USING TECHNOLOGY TO BRIDGE MARITIME SECURITY GAPS

Dale Ferriere

National Infrastructure Institute Center for Infrastructure Expertise
100 Arboretum Drive
Suite 306, Portsmouth, NH 03801 USA, dferriere@ni2.org

Khrystyna Pysareva, Andrzej Rucinski

University of New Hampshire, Department of Electrical and Computer Engineering,
Kingsbury Hall, Durham 03824, USA, pisareva@unh.edu, andrzej.rucinski@unh.edu

Summary

The International Ships and Port Facility Security Code (ISPS Code) [4] has established security requirements for applicable waterfront facilities, commercial ships, and port areas. Although these regulations have improved maritime security, gaps and regulatory bottlenecks remain.

An ongoing security concern is the inability of port state control and customs officials to obtain comprehensive background information associated with an arriving merchant ship's commercial enterprise i.e., ships management, crew management, charterers, cargo broker, etc. This situation is especially alarming for container ships, car carriers, and other cargo ships, where potential hiding places for Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) weapons and their components are enormous.

This paper identifies critical maritime security gaps and explores adapting existing commercial off-the-shelf technologies as possible solutions. Operation Safe Commerce – Canada United States Cargo Security Project [2] is presented as an illustration of resolving potential cargo security problems with technological solutions.

The merit of utilizing technologies for maritime security is undeniable. The use of proven technology will minimize regulatory oversight costs for legitimate shipping companies, creating economic and security incentives for all stakeholders.

1. Introduction

Government authorities know where gaps in port and maritime security exist. Through implementation and eventual enforcement of new maritime security regulations (e.g., International Ship and Port Facility Security Code and US Maritime Transportation Security Act), officials are mandated to improve port security. Consequently, these officials are put in the unenviable position of enforcing new regulations without adversely affecting commerce. Critics of these efforts seem to focus on one of two things: criticize security gaps, or criticize the adverse impact increased security has on maritime

commerce. The key to overcoming these criticisms and the challenge for technologists is to apply technology, which enables regulators, law enforcement, and industry officials to concurrently improve maritime security while also enhancing maritime commerce.

2. Maritime Security Gaps and Vulnerabilities

Gaps in maritime security are defined as possible areas where terrorists may target either a commercial ship, or a port facility, or use the ship, or its cargo, or its crew to execute an act of terrorism directed at critical port infrastructure. For instance, if terrorist attacks were to simultaneously disable two large American port facilities, one on the Pacific coastline and one on the Atlantic coastline, then this could be the catalyst for a possible global economic catastrophe. The following description summarizes existing maritime security gaps and frames the associated challenges for technologists to resolve.

2.1. Containerized Cargo for Intermodal Transportation

The use of containers to transport cargo has increased exponentially [5]. Because of challenges associated with being able to unobtrusively verify a cargo container's contents without incurring a commercial delay, there is an obvious security vulnerability associated with the potential use of a container for transporting weapons, illegal substances, or terrorists. The technologist's general challenge, therefore, is to make the contents of the cargo transparent to port authorities while maintaining container integrity, and not incurring commercial delays detrimental to the free flow of commerce.

2.2. Ferries

Municipal ferry services transport hundreds of thousands of people and vehicles each year. Also, in remote locations, such as Washington State, Alaska, and Maine, the state operated ferry services are critical to the survival of outlying coastal communities. Access to the ferry terminals and surrounding areas is relatively open. This openness, while making it easier for commuters and visitors to access the ferry service, also presents serious vulnerabilities. Disruption of a major ferry service could have disastrous economic ramifications in addition to the possible significant loss of life. The technologist's challenge, therefore, is to distinguish legitimate port users and ferry passengers from those desiring to do harm without infringing upon civil liberties, and without creating adverse delays during the ferry passenger screening process.

2.3. Cruise Ships and Large Pleasure Vessels

The port vulnerability presented by cruise ships is similar to what is posed by ferries, except that there is more significant potential for loss of life. Because of the typically large number of multi-cultural crew members on a cruise ship or a pleasure vessel, the threat to port security created by an arriving cruise ship is more diverse. Hence, the technologist's challenge is to distinguish legitimate cruise ship passengers, large numbers of crew, and other service providers from those desiring to do harm without infringing upon civil liberties and without creating commercial delays. Additionally, the technologist's challenge is to identify better ways to unobtrusively protect the cruise ship while it is in port and underway from possible external threats e.g., USS Cole style attack, without infringing upon the passengers' enjoyment of their cruise ship experiences.

2.4. Car Carriers

Tens of thousands of vehicles are imported to various countries on a daily basis. Often, these vehicles are kept at the holding facilities where they are manufactured until they are ready for shipment. Similarly, once off-loaded from the ship, thousands of vehicles are rolled (driven) by longshoremen into a holding area and made ready for the next leg of their journey through the supply chain. It is at the load port, arriving port's vehicle-holding-facilities, and during the sea transport phase, when the vehicle is vulnerable to the possibility of it being converted to a possible weapon delivery tool. During the sea-phase of the importation, even with closed circuit television and other monitoring devices on the cargo decks, there is ample opportunity for a distraught seafarer or stowaway (terrorist) to tamper with the to-be-imported vehicle. Citing the vast quantity of

vehicles and the pace at which longshoremen transport the cars from ship to the shore, the opportunity to visually detect any tampering is limited. Therefore, the challenge for the technologist is to identify a process to unobtrusively detect whether or not a to-be-imported vehicle has been tampered with, and to accomplish this without delaying the vehicle transfer from ship to shore.

2.5. Underwater Sabotage of a Port Facility

With the advent of today's terrorist-risk-reality, and with respect to the nation's economy, America's private and public port facilities are identified as being vulnerable to attacks from underwater divers and remotely operated underwater vehicles. The challenge for the technologist is to protect the port infrastructure by identifying counter-technologies to combat possible attacks by underwater divers and remotely operated underwater vehicles without adversely impacting a port's capability to openly and freely accommodate maritime commerce.

2.6. Tankers and Gas Carriers

When determining if an at-sea armed boarding of an arriving foreign flagged commercial ship should be performed prior to it being allowed port entry, some port state authorities give special recognition to high consequence cargoes e.g., crude oil, petroleum products, LPG (Liquefied Petroleum Gas), LNG (Liquefied Natural Gas), etc. Because the incident magnitude associated with a potential terrorist act involving a high consequence cargo is so great, port security officials require a greater level of assurance about the people intimately involved with the high consequence cargo shipment.

Therefore, the challenge for the technologist is to create a system, which concurrently improves the port officials' capability to have adequate assurances that those overseeing the ship and cargo operation are not intending to use them as weapons while minimizing port delays.

2.7. Hazardous Material Cargo Placards

Shippers are required to place placards on containers with hazardous materials [3]. However, officials have expressed their concern that these placards might also identify potential targets for terrorists. The challenge for the technologists, therefore, is to make first responders aware of hazardous material containers, drums, and other means of hazardous material stowage for transportation, without facilitating the identification of the hazardous material contents to potential terrorists.

2.8. Terrorists Masquerading As Professional Seafarers and/or Professional Waterfront Workers

Similar to the possibility of terrorists posing as passengers, the potential threat also exists for terrorists to infiltrate a shipping company posing as a legitimate seafarer with proper marine licenses, visas, and passports. The concern here would be the risk associated with access to key ship components and/or the ship's cargo.

The challenge for the technologists, therefore, is to design a process of credentialing. An effective credentialing system should enable the Ship Security Officer, Facility Security Officer and port officials (coastguard, customs and immigration officials) to easily distinguish an arriving foreign seafarer and/or a newly employed waterfront worker as legitimate, and to develop assurances that these workers and seafarers do not have the intent to do harm when at their shipboard or shore-side workplace.

3. Technologies for Maritime Security

3.1. X-Ray, Gamma Ray, and Neutron Scanning

These are devices used to scan objects for the presence of drugs, weapons, and explosives. Systems vary with the method of detection: X-Ray scan, backscatter X-ray, gamma ray, fast (or high energy) neutron scan. They also vary in size and configuration: small handheld devices, stationary devices (like those used in the airports for baggage scan), and large fixtures for container or truck scanning. Among major tradeoffs of these systems are high cost and slow speed.

3.2. Biometrics

Voice recognition is one of the most studied and developed trends of biometrics. Currently,

fingerprint identification acquires more and more popularity with the increasing number of available COTS (Commercial Off-The-Shelf) products for fingerprint scanning, processing, and database support. Technology development in this area tends towards miniaturization of the system. Currently a PC station is needed for fingerprint identification. Implementation of the system in ASIC (Application Specific Integrated Circuit) would reduce not only the size of the system, but also its cost [6].

Other biometric technologies include iris scan, retinal scan, facial recognition, and vascular patterns recognition (thickness and location of the veins in human's hand or face) [11].

The best approach for a successful human identification is a multimodal biometrics, i.e., incorporation of several biometric parameters to identify a person. This approach provides higher reliability and reduces the number of false alarms.

3.3. RFID (Radio Frequency Identification) Tags

A simple RFID tag consists of a microchip attached to a radio antenna. The microchip contains information about the type of cargo, manufacturer, serial number, etc. A variety of tags are available on the market: passive tags, active tags, low-, high- and ultra-high frequency ones. An RFID tag is typically mounted on a container.

There are special cases when it is desirable to place a tag on the cargo itself, for example, when transporting high-value cargo. In this case reading of a tag cannot be done directly from outside of the container. For smart containers, an RFID interrogation device can be incorporated into the system installed inside of the container. By doing this, readings from the tags are transmitted to the outside world by an in-container transmitter.

3.4. Underwater Surveillance

One of the methods of underwater ship hull inspection is to use specially trained divers. Liability and risk associated with this method call for a technical solution. Remotely operated vehicle (ROV) is a robotic system for underwater operation. ROVs vary in size and configuration, e.g., number and type of cameras, mechanical tools, presence of sonar and other sensors. There are a number of commercially available ROVs specifically designed for harbor security. These devices are used for underwater surveillance, ship hull inspections, dock inspections, etc.

Another approach is to use stationary underwater installations equipped with sonar or other acoustic technologies.

3.5. Smart Containers

Designing smart container technology is currently one of the most noticeable trends in the cargo security area. One illustration is the Canada-United States Cargo Security Project [2]. The container part of the system consists of a number of sensors for detection of CBRNE substance presence, sensors for detection of tampering, data logging unit, a GPS receiver, and a transmitter. Ultimately, an interoperable system should be able to communicate, collaborate, and integrate with other systems used by shippers, law enforcement, and first responder officials. Currently this issue is addressed through use of a secure website, which authorized person may log on and view the container status.

3.6. Port Security Web Board Query

This is an initiative to create an interactive, secure web-board software application for remote interviewing foreign ship representatives prior to the ship being allowed entry into a country's national waters. Advantages of this proposed system are real time communication, and the capability of involving more than two parties during the remote interview. Along with the ship's Master, behind-the-scenes parties like the ship owner representatives and chartering company representatives would logon to the web query. As part of the screening process, port state officials would require the foreign ship's Master, (Shipping) Company Security Officer, and representative from the charter to provide answers to questions. Risk assessment software could process their answers and generate a decision on whether: (a) the ship should be allowed direct port entry; (b) the ship's entry would be rejected; or, (c) the ship should be required to pass additional security screening. This system would provide

legitimate shipping companies with an opportunity to be distinguished for their enhanced security efforts, and their ships be given access to a "maritime green lane", enabling them to optimize their in port cargo operations.

4. Technology Application Summary

4.1. Containerized Cargoes for Intermodal Transportation

X-ray screening is already adopted in some ports for containerized cargo. Other ports are still reluctant to use this method due to the high cost of screening equipment, the need for specially trained operators, and time delays associated with the screening process. Using smart containers should address the issue of cargo container security.

4.2. Ferries and Cruise Ships

The biggest security challenge for both cruise ships and ferries is associated with the large number of passengers and their baggage. Biometric technology and baggage screening help to acquire better control of people and substances present on the vessel.

Another security measure is to equip the ship with an advanced surveillance system and sensor network [1, 9]. The surveillance system can use face recognition for detection of unauthorized human presence in certain parts of the vessel. The sensor network monitors the environment for presence of radiological materials and biochemical hazards.

4.3. Car Carriers

The best and the most convenient time for the security screening of the vehicles is during loading and unloading when the vehicles are driven on and off the vessel at a low speed. It is possible to install a booth with a CBRNE detection system in a vehicle's path. Development of such a system for a highway tollbooth application is already in progress [7]. Along with this nuclear detection system, an x-ray scan system could be installed at the same point. The system would be equipped with pattern recognition software that detects deviation of the image from the standard pattern expected from an automobile during transportation.

4.4. Underwater Sabotage of a Port Facility

Underwater surveillance systems are already widely used in port facilities. There are also mechanical solutions to the problem, such as buoys specially designed for security applications. Buoys essentially create a mobile marine security barrier.

4.5. Tankers and Gas Carriers

The security measures for these types of ships are already at a very high level. The greatest remaining security concern is ensuring that all the parties involved in the ships operation are legitimate. This is yet another reason for the port security web board query.

4.6. Hazardous Material Cargo Placards on Marine Containers

RFID tags represent the best solution for the hazardous material cargo marking. Placing an RFID tag on the container reduces possibility of tampering with the label and with mislabeling. It would also require much greater effort by a potential terrorist to identify the hazardous material cargo.

5. Risk Analysis

Security related risk can be described and estimated using probabilistic mathematical models. A commonly accepted formula for risk evaluation is the following [8]:

$$\text{Risk} = (\text{Threat} \cdot \text{Vulnerability}) \cdot \text{Consequence} \quad (1)$$

Threat – is the likelihood that a given malicious action or attack will be initiated against a specific target.

Vulnerability – is the likelihood that a particular malicious action or attack is successful.

Consequence – is a measure of loss experienced in case of a successful attack.

Threats are external factors that we can not eliminate or influence *directly*. We also cannot reduce the cost of loss in case of a successful

attack. Trying to reduce this factor would actually mean reducing the value of the assets we are trying to protect. Hence, the only way to reduce a risk is to directly reduce vulnerability by using countermeasures. In a risk equation, Countermeasures can be accounted for in the following way [10]:

$$\text{Risk} = \left(\frac{\text{Threat} \cdot \text{Vulnerability}}{\text{Countermeasures}} \right) \cdot \text{Consequence} \qquad (2)$$

Risk management is an evaluation process for determining how much one or more of the countermeasure technologies is capable of reducing the risk for particular assets. It is important to remember that risk can not be eliminated completely, and that after a certain point, investing in countermeasures becomes economically unfeasible due to small risk reduction. This is demonstrated in Fig. 1.

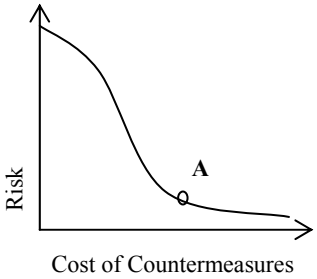

Figure 1. Risk as a function of countermeasures.

Before a country allocates its port security funds for counter-terrorism technology, there needs to be a recognized and accepted risk management process. By standardizing how risk is evaluated at the port level, taking into account a port's inter-dependency factors i.e., economic, iconic, population, etc., this will allow the creation of an equitable process for comparing counter-terrorism technology effectiveness. By measuring counter-terrorism technology in terms of how well it mitigates standardized terror-related risks at the port level, a country will have a qualitative understanding how well it is allocating funding to enhance port security.

6. Conclusion

Considering the above from a technology standpoint there are a number of challenges to improve maritime security (in order of importance): (1) Need for national and international standards with how terrorism-related risks are, at the port level, defined, evaluated and contrasted; (2) Need for further exploration and further development of port security technologies; (3) Need for turn-key port security solutions, which address administrative and technological interoperability; and (4) Need for greater inclusion in the development and application of port security technologies of leading, distinguished, non-national shipping companies and international seafarers.

References

[1] D. Campbell: *Designing automated wide-area surveillance systems*, Security Magazine, April 1, 2005

[2] *Canada-United States Cargo Security Project*, National Infrastructure Institute Center for Infrastructure Expertise www.ni2cie.org

[3] *Chertoff to first responders: Hazmat placards stay, IAFC On Scene*, Volume 19 Number 8, 2005

[4] International Maritime Organization: *International Ship and Port Facility Code*, 2003 edition

[5] P.T. Leach: *Power play*, Journal of Commerce, Volume 6, Issue 20, May 2005

[6] J. Mocny: *SoC prototyping for biometric authentication*, University of New Hampshire Department of Electrical and Computer Engineering, 2004

[7] *PPPL researchers develop anti-terrorism device*, PPPL Digest, 2003

[8] *Risk assessment and prioritization*, Volpe Journal, 2003

[9] *Security and Surveillance Solutions, White* paper, Sarnoff Corporation, Pyramid Vision, 2004

[10] I. Winkler, *Spies Among Us: How to Stop the Spies, Terrorists, Hackers, and Criminals You Don't Even Know You Encounter Every Day,* Wiley, 2005

[11] J. D. Woodward, N. M. Orlans, P. T. Hoggins: *Biometrics*, McGraw-Hill, New York, 2003