipate unique, elevated threat and risk.

