CHALMERS

Providing Port Resiliency through Technology

Terrorist and Natural Threats: The ISPS Code and Emerging Technologies

Master of Science Thesis in the Master Degree Program

Nordic Master in Maritime Management

VAHİDE BELGİN ÖNEM

Department of Shipping and Marine Technology

CHALMERS UNIVERSITY OF TECHNOLOGY

Göteborg, Sweden, 2011

REPORT NO. NM-11/18

Providing Port Resiliency through Technology

Terrorist and Natural Threats: The ISPS Code and Emerging Technologies

Master's Thesis in the Master's Program in Nordic Master in Maritime Management

VAHIDE BELGIN ONEM

Supervisor: ROBERT SEVERIN

Department of Shipping and Marine Technology
CHALMERS UNIVERSITY OF TECHNOLOGY
Göteborg, Sweden

Title: Providing Port Resiliency Trough Technology

Terrorist and Natural Threats: The ISPS Code and Emerging Technologies

Author: Vahide Belgin Önem

Report No: NM-11/18

Department of Shipping and Marine Technology

Chalmers University of Technology

Göteborg, Sweden, 2011

SE-412 96 Göteborg

Sweden

Telephone: +46 (0)31 772 10 00

Chalmers reproservice

Göteborg 2011

ABSTRACT

With the virtual removal of country borders and changing modes of production, maritime ports have emerged as vital components of the global supply chains. Significant potential repercussions of long term disruptions to the global supply chain operations have rendered the maritime ports an attractive terrorist target and important asset during natural disasters. Referring to the quick recovery ability of ports from natural and terrorist threats, authorities have coined the term resiliency and devised strategies and frameworks for providing increased resiliency.

In the aftermath of the terrorist attacks of the new millennium targeting maritime assets, the IMO has introduced the ISPS Code as an appendix to the SOLAS. The ISPS Code introduces new mandatory security and risk assessment procedures to improve the security of the ports. However, this code does not include any guidelines for the implementation and assessment of its requirements leaving the stakeholders in the dark.

The purpose of this thesis is the identification of emerging technologies that can help in implementing policies aimed at increasing the port resiliency against terrorist and natural threats. Additionally, guidelines regarding the incorporation of these technologies into the implementation process of the ISPS Code as well as how much the ISPS Code is pertinent to the resiliency planning process is also discussed.

In the beginning, resiliency is defined as a measure of robustness. In the theoretical part, the major elements of resiliency planning work, namely the threats to resiliency, how to assess the risks of these threats in the port operation, and how to mitigate these threats and risks to provide

increased resiliency are described and discussed in detail. The problems of risk assessment against terrorist threats due to the involved human factors are included and its deviation from traditional risk assessment procedures is discussed. To relate the resiliency planning process to the tasks of the ISPS Code implementation, the ISPS Code is discussed in detail. Following these summary sections, a literature review of emerging technologies pertaining to the maritime domain is included and a discussion as to how these technologies can be adopted for providing increased resiliency.

In conclusion, emerging technologies such as radars, sonars and imaging technologies are very useful in providing awareness in the port environment and can provide knowledge aids in the aftermath or during the terrorist or natural events and result in increased resiliency. The key element in providing these aids is the use of emerging information technologies to condense the huge amount of information incoming from various sensors into usable and easily sharable information aids, this is the main idea behind the cognitive ports which also involve automated decision making rules. However, this vision is only realizable given the information sharing incentives and framework are available among various stakeholders, the ISPS Code partly achieves this goal.

TABLE OF CONTENTS

TABLE OF FIGURES

LIST OF TABLES

ABBREVIATIONS

The ISPS Code …….. The International Ship and Port Facility Security Code
US ……..United States
DHS……The US Department of Homeland Security
JIT……..Just-in-time strategy
FBI……Federal Bureau of Investigation
IMO……..International Maritime Organization
MTSA……Maritime Transportation Security Act
FSPs……Facility Security Plans
LNG……..Liquefied Natural Gas
SOLAS……Safety of Life at Sea
ISSC……International Ship Security Certificate
EU……..European Union
DOS ……..Declaration of Security
SOC……..Statement of Compliance
SSA……Ship Security Assessment
PFSA……..Port Facility Security Assessment
SSP……Ship Security Plan
PFSP……..Port Facility Security Plan
PFSO……Port Facility Security Officer
RSO……..Recognized Security Organization
CSO……..Company Security Officer
SSO……Ship Security Officer
GPS……..Global Positioning System
HF……..High Frequency
AIS ……Automated Identification Systems
MDA……Maritime Domain Awareness
OTH……Over the Horizon
SAR……Synthetic Aperture Radar
M/V……..Motor Vessel
CBR……Chemical Biological or Radiological
VTS……..Vessel Traffic Services
OCR……..Optical Character Recognition
ICIS…….. Integrated Container Information System
SAIC ……Science Applications International Corporation
RPM……Radiation Portal Monitor
RFID……..Radio Frequency Identification
CGC……Coast Guard
TSA……..Transportation Security Administration

1. INTRODUCTION

With the virtual removal or country borders and trade tariffs, production facilities have been centralized and moved to the locations where cheap labor is abundant. As opposed to the traditional approach in which the production takes place at several locations where the raw production resources are available, the emerging mode of production requires transportation of raw materials to the production facilities as shown in Figure 1. Consequently, the finished products have to be taken to the customers or sales points, requiring another transportation effort. Maritime, being the most efficient and cheapest mode of transportation as indicated by Figure 2, has an important place in this novel mode of production and also has the highest share compared to land and air transportation modes.

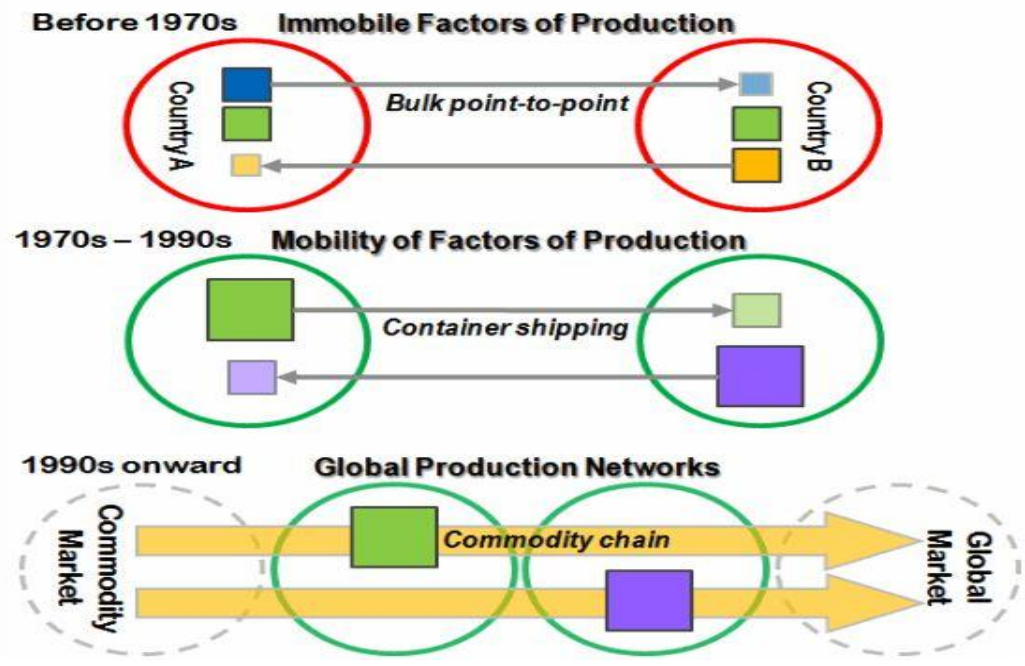


Figure 1 Changes in the factors of production and the emergence of a global supply chain. (Rodrigue, THE GEOGRAPHY OF TRANSPORT SYSTEMS, 2011)

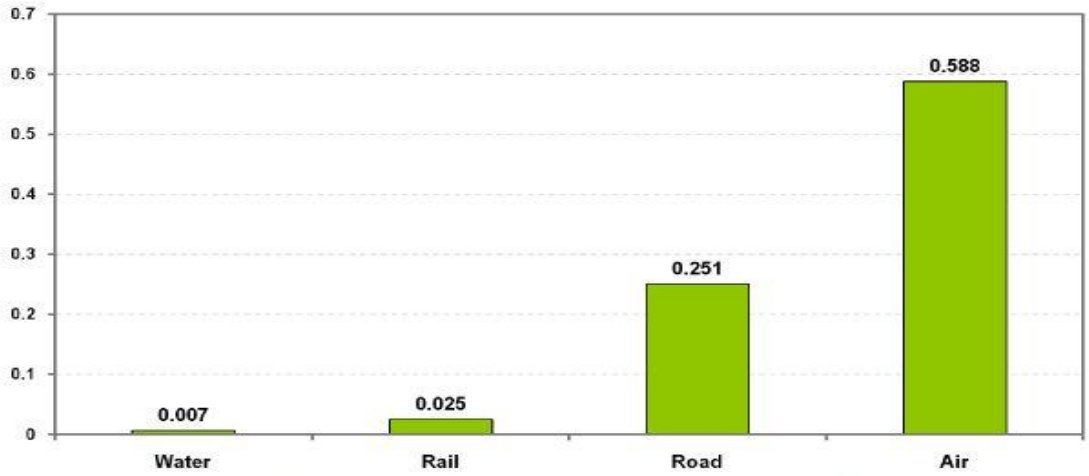


Figure 2 Transportation costs per ton-mile. (Rodrigue, THE GEOGRAPHY OF TRANSPORT SYSTEMS, 2008-2012)

Since the production efforts take place in centralized locations, efficient operation of production facilities require complicated networks of suppliers, transportation mechanisms, and sales points which can be termed as the global supply chain, this mode of operation is shown in the bottom part of Figure 1. Disruptions in one of the elements of the global supply chain can bring all the production and sales efforts to a halt and can have dire consequences.

As maritime transportation is becoming more and more the major mode of transportation, ports where transition from maritime to other modes of transportation or vice versa takes place, become essential constituents of the global supply chain. It can easily be said that ports are not the places to unload or load goods anymore but an important component of the global supply chain, therefore, their proper operation has to be ensured at all times to prevent disruptions in the global supply chain. The increased dependency of the world on the free movement of trade by vessels as indicated by Table 1 suggests that the maritime operations should not be disrupted for prolonged times.

In maritime context, a port is defined as the interface between the waterborne vessels and land adjacent to a body of water. A port can be a facility for managing the transfer of cargo, raw materials, and/or people between the land and the water. As the dependency of the world increased on maritime transport has increased, the worldwide value of shipping routes and ports to the economics of nations took on greater and greater importance.

This dependency makes the ports an important component of the global supply chain and an attractive terrorist target. Scenarios involving the dispersal of radiological materials or nuclear detonation and extended port operational disruptions have been identified as a major risk to the container shipping industry (Greenberg, Chalk, Willis, Khilko, & Ortiz, 2006). There are several indications that global terrorist organizations such as Al-Qaeda are interested in causing economic harm to a targeted country or region as they carry out their plans.

Table 1 Growth in Container Trade, Top Ten U.S. Ports, 1999 and 2004 (in TEUs)

TOP TEN PORTS IN U.S CONTAINER TRADE	1999	2004	%CHANGE 1999 TO 2004
LA/Long Beach	5,599,524	8,638,986	54.3
New York	2,027,188	2,200,343	56
Charleston	1,169,552	1,421,047	21.5
Virginia Ports	908,902	1,302,122	43.2
Savannah	624,497	1,209,178	106.6
San Francisco	943,977	1,221,111	29.4
Houston	713,677	1,097,769	53.8
Seattle	961,847	1,049,105	9.1
Tacoma	581,162	940,638	61.9
Miami	618,436	1,043,839	68.7
Top Ten Total	14,148,762	21,064,776	48.9

Data Source: U.S. Maritime Administration.2005.

The economic impacts of terrorism can be classified into three categories (Jackson, Dixon, & Greenfield, 2007):

1. The costs of the attack itself
2. The costs of security in mitigating the threat of future attacks as well as the associated indirect costs, such as increased wait times for security searches
3. The costs resulting from behavioral changes as a result of the fear of future attacks, such as decreased demand for goods and services (e.g., air transportation).

These possible consequences and economic impacts of terrorism necessitate a change in the public policy direction in the maritime and port security realm serving to reduce not only the immediate physical threats from terrorism, but the long term economic threats that could befall the industry, the nation, and world markets. This fact makes it very easy to understand the push for new government security regulations in the maritime and port environment stating that the maritime industry as a whole must be viewed as a critical infrastructure and included in comprehensive planning process. This increased dependency is the reason why the security management process must now reexamine port applications and plans that place a high priority in reducing threats to this industry. This fact also necessitates the development of joint initiatives and relationships between the private and public sectors in securing maritime interests from the threats of terrorism and criminal activity.

In addition to terrorism, there are several other factors capable of disrupting the port operations including but not limited to natural disasters, accidents, human related reasons, security lockdowns, port network failures, and equipment breakdowns. To minimize the probability and extent of the disruption, the port authorities, and management have to be ready

for such factors and should have an action plan in place. Resilience in the context of port operations refer to such a readiness for possible future uncertainties and are gaining more and more importance as the ports become essential constituents of the global supply chain. Several natural events as well as recent terrorist attacks have shown that there are no guidelines or instructions on how to prepare for or proceed after an event disrupting the port operations. Because of the lack of guidelines, the port operations take very long to resume or fully recover resulting in poor resiliency. The ISPS has recently been modified to address the risks associated with ports and provide increased resiliency but the changes are far from complete and their implementation is not very clear. For a better implementation of the ISPS code, risks associated with port and vessel operations has to be identified, procedures and security measures have to be identified and designed to minimize the consequences of each of these threats, and ways of utilizing the newly emerging technical tools should be postulated.

In the implementation of the new security and resiliency measures, both technological changes and behavioral changes needed. Port directors and port security managers play pivotal roles in managing the complex interrelationships of the port stakeholders necessary to maximize productivity, while concurrently generating a safe and secure port environment. For example additional checking of the port entrances and exits may necessitate additional security personnel or automated scanners. The important and complex role of technology in this context is the balancing of technological and human resources in port protection systems.

The purpose of this thesis is answering the following five questions:

1. What are the major threats to the port resiliency?

2. What actions and guidelines can be formulated to either prevent these threats or minimize the consequences if prevention is not possible?
3. What is the role of the mandatory ISPS Code in addressing the natural and terrorist threats to the port resiliency?
4. What are the similarities of resiliency planning process and the ISPS Code implementation tasks?
5. How can the technological developments in the maritime industry help in providing port resiliency while causing minimal disruption to daily port operations?

2. BACKGROUND

2.1 What is resiliency

The 2008 edition of the Merriam-Webster Dictionary defines resiliency as "an ability to recover from or adjust easily to misfortune or change." In the light of the recent terrorist attacks with global consequences, this term has gained a lot of popularity especially in the context of national security. For example, U.S. Department of Homeland Security (DHS) has included these three very similar definitions of resiliency in their lexicon:

- The ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions
- The ability of systems, infrastructures, government, business, and citizenry to resist, absorb, recover from, or adapt to an adverse occurrence that may cause harm, destruction, or loss of national significance.
- The capacity of an organization to recognize threats and hazards and make adjustments that will improve future protection efforts and risk reduction measures.

In a more detailed definition, Rita Parker (2010) claims that the resilience from a strategy point of view is the result of four factors being achieved. These factors are:

- Robustness: An ability to maintain and continue to function during disruption
- Resourcefulness: Managing the response to a disruption as it unfolds
- Rapid Recovery: Ability to return to normal after a disruption.
- Absorption: Extract lessons after a disruption to reduce vulnerability.

From these four factors, the absorption stands out as an important factor because resiliency plans deal with future uncertainties. According to the report "Evaluating Transportation Resilience" by Victorian Transport Policy Institute (2008), resilience addresses uncertainty. If the future was predictable, the resilience would lose its importance. Currently resilience plans must address a wide range of possible conditions, including some which may be unlikely but which could result in significant harm if they are not anticipated. As a result, absorption becomes very important since it involves extracting information from previous events and estimating the consequences of a similar future events and developing plans to address these consequences.

In his PhD dissertation, Pitera (2010) extends this definition to cover the supply chain operations and states that "resiliency also includes the ability to avoid or reduce exposure to disruptions." According to Pitera (2010), a resiliency strategy has to reduce the occurrence of or mitigate the effects of disruptions, allowing a supply chain to maintain or return to normal operating conditions. For port and harbor operations, which are essential parts of the global supply chain, resiliency has other important implications. The Harbor Safety Committee Conference defines resilience as "the capability to expeditiously recover and reconstitute vital services with minimum disruption". In port operations concept, the word expeditiously becomes significantly important since extended disruptions can lead to irrecoverable consequences. Christopher and Peck (2004) define supply chains as dynamic networks that are ever-changing. If a disruption in a port takes very long to return to normal conditions, the supply chain can adapt to changing these conditions by shifting the traffic to another port. Worse, this shifted traffic may not return back to the original port after the disruption is long gone as the past examples have shown such as the case of Port of Kobe after the Great Hanshin Earthquake. This is the main

discerning factor of the port resiliency from the definitions of resiliency in other contexts and significantly increases the importance of resiliency in port operations.

2.2 The importance of resiliency in the context of supply chains

With the recent changes in the world trade patterns to further reduce the costs and increase the profits such as the emergence of China and India in the world's largest economies, the supply chains are becoming more complicated as they are lengthened and leaned, and they can rapidly adapt to changes (Christopher & Peck, 2004).As a result of these changes, the supply chains are more prone to disruptions (Yossi, 2005).With the supply chain becoming more and more global, the disruptions abroad now have as much capacity to effect supply chains as domestic disruptions (Pitera, 2008).

Additionally, to further increase the profit margins, enterprises have started operating on a Just-in-Time (JIT) strategy, where supplies or components arrive at the exact time they are needed instead of being held in inventory (Yossi, 2005). This mode of operation, make supply chains even more vulnerable to disruptions. For example, after the events of September 11, the trucks carrying the vital components for the Ford Motor Company had been held at the borders due to security reasons, and as a result the production had to stop along several assembly lines. Similarly, after the 2011 Japan earthquake, several car companies in the US had to reduce their production since the suppliers in Japan could not resume production immediately.

As a result of the above explained changes in the world trading patterns and new modes of operation to further increase the profit margins, the supply chains and their components including the ports have become more vulnerable to the possible sources of disruptions and better resiliency is needed to evade global disruptions that can have catastrophic consequences.

2.3 Threats to the resilience:

As stated by Victorian Transport Policy Institute (2008), the resiliency addresses the uncertain events and plans to remedy the after effects with minimal disruption. As a result, there can be many threats to the resilience being known and unknown. We can currently classify these possible threats into the following categories, however, there can be many more threats that are currently unknown to us at this time:

- Terrorism
- Natural disasters
- Accidents
- Worker strike (human related reasons)
- Security lockdowns
- Port network failure
- Equipment breakdowns

Since the technological developments can mainly help in providing resilience against the terrorism and natural disasters, the other threats to the resilience will not be studied in this thesis to limit the scope of this study.

2.3.1 Natural Disasters

The recent earthquake in Japan and the consequent failure of the nuclear power plants have shown that preparation for natural disasters have to consider all possible consequences. The nuclear power plants are built to withstand strong earthquakes but same cannot be said for the

tsunamis happening just after the earthquake. The natural disasters that can disrupt port operations can include but not limited to earthquakes, tsunamis, lightning strikes, strong winds, and fires. A photo of the Port of Kobe after the Great Hanshin earthquake is shown in Figure 3 to emphasize the possible amount of damage in an earthquake.

Figure 3 Port of Kobe after the Hanshin earthquake. (Georgia Tech)

2.3.2 Terrorism

According to the U.S. Federal Criminal Code (2004), terrorism involves violent or harmful acts that appear to be intended to intimidate or coerce a civilian population, to influence the policy of a government by intimidation or coercion, or to affect the conduct of a government by mass destruction, assassination, or kidnapping.

For terrorism in the maritime domain, the Council for Security Cooperation in the Asia Pacific has put forward the following definition: (Maritime Terrorism)

"…the undertaking of terrorist acts and activities within the maritime environment, using or against vessels or fixed platforms at sea or in port, or against any one of their passengers or personnel, against coastal facilities or settlements, including tourist resorts, port areas and port towns or cities."

However, this definition is not complete since it does not include the use of maritime transportation systems to smuggle terrorists or terrorist materials into the targeted countries. (Maritime Terrorism)

With the increased dependency of the world countries to the free transfer of goods/products using the free waterways and oceans, the definitions of terrorism given in the previous paragraphs have started to lose their validity. Of course, terrorism can fulfill its purposes by killing many people, or causing extensive damage which create a lot of publicity, fear, and news coverage. However, all of these consequences take place immediately after the event and they are not prolonged consequences. When structures that support world economies, trade and supply of goods and commodities, such as maritime ports, we see another potential motivation for terrorist attacks which aims to create long lasting consequences. Ports being an essential part of the global supply chain are such structures which can have prolonged economical and psychological consequences with a potential to become spread worldwide. These sequences cannot be immediately determined but will definitely be much worse and long duration than the attacks seen in the history. Such an effect can be seen in the air travel industry after the 9/11 attacks, people are still suffering the consequences 10 years after the event and airlines are operating with huge losses.

For terrorism in the maritime domain, government officials are considering the possibilities of the use of oil, natural gas or other hazardous cargo-laden ocean-going vessels as terrorist weapons against seaports and the communities they serve. A 2004 FBI report asserts that "Ports, because of their accessibility to both water and land, together with the chemical and natural resource storage facilities that are often located within close proximity, are inherently vulnerable." For U.S. ports such as the Port of Los Angeles/Long Beach which handle a huge amount of container traffic, one plausible scenario is the use of conventional explosives to destroy three bridges and one rail line connecting major port facilities (Masters, 2008). The total direct and indirect economic cost of such an event is estimated to reach $45 billion. Similarly, cargo containers, only 2% of which can be checked with the current technology, can be used to transport weapons of mass destruction into the United States. To mitigate this event, radiation detection equipment has been installed at many major ports all around the world.

Vessels, which are fairly fast and maneuverable on open waters, become potential targets in the tight confined spaces of seaports. Because navigating and moving a vessel in the tight confines of port facilities and inland waterways is a tough job, we see a lot of increasing attacks in the narrow waterways such as around the Gulf of Aden (Figure 5). Such events include the increased pirate activity in the Gulf of Aden. Similarly, the French oil tanker Limburg was rammed by a small boat laden with explosives in the Arabian Sea. In the 2008 Mumbai terrorist attacks, small teams of attackers infiltrated the commercial center of Mumbai using small inflatable vessels. They have sailed from Pakistan on a cargo vessel, and a hijacked Indian fishing trawler (Christopher K. , 2009). In 2000, the U.S. guided missile destroyer USS Cole was attacked while refueling in the port of Aden. Again a small boat loaded with explosives had rammed into the bow section of the destroyer leaving a huge gap and causing seventeen

casualties (Figure 4). This event is very significant because an act of global terrorism took place in a port during a routine ship refueling operation. Such events underline the importance of the management process in port security management and planning.

From a management perspective, a port facility's existence depends on two intertwined goals: (1) being responsive to the commercial needs and economic interests of the maritime industry, and (2) providing a safe and secure harbor for the transaction of the business operations for shipping and trade. However, in the light of the recent events and the above discussion, these two goals can seem conflicting. Too much security may close slowness in responding to the commercial needs, and lack of security for quick response may cause safety risks. These conflicting goals create challenges for all government, business, and security organizations in recognizing and implementing risk management and security planning processes that can simultaneously fulfill the two goals. This is partially solved by the movement toward a convergence approach to security, one where the port security managers can engage the diverse actors in the port in collaborative ways, should work to develop a framework of public policy, security regulations, and plans that are flexible enough to allow port tenants and security operations to work in tandem in developing a safe, secure, and economically completive port environment. Use of emerging technologies can provide the required additional security while keeping at the same level or increasing the responsiveness of the ports. This balanced approach is proposed by one study aimed at securing an efficient global supply chain (Willis & Ortiz, 2004) in terms of three interconnected strategies:

1. Government-driven policies strengthening the global container supply chain
2. Multi-sector efforts to improve container shipping system security

3. Research and development on new technologies for low-cost, high-volume remote sensing and scanning.

The challenging maritime security environment and the emergence of new potential threats make the decision-making roles of security managers very powerful. A decision to build a new fence, to curtail operating hours at an access point, installation of new security check points, or restriction of certain people or vehicles from entering particular areas can have powerful consequences for a business operating on a thin profit margin. A balanced strategy based on building consensus and productive working relationships with port stakeholders are crucial.

Figure 5 Photo showing the attack on USS Cole (USS Cole Bombing)

Figure 4 Somalian terrorists attacking a commercial vessel (Monstersandcritics)

To address some of the emerging terrorist threats and develop some government driven policies strengthening the security of the global shipping industry, IMO critically reviewed its

agenda concerning vessel and port facility security and proposed the International Ship and Port Facility Security (ISPS) Code in 2002.

The ISPS Code defines the minimum standards for port facility and vessel security for countries that have signed the IMO convention. It establishes an international framework for cooperation between most of the world's governments, government agencies, and the shipping, and port industries to detect security threats and implement countermeasures. Several countries made it mandatory for the ports to implement the ISPS Code. For example, the United States enacted the Maritime Transportation Security Act (MTSA) of 2002 in response to calls for enhanced security for vessels in the nation's ports. MTSA requires the U.S. seaports to conduct vulnerability assessments, which are necessary to determine the nature and type of threat or risk for each particular port facility. Based on the assessment, ports must develop Facility Security Plans (FSPs) to mitigate the threats. All of these will be discussed in detail in the Chapter 6 devoted to the ISPS Code.

However, there are a lot of challenges involved in conducting the vulnerability assessment for the implementation of the ISPS Code. Since terrorism is a result of wrongdoing by human beings, the consequences of terrorism cannot be modeled using the traditional methods that are probabilistic, deterministic, or actuarial based. This is due to both the lack of historical data, and the nature of human beings who may or may not act rationally (Rice Jr, 2003). To elaborate more on this issue, we need to compare and contrast the terrorism to the other threats to the resilience such as the natural disasters of section i.

Natural disasters are naturally occurring processes that impact people's daily living and routines. Examples of natural disasters include landslides, earthquakes, blizzards, and naturally

occurring diseases (Greenberg, Chalk, Willis, Khilko, & Ortiz, 2006). One major distinguishing feature of natural disasters is the following; human activities have little involvement in the orientation and occurrence of such events and the consequences. Terror disasters are the antithesis of the natural disasters because they are directed completely by human activity, thought and decision. Terrorists act through, and rely upon, the manipulation of various known and potentially unknown hazardous sources (explosive devices, radioactive isotopes, biological warfare) for disaster execution (Greenberg, Chalk, Willis, Khilko, & Ortiz, 2006). Terrorists are also sensitive to available resources and the political environment within which they operate, resulting in very strategic and adaptable attack plans.

A second difference that differentiates the terror disasters from other types of disasters is the level of inherent uncertainty. Natural disasters tend to be easier to study because they have occurred, continue to occur, and there is plenty of data for comparative and risk analysis. Since scientists have recorded the occurrence of natural disasters for decades, much knowledge has been acquired. For example, future hurricanes/typhoons and their effects can majorly be estimated by conducting experiments, using statistical analysis, and examining geological records. This adds an increased sense of security and lessens the extent of perceived disaster consequences.

On the other hand, terrorism uncertainties are unique in that they involve ever changing human beliefs and values foreign to other nations. Researchers' understanding of human beings and their behavior is significantly limited compared to natural disasters. The recent attacks and their consequences have almost been impossible to anticipate because the understanding of terrorist motivations, capabilities, and intent is limited. Furthermore, there is an unlimited number of uncertainties related to the planning, preparing, and execution of a terror attacks. The

vast potential and unpredictability of terrorism is more uncertain compared to that of natural disasters. This renders the data about the previous terror attacks vastly unusable for prediction and risk assessment.

The level of uncertainty in the terror disasters also makes it very difficult to assess the effectiveness of available risk reduction alternatives or to determine reasonable minimum standards for community preparedness. (Greenberg, Chalk, Willis, Khilko, & Ortiz, 2006). It is very difficult to prepare for an innumerable amount of possible attacks varying in type and severity. More importantly, the terrorists have the ability to modify their decisions adaptively, making it difficult to track a moving and adaptable adversary.

All of the above discussed reasons and distinguishing makes the traditional risk analysis approaches ineffective in capturing terrorism related risks. The main reason is the failure of the traditional risk analysis methods in capturing the resourcefulness and adaptability of the human beings. This will be discussed in detail in the risk assessment subsection which is a critical element of the resiliency planning, the topic of next section.

2.4 Critical elements of resiliency planning

Careful resiliency planning is a very important process for communities and businesses. With careful planning, the recovery process will be much easier and rapid minimizing the disruptive effects. A good resiliency planning process involves four components; preparedness, protection, response, and recovery.

2.4.1 Preparedness

In the preparedness components, emergency and continuity plans have to be developed. These efforts include the preparation of an emergency supply kit and organizing workshops or

training sessions to disseminate these emergency plans to the state and local governments and their employers. Also potential scenarios should be developed and thoroughly tested through exercises and simulations. More importantly, the governments and businesses should cooperate to acquire a full understanding of the risks and develop long-term plans to confront them. (Building a Resilient Nation, 2008)

2.4.2 Protection

Protection is not something that is only the responsibility of the federal government. The business owners should undertake this component very seriously in their day to day operations to protect their employees and assets from a variety of unexpected events and prevent long disruptions.

Modernizing the aging infrastructure and understanding and strengthening the vulnerabilities in the supply chain and port operations will prevent severe disruptions in the port activities that could result from a natural disaster, or from a terror attack. Technology can be a very useful tool in strengthening the port operations such as implementing container scanning technology, and protecting sensitive operation data from the hackers.

2.4.3 Response

In reducing the detrimental effects of natural disasters, and terrorist threats, timely response is highly essential to prevent the consequences from becoming uncontrollable. In other words, the quick response will mitigate the long-term negative effects of a disaster. In a quick response, the communication, both internal and external, is a key element. First responders must be able to communicate with each other, government authorities must communicate with the general public, as well as with businesses and other organizations in order to coordinate the activities. For example, in the aftermath of the 9/11 events, there is substantial research effort in

establishing communications in the stairwells of buildings to facilitate communications between the firefighters (Soo Yong, Zhengqing, Baker, Celik, Hyoun-sun, & Iskander, 2009).Also, the slow response to the Hurricane Katrina resulted in a calamity of epic proportions. (Building a Resilient Nation, 2008)

2.4.4 Recovery

Recovery is the return to the normal state of operations. This is deemed as the ultimate point of resilience. Following a catastrophe, a quick return to a state of normalcy is the ultimate goal of resiliency. The time passed from the event to the recovery is the performance benchmark for a resilience strategy, and this criterion is mainly used in ranking several approaches in a simulation type of study.

2.5 Risk Assessment

The definition of risk always involves a discussion of the concept of safety. "Safety" can be explained as the degree of freedom from danger and the risk is a way of evaluating this degree of freedom. Among engineers, the risk is usually defined as the product of the probability of occurrence of an undesired event (e.g. a terrorist attack) and the expected consequence of that event in terms of human, economic, and/or environmental loss. For example, an event with a high probability of occurrence and a high consequence has a high level of risk. In terms of safety, this corresponds to an unsafe system. In general, safety is determined by adding all the relevant risks for a specific system. Reducing the risk of a system, or increasing the safety involves either decreasing the consequences (response, recovery) or decreasing the probability (protection) of unwanted events. An important question that often arises in the concept of risk pertains to how people relate to and understand the concept of risk. This is often a complicated issue because some of the risks and unwanted events involve some degree of subjectivity that

results in differences between the actual and perceived risks (Kristiansen, 2005). This often necessitates improved communication with different individuals/groups to achieve a mutual understanding of complicated safety issues for reducing the discrepancies with the actual and perceived risks.

Quite often, the consequences of an unwanted event are very hard to quantify and foresee. This usually requires involvement of subject matter experts who are really familiar with the operation of the related systems (ports, ships, engines etc.). These subject matter experts use their experience to derive possible consequences, their severity, and present the risk as the probabilities of all possible consequences. These unwanted events and their possible causes can be combined in a flowchart, namely the fault tree for the determination of overall probability of an unwanted event in a system. Such a fault tree is shown in Figure 6 for deriving the probability of the release of Liquefied Natural Gas (LNG) from Boston Harbor. For deriving the risk, a similar analysis has to be conducted showing the consequences of a possible LNG release.

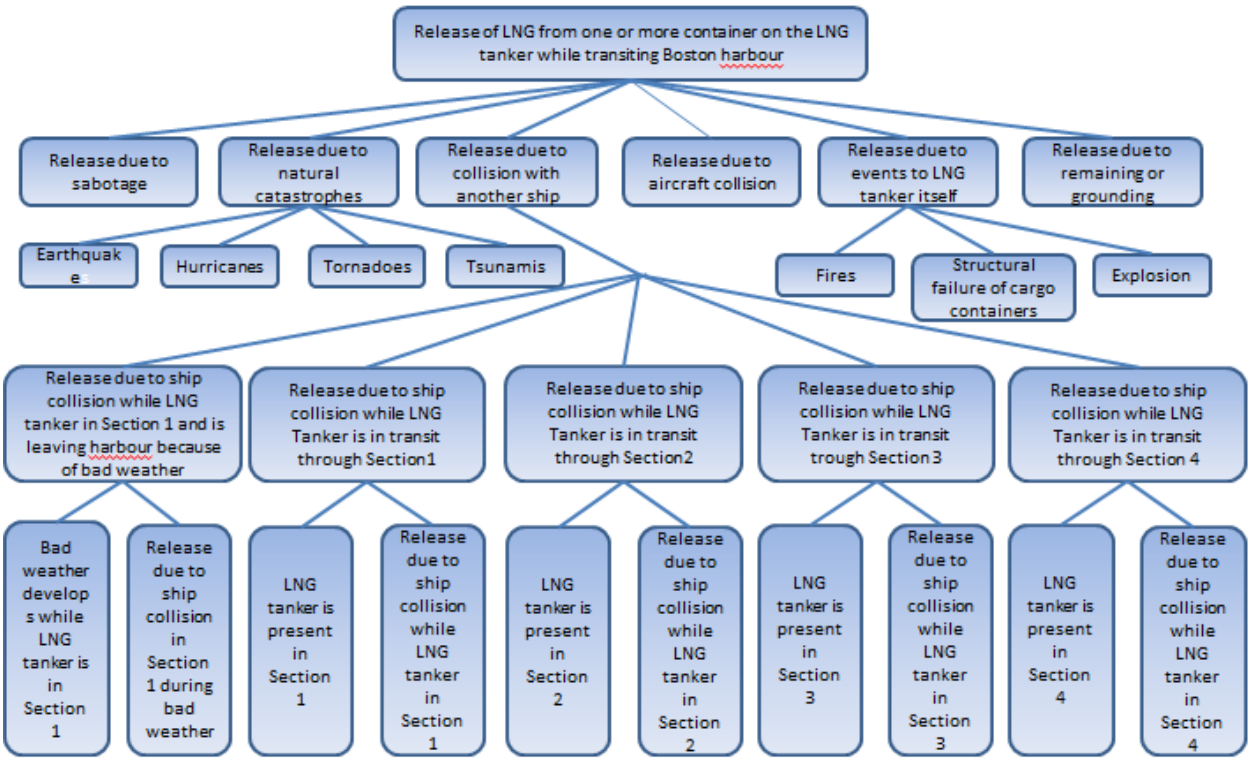


Figure 6 Top of a fault tree for estimation of the probability of LNG release in Boston harbor. (Kristiansen, 2005)

As mentioned before, the derivation of the risks of any unwanted events associated with a system is a tedious process and often requires help from the subject matter experts. In the risk analysis process, the first task is the problem definition and system description, for example the propulsion system of a tanker in determining the risks of loss of propulsion. The second step is the hazard identification exercise in which possible events and conditions that may result in the loss of propulsion. As Figure 7 indicates, this task requires the detailed knowledge and understanding of how the propulsion system operates and the interrelations of the involved components.

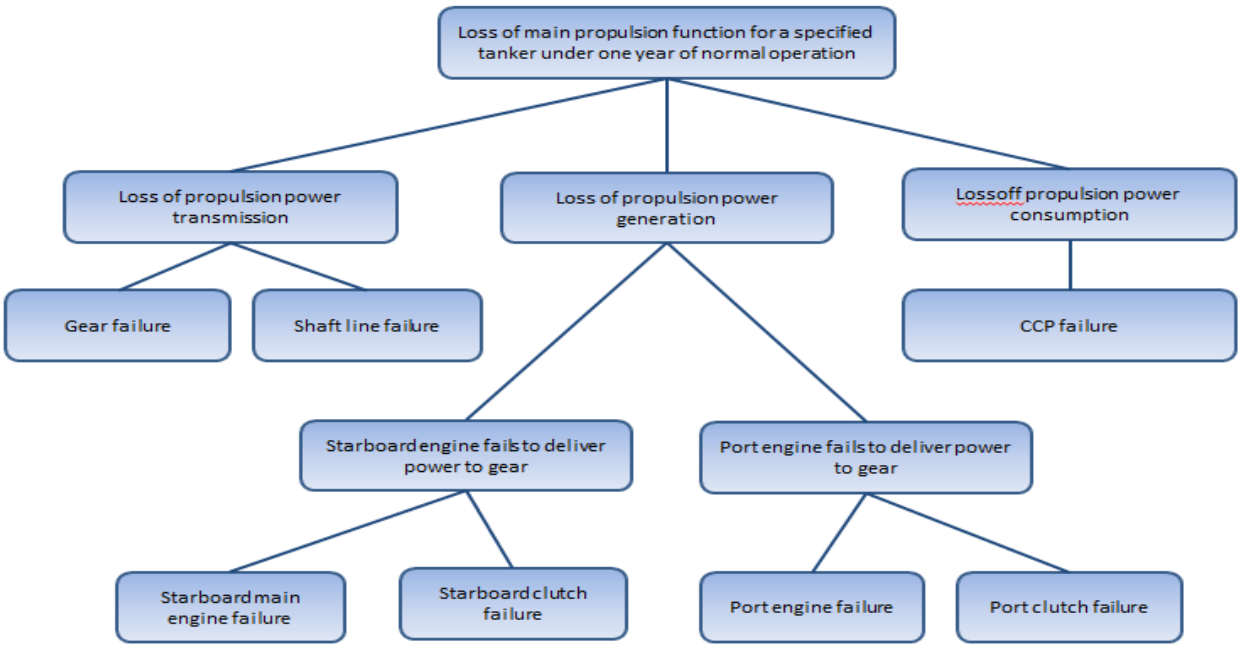


Figure 7 Fault tree for the top event of 'loss of propulsion for the tanker'. (Kristiansen, 2005)

Once all the hazards associated with an unwanted event such as the loss of propulsion for the tanker, the risk analysis can be performed which is the process of estimating the risks and consequences either qualitatively or quantitatively. The probabilities of occurrence for each accident/hazard are derived using a frequency analysis method based on the historical data. Similarly, the costs of resulting consequences/effects are evaluated through consequence modeling. In a maritime scenario, the consequences can be on the vessel, its passengers, crew, cargo, and environment. When both of these values are determined, the overall risk can be calculated. These calculated risk values can further be classified as negligible, acceptable, and intolerable.

To reduce the risk into acceptable levels, safety measures need to be developed and its effectiveness need to be estimated. An example safety system can be the construction and implementation of a marine evacuation system on board a ship. To evaluate the feasibility of such safety measures, a cost-benefit analysis is conducted to justify the costs of implementing them.

All of the processes used to derive the risk associated with a system and the necessary safety measures are summarized in Figure 8. Based on this process, conclusions may be drawn and recommendations can be proposed to the stakeholders (Kristiansen, 2005).

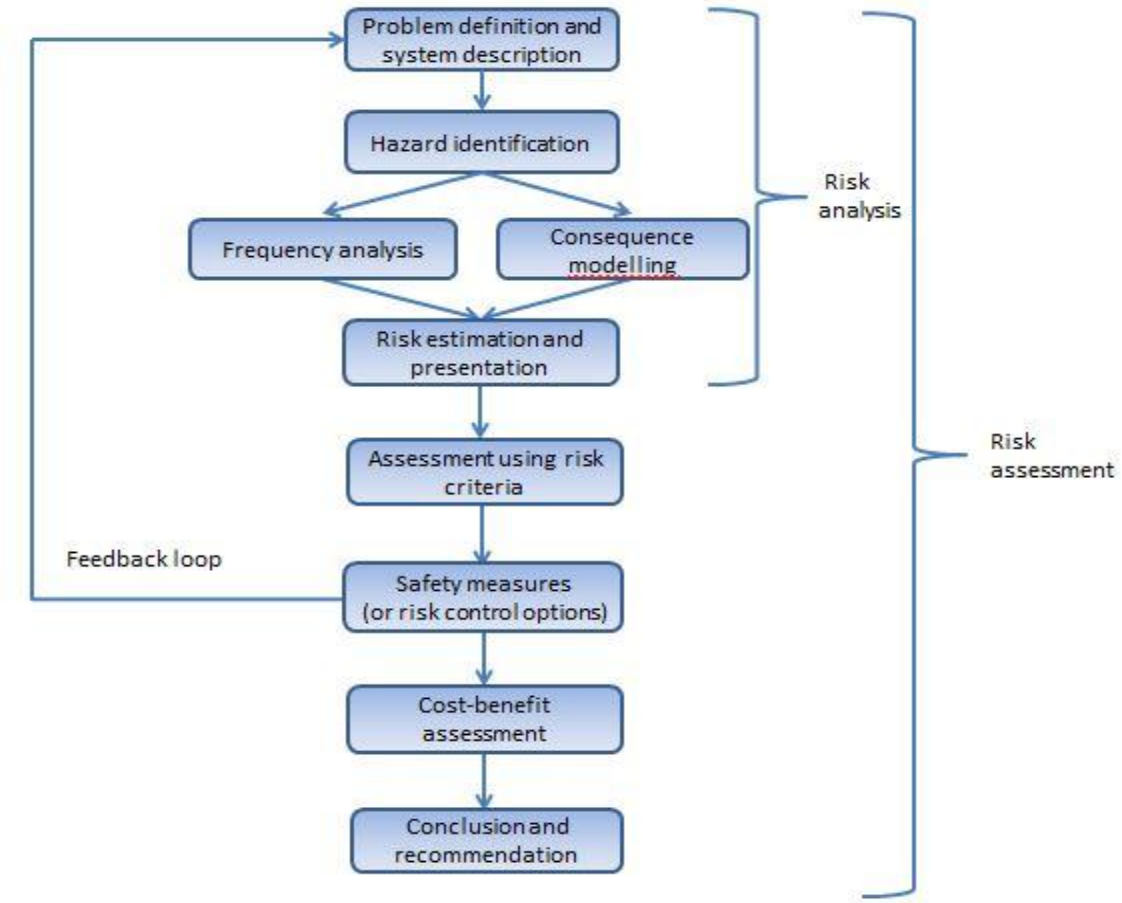


Figure 8 The process of risk analysis and risk assessment (Kristiansen, 2005)

For a successful risk analysis, several resources such as subject matter experience are needed. Substantial knowledge is also necessary in order to be able to make the right simplifying assumptions and keep the complexity of the assessment tractable. Because of the inherent complexity of the underlying structures/relations, risk analysis normally needs a combined work of several people with a wide range of different backgrounds. Therefore, team working and communication skills become highly important.

For the frequency analysis part, another important resource is the statistical data. The statistical data can provide important information about accident frequency and the most likely consequences when a certain hazard occurs. In the maritime environment, where the number of serious accidents is quite low due to relatively small ship populations, historical recordings over several decades can be used to establish a statistical basis for risk analysis. Even with a long history, the amount of available statistical data can still be insufficient. This, results in huge uncertainties in the analysis outcomes, and one should always be aware of these uncertainties and consider them in the decision making and recommendation process. Several other uncertainties can also result from the simplifying assumptions.

The traditional risk analysis approaches also involve limitations because of the lack of consideration given to the human and organizational factors. Events of last decade has proven that human and organizational factors affect the safety of technically complex systems such as conventional ships, tankers like Exxon Valdez and other types of vessels. Investigations suggest that approximately 60% of all accidents are caused directly by human errors. These factors include active failures and latent conditions that breach the security measures and create severe losses. These human and organizational factors are usually considered in the qualitative risk analyses because of their nature.

The international trade which is an essential part of world's large economies including the U.S. has become a prime target for the terrorists because of its large and long lasting possible consequences. Therefore, terrorist/safety threats have become identical to others caused by either natural hazards or human errors (Ung, 2010). The ISPS code developed by IMO in December 2002, and came into force in July 2004 aims to proactively reduce the risks of maritime trade due to several factors including the terrorist events. The previously described risk assessment procedures are recognized by the IMO and constitute an essential part of the International Ship and Port Facility Security (ISPS) Code implementation.

The ISPS code agrees that ensuring the security of ships and port facilities is basically a risk management activity. A risk assessment is needed to determine what security measures are appropriate and cost effective.

When the newly emerging threats such as terrorism are considered, however the maritime security risk assessment becomes very tedious due to the characteristically unpredictable outcomes associated with high consequences. Considering the complexity of the fault trees for relatively simple mechanical structures such as the propeller systems, one can understand the complexity of complicated and ever changing human related systems such as the terrorist organizations. In the light of this fact, a decent and novel methodology for maritime security risk assessment is important (Ung, 2010).

After this risk assessment is completed and the relations are understood, safety and resiliency strategies to reduce the probabilities of unwanted events or to minimize the consequences can be developed. This thesis discusses the role of emerging technological tools in performing these tasks and implementing the ISPS requirements. The following chapters are devoted to the review

of these emerging maritime technologies and their potential use in providing safety and resiliency.

2.6 Devise Risk Mitigation/Resiliency strategies

Table 2 Risk Control Measure Characteristics (Kristiansen, 2005)

Risk Control	Description
Passive or active	Passive risk control is where there is no action required to deliver the risk control measure, whereas active risk control is where the risk control is provided by the action of safety equipment or operators.
Independent or dependent	Independent risk control is where the risk control measure has no influence on other elements, whereas dependent risk control is where one risk control measure can influence another elements of the risk contribution trees (i.e. fault and event trees).
Human factors involved and critical	Human factors involved risk control is where human action is required to control the risk but where failure of the human action will not itself cause an accident or allow an accident sequence to progress. Human factors critical risk control is where human actions are vital to control the risk, and where failure of the human actions will directly cause an accident or allow an accident sequence to progress. Where human factor critical risk control exists, the human action (or critical task) should be clearly defined in the risk control measure.
Auditable or not auditable	Auditable or not auditable reflects whether the risk control measure can be audited or not.
Quantitative or qualitative	Quantitative or qualitative reflects whether a particular risk control measure has been based on a quantitave or qualitative assessment of risk
Established or novel	Established risk control measures apply currently existing technology and solutions, whereas novel risk control measures are where the measure is new. However, the measure may be novel to shipping but established in other industries.
Developed or non-developed	Developed or non-developed reflects whether the technology under-lying the risk control measure is developed both in its technical effectiveness and in terms of costs. Non-developed is either where the technology is not developed but it can be reasonably expected to develop, or where the costs of the measure can be expected to decline over a given period of time.

3. METHODOLOGY

First of all, as the aim of this thesis is the impact of new technological developments on the resilience strategies and how they can be utilized in the resilience planning process and appended into the ISPS code, several threats to the port resilience will be reviewed and studied. For this purpose, the vast amount of literature studying the effects of several threats including the natural and terrorist threats in the maritime domain will be reviewed and summarized to indicate the possible consequences. The consequences to be reviewed include the direct ones such as damage to the several port facilities, personnel and equipment as well as the indirect ones such as the long lasting economic impacts and loss of customers. Especially, the indirect effects are caused by the long term disruptions to the port operation and will be described in detail since they are pertinent to the motivations of the terrorist events.

Resiliency planning process will be described together with its steps such as the risk assessment through a careful review of the related literature. In doing this, also the literature dealing with the risk assessment when human factors are included will be studied and the associated difficulties will be discussed.

In the next section, the ISPS code is reviewed and evaluated by how much it addresses several natural and terrorist threats. The implementation details such as the risk evaluation and the use of event trees for various threats are described and compared against the tasks of the resiliency planning.

In another literature review effort, the emerging maritime and port technologies are going to be studied and examined in detail. For this part, publications in the engineering and maritime journals as well as leading technology companies' web sites are scanned for emerging new

technologies. Then these technologies are evaluated as to how they can contribute to the resiliency and implementation of the ISPS code. In this context, the concept of cognitive ports will be studied in which all the sensory information are combined and condensed at a central location to provide decision aids and possible automated decision making capabilities.

Finally, possible scenarios for terrorist attacks and natural disasters will be explained and several actions and decisions will be given using the information from the emerging technologies.

4. EXPECTED OUTCOMES

The literature review conducted in this thesis will identify the motivations for the terrorists to move their attacks into maritime domain and the possible significant consequences of these threats.

Similarly, the natural threats such as the earthquakes are reviewed and their consequences are derived.

The discussion on the details of the ISPS code will lay the groundwork explaining why this code is proposed and mandated. Various components and details of their implementation will shed light into these complicated processes and help port authorities responsible for implementing this code.

In the engineering domain, there are a lot of technologies under development that present significant opportunities for providing port resiliency and maritime domain security. However, the technicality of this content is hard to understand for the port authorities and this thesis will serve as a bridge conveying the outcomes of the research efforts in a language that is understandable by the maritime specialists.

At the end, examples of how these emerging technologies can help the efforts to provide port resiliency and implement the ISPS code are given and discussed. This is also a very useful outcome highlighting the ways of adopting the emerging technologies in the day-to-day port operations.

5. LIMITATIONS

Given the limited scope of the study and to increase the understandability, only the terrorist and natural threats out of all the threats to the port operation will be studied. However, the methodology proposed by this study can be applicable to many other threats with minor modifications.

Additionally, some of the technologies studied in the dissertation may not be mature enough to be deployed in actual operational scenarios and may need some more time for development and commercialization. Moreover, given the limited time and scope of the study, it is not possible to review all of the emerging technologies and to include all aspects of them, therefore, some technologies may be unintentionally left out. However, with the included guidelines, ideas about how to incorporate these newly emerging technologies in port operation can be inferred.

Finally, again due to the limited scope, the financial burden of incorporating the newly emerging technologies into port operations has not been discussed. This is mainly due to the fact that most of the emerging technologies are still in their test phases and far from being commercially deployable. However, there is enough potential and efforts to make these technologies affordable for many ports if there is interest. Another discussion point in this sense is that who will handle the financial burden of implementing these technologies at port. This question is left unanswered for the implementation of the ISPS Code and is an active research topic for policymakers.

6. REVIEW OF THE INTERNATIONAL SHIP AND PORT SECURITY CODE AND EVALUATION OF ITS EFFECTIVENESS IN PROVIDING RESILIENCY

In the wake of the terrorist attacks on World Trade Center and Limburg oil tanker, the International Maritime Organization (IMO) has developed the International Ship and Port Facility Security (ISPS) Code and appended it to its SOLAS as a response to prevent such events from happening in the maritime domain (Mazaheri, 2008).

Before the ISPS Code, the SOLAS had Chapter XI that contained some measures to increase maritime safety. In December 2002, this Chapter XI was renamed as Chapter XI-1, and a new Chapter, XI-2, was added to incorporate new measures in the aftermath of recent terrorist activities. ISPS Code has been incorporated as a supplement to this Chapter XI-2.

ISPS Code is a comprehensive set of measures to enhance the security of ships and port facilities. The rules of Chapter XI-2 only applies to passenger ships and cargo vessels of 500 gross tonnages and higher, including high speed craft, mobile offshore drilling units and port facilities which serve such ships on international voyages. As mentioned by IMO, the general objectives of the ISPS code are as follows (Mazaheri, 2008):

- For instituting an international framework, establish cooperation between contracting governments, government agencies, local administrations and the shipping and port industries to detect and assess security threats and take preventive measures against security incidents affecting ships or port facilities used in international trade.
- To define the respective roles and responsibilities of all these parties concerned, at the national and international level, for ensuring maritime security.

- To ensure the early and efficient collection and exchange of security related information.
- To provide a methodology for security assessment so as to have in place plans and procedures to react to changing security levels.
- To make sure that adequate and proportionate maritime security measures are in place.

The ISPS Code consists of two parts, Part A and Part B, the former is compulsory and the latter serves just as a guideline for implementing the requirements of Part A (Mazaheri, 2008). However, it is recognized that extent of the guidance strongly depends on the nature of the port facility and of the ship, its trade and cargo. On the other hand, USA has made it mandatory to comply with the rules of Part B for all US flag ships and all foreign ships visiting the US. The attempts of US to make Part B compulsory by incorporating it to the ISCC2 template has not been accepted (Mazaheri, 2008). The European Union Parliament has made some sections of Part B mandatory for their member states by its new regulation (Mazaheri, 2008). In addition, the definition for port area that must be protected has been changed by the EU directive. With this new directive, properties and infrastructures like oil tanks or power plants which are located in the port area are also included in the protected area definition as well (Mazaheri, 2008).

In summary, the Code can be seen as a risk management activity to ensure the security of ships and port facilities. This activity is the assessment of what security measures are appropriate for the risks determined for each particular case. From this aspect, the Code provides a standardized framework for evaluating risk, enabling governments to offset changes in threat with changes in vulnerability for ships and port facilities through determination of appropriate

security levels and corresponding security measures (IMO). These assessment needs and activities will be discussed in detail after a brief overview of the ISPS code.

The implementation of the ISPS Code and additional security measures results in increased annual costs, and administration and manning needs (Mazaheri, 2008).

6.1 ISPS Code: A Brief Overview

As mentioned in the previous paragraphs, the ISPS Code consists of two main parts. I will briefly describe the contents and purpose of each part in the following subsections.

6.1.1 ISPS Code Part A

In Part A, there are 19 sections and 2 appendixes. In a nutshell, definitions, applications, and responsibilities of the parties in charge, and technical information about the requirements of the Code are described in the Part A. Specifically, Part A defines:

- The obligations of the company, ship, port facility, and of the contracting government
- The mandatory requirements of the risk assessments and security plans.
- Data recording and keeping requirements.
- The training and exercise information of the crew and staff.
- The certification and the verification requirements for vessels.

In the appendices, there are two sample forms for the International Ship Security Certificate (ISSC) and Interim-ISSC to serve as an example for the issuing requirements of these certificates.

6.1.2 ISPS Code Part B

Similar to Part A, in this part there are 19 sections and 2 appendices as well. Part B mainly includes more details and guidelines needed to implement part A's requirements. If Part B is considered in the implementation of Part A by all parties, the main weakness of the Code, which is the different interpretations, can be overcome. In the appendices, the Declaration of Security (DOS) form and Statement of Compliance (SOC) form for port facility are included as samples.

6.2 Risk and Security Assessment Needs as Defined in the ISPS Code

The first step in the implementation of the ISPS Code is the risk and security assessment. In the risk and security assessment, weaknesses of the infrastructures, physical structures, databases, information systems, communication systems, personnel protection systems, processes or other areas that can lead to security breaches are identified. This step also involves the determination of the options to eliminate or mitigate the risks and their consequences. When the resiliency planning process and its steps are considered, a resemblance to the risk and security assessment requirements of the ISPS Code is observed. In other words, the ISPS Code itself indeed addresses some of the resiliency concerns for the ports which become obvious after the terrorist attacks and recent natural disasters.

In the Code, these risk and security assessments are defined separately for ships (Ship Security Assessment, SSA) and port facilities (Port Facility Security Assessment, PFSA). After implementing the SSA and PFSA, the Ship Security Plan (SSP) and Port Facility Security Plan (PFSP) shall be prepared accordingly. In other words, the risk and security assessments are an essential and integral part of the process of developing and updating security plans. For each security plan, a security officer is assigned to be in charge of the implementation (Mazaheri, 2008).

6.2.1 Ship Security Assessment (SSA)

The SSA aims at determining the vulnerable parts in ship structure or operation. Part A of the ISPS code requires an on-scene security survey. This survey should include the people, activities, services and operations that require protection. Similarly, all probable threats and vulnerabilities during the berthing, anchoring, or seagoing should be included. The SSA needs to be reviewed periodically since it is an essential part of the ship security plan.

For all the ships belonging to a company, the Company Security Officer is the responsible person for the preparation of the SSA for each ship as shown in Figure 9. After SSA is completed, an Interim-ISSC can be issued. Alternatively, the shipping company can assign a Recognized Security Organization (RSO) as a proxy responsible for the preparation of the SSA.

6.2.2 Ship Security Plan (SSP)

After the completion of the SSA, the Ship Security Plan (SSP) is prepared. An SSP outlines all the measures to protect the ship, people on board, and cargo from the risks of all possible security incidents. In these preparation efforts, all possible scenarios should be considered together with the proper actions. Similar to SSA, the SSP requires periodic updates and reviews. After SSP is prepared and approved, the International Ship Security Certificate (ISSC) can be issued.

The Ship Security Officer (SSO) is the person responsible for the implementation and maintenance of the SSP on board. The SSO works with the CSO, and the PFSO to consults with the implementation and modification of the SSP. The master of the ship can be selected as the SSO with the permission of the ship administrator. Figure 9 illustrates the components and relations of the ship security as defined by the ISPS code.

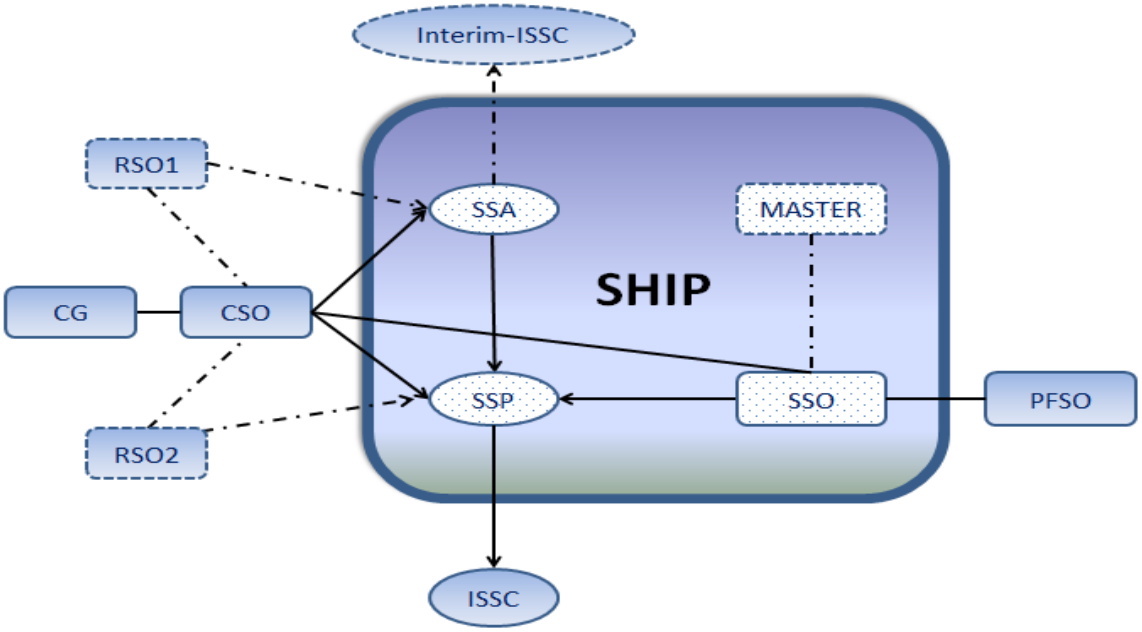


Figure 9 Ship Security diagram according to the ISPS code (Mazaheri, 2008)

6.2.3 Port Facility Security Assessment (PFSA)

In PFSA, all operational components and aspects of a port facility are evaluated in order to determine the vulnerabilities for possible terrorist attacks. In doing this, all possible threats should be included. The vulnerability of each target and the severity of the possible consequences shall be considered as well. This assessment, at minimum, should include the following elements:

- Identification and evaluation of important assets and infrastructures for protection.
- Identification of possible threats to the assets and infrastructures and the likelihood of their occurrence along with their consequences, in order to establish and prioritize security measures.
- Identification, selection, and prioritization of counter measures and procedural changes and their level of effectiveness in reducing vulnerability.

- Identification of weaknesses, including human factors in the infrastructures, policies and procedures.

For implementation of the PFSA, the contracting government has the responsibility for the port facilities that are located within its territory. The PFSA should be reviewed and updated periodically; specifically when major changes to the port facility are made. After the PFSA is completed, the PFSP shall be prepared accordingly.

6.2.4 Port Facility Security Plan (PFSP)

The PFSP is a plan to ensure the application of measures designed in PFSA. Namely, the PFSP ensures that the port facility, ships, persons, cargo, cargo transport units, and ship's stores within the port facility are protected from the risks of a security incident. A Port Facility Security Officer (PFSO) is assigned the responsibility for development, implementation, revision and maintenance of the PFSP. The contracting government has the authority to approve the PFSP.

6.3 Security Levels Defined in the Code

The ISPS code defines three security levels for ships and port facilities; Level 1, Level 2, and Level 3. Security Level 1 means; minimum appropriate protective security measures shall be maintained at all times. Security Level 2 means; appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a security incident. Security Level 3 means; further specific protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target.

The contracting government has the responsibility to set the appropriate security level for port facility and also for the ships at all times. For a ship to berth near a port facility, the ship has

to have the same level of security as the port facility. In other words, if one of them has a lower security level than the other party, the party who has the lower level has to increase its security level. The security level of the ship is reported to the port facility by the DOS form before entering the port territory (Mazaheri, 2008).

6.4 Impact of the ISPS Code on Port Activities

Compliance with the requirements of the ISPS code incurs additional costs at ports such as the ones associated with the risk assessment, training and physical improvements. Similarly, shippers have to make changes to their operating procedures such as how they document the cargo, transmit it, and how they interface with ships at port (Babins, 2006).

On the other hand, the additional security that comes with the implementation of ISPS code has direct measurable and indirect impacts upon the port community. Physical security measures such as fencing, lighting and video monitoring have the effect of controlling access/movement within the port areas allowing better management of people and activities. In addition to serving as a deterrent to terrorism, these port area improvements curb looting and prevent unauthorized access to restricted areas. Additionally, through the identification of risks and the countermeasures as well as the technological improvements, the local port capacity is significantly improved (Babins, 2006).

To summarize, the implementation of the ISPS code, in spite of being costly, has proven to be successful in the Caribbean region and it has even been shown to improve local port productivity (Babins, 2006). Than the question that remains unanswered is who to charge these costs of implementation since shippers are sensitive to the increased security fees. Currently, some ports chose to not charge additional fees whereas some ports have increased their fees

without separately indicating any implementation costs. The additional costs of ISPS implementation and how they are going to be compensated is beyond the scope of this thesis, therefore, not discussed in detail. Instead, we will examine the direct and indirect impacts of the ISPS code implementation on the day to day activities of the ports will be discussed in detail in the following subsections.

6.4.1 Direct Impacts on Activities

In order to determine the direct impact of the ISPS code on the port activities, it will be good to consider the worst case scenario, namely the security level 3. The security level 3 corresponds to a possibility of an imminent attack and requires 100% of the cargos to be checked. Compared to security levels 1 and 2 in which 5% and 20% of the cargo has to be checked respectively, the implementation of security level 3 is expected to be very time consuming. To avoid these time consuming and costly security checks, some ports can even consider stopping the operations (Mazaheri, 2008).

Because all these scanning operations are conducted after the cargo unloading for incoming vessels (or cargo loading for outgoing vessels), the additional security measures of the ISPS do not effectively change the serving time for ships. According to a survey conducted by Mazaheri, 96% of the responding port employees indicated that there is no significant change in the serving time with the implementation of the ISPS code. Therefore, we can conclude that the implementation of the ISPS code can bring additional security without any effect on the ship service times. Additionally, because of the increased monitoring of the port access, the effectiveness of the operations such as cranes, lift trucks can significantly increase.

Because, Part B of the ISPS code is only mandatory for the U.S. and E.U., there are no immediate results indicating the implementation of Part B has any impact on the port operations.

6.4.2 Indirect Impacts on Activities

To determine the indirect impacts of the ISPS implementation on the port operations, Mazaheri conducted a survey asking questions about the essential elements of the supply chain such as lead-time, service price, effectiveness, service level etc. The results of this survey are shown in Figure 10. According to this study, 80% of the respondents believe that the security level has increased with the implementation of the ISPS code. The administrative factors such as the documentation, costs, and checking process have increased in their levels as well. However, the performance measures such as the lead time, effectiveness, service level, and damages have not been affected significantly by the ISPS code confirming the results indicated in the previous section. This survey was inconclusive in terms of the effects on profit, manning, customer satisfaction, service price, and competitiveness.

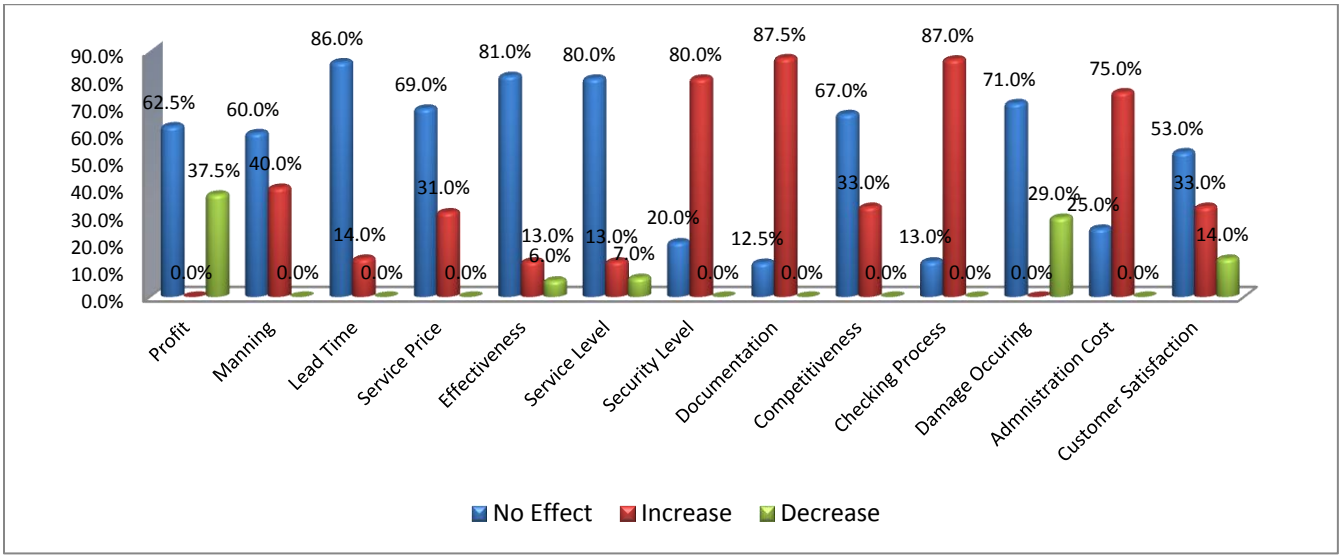


Figure 10 Indirect effects of the ISPS implementation on the port operations. (Mazaheri, 2008)

Although, the implementation of the ISPS code translates into more paperwork, higher costs, and additional administrative tasks, 91% of the respondents were satisfied with the implementation of the ISPS code because of its security advantages (Mazaheri, 2008).

7. VULNERABILITIES OF PORTS TO TERRORIST AND NATURAL THREATS AND THEIR CONSEQUENCES

Before proceeding with the implementation of the ISPS Code, how emerging technologies can help with this implementation and address the resiliency needs for natural and terrorist threats, a review of the vulnerabilities of ports and possible consequences of such natural and terrorist threats is necessary.

7.1 Vulnerabilities of Maritime Targets and Ports to Terrorist Threats

Global shipping largely takes place on unpoliced high seas, and many governments lack the resources and the willingness to implement coastal surveillance programs. A subject of increased international concern is the dependence of the maritime traffic to narrow and congested maritime choke points, where, owing to forced restrictions on speed and maneuverability, vessels remain high vulnerable to attacks. This vulnerability is amplified by the recent company policies such as "skeleton" crews, significant reduction of the number of crew members as a cost cutting measure. With the reduced number of staffing, gaining the control of a ship becomes much easier.

From the terrorists' point of view, extending the operational mandates to the maritime environment can be seen as a means for overcoming the extant security measures on land. The security measures on land, customs, and immigration have increased significantly after September 2001, while the overall level of action on the world's oceans and coastal waters has remained limited. With the thrust of several homeland security initiatives, many countries (Philippines, Indonesia, Turkey, Eritrea, and Kenya) have tried to implement coastal surveillance systems while stretching the already limited resources for offshore surveillance. This limited the

amount of countermeasures for the offshore terrorist operations and created a void. This void in offshore monitoring provides the extremists the opportunity to move, hide, and strike in a manner not possible in a terrestrial theater (Herbert-Burns, 2005).

Another source of attractiveness stems from the potential of maritime attacks in causing mass economic destabilization. Today, roughly 80% of global freight moves by sea, much of which takes the form of cargo that is transshipped on the basis of a "just enough, just in time" inventory. Disrupting the mechanics of this highly intensive and efficient trading system, has the potential to trigger large and cascading financial consequences particularly if the operations of a major commercial port are severely inhibited. Michael Richardson states this fact as follows (Richardson, 2004); "The global economy is built on integrated supply chains that feed components and other materials to users just before they are required and just in the right amounts. That way, inventory costs are kept low. If the supply chains are disrupted, it will have repercussions around the world, profoundly affecting business confidence." To further support this idea of cascading effects, the case of suicide attack against the M/V Limburg in October 2002 can be examined. Although this incident resulted in only three deaths including the two bombers, it directly contributed to a short-term collapse of international shipping business in the Gulf of Aden and nearby waters, led to a $0.48/barrel hike in the price of Brent crude oil, and as a result of the tripling of war-risk premiums levied on ships calling at the Aden. In the overall, this event caused the Yemeni economy to lose an estimated $3.8 million a month in port revenues. (Herbert-Burns, 2005) (Richardson, 2004)

The significant disruptive economic dimension of maritime terrorism has been recognized by several terrorist organizations such as al Qaeda. Attacks on maritime facilities serves the interests of these groups since Osama bin Laden has emphasized that attacking key pillars of the Western

commercial and trading system is integral to his self-defined war on the United States and its major allies. There is evidence of many repeated statements urging young Muslims to wage their jihad against Washington by focusing on targets that are liable to have a disruptive economic effect, including shipping (Campell & Gunaratna, 2003) (Greenberg, Chalk, Willis, Khilko, & Ortiz, 2006). This is further exemplified by the al Qaeda communique that was issued after the bombing of the M/V Limburg; "By exploding the oil tanker in Yemen, the holy warriors hit the umbilical cord and lifeline of the crusader community, reminding the enemy of the heavy cost of blood and the gravity of the losses they will pay as a price for their continued aggression on our community and looting of our wealth." (Herbert-Burns, 2005)

In addition to the significant cascading economic consequences, the maritime security experts also claim that sea-based terrorism can also be used for inflicting "mass coercive punishment" or triggering a major environmental disaster. The mass coercive punishment, which is outside the scope of this study, can be inflicted by attacking cruise ships and passenger ferries. These type of vessels cater to a large number of people, and in the case of a luxury liner, such an attack represents a high-prestige, symbolic attack. With today's communication technology, these types of attacks will provide the necessary exposure and publicity serving the major purpose of terrorist attacks. In regards to creating potential environmental disasters, which pertain more to the scope of this thesis, government officials and environmental groups agree that maritime attacks can cause extensive ecological damage and, quite possibly, instability. This can be better understood when the BP oil well crisis of last year is considered. Because heavy crude oil will not be easy to clean, a major spill from an oil tanker is liable to devastate the marine environment in the immediate vicinity of the spill. If not accounted for, such a spill can degrade elongated stretches of fertile coastline (Richardson, 2004). Such an effect can have

significant consequences such as socioeconomic unrest and political instability in coastal resource dependent developing states in Africa and Asia.

Real world examples of some of the terrorist attacks modalities described above have yet to be seen but given the fact that international terrorists have started exhibiting greater tactical sophistication and innovation than in the past, these types of attacks are highly probable. Considering the number of terrorist attacks that utilize the maritime domain since 2001, we can comfortably agree that many militant agendas include specific experimentation with seaborne modalities.

On the other hand, decreasing the attractiveness of the maritime domain to the terrorist attacks is the limited resources for terrorist in this relatively new domain of operations. Most of the terrorist groups and individuals lack the certain skills and knowledge to operate in the maritime domain with the complicated vessels, dive equipment, etc. For the compensation of these deficiencies, there are two broad issues being raised. First, the growth of offshore industries combined with the general popularity of maritime sports help the terrorist groups gain basic skills and equipment for seaborne attacks. Second option for the terrorist group is contracting out to pirate syndicates to compensate for their existing shortcomings in the seaborne attack capabilities. Highly popular scenario in this regard is the possible employment of maritime crime groups to hijack and deliver major ocean-going vessels such as oil tankers, or LNG carriers, which might then be sank to block critical sea-lanes or detonated to cause a major explosion at a target port of opportunity. Such a critical sea-lane is the Malacca Strait, and Lloyd's Joint War Council has designated this lane as an "Area of Enhanced Risk".

After establishing the fact that maritime domain is an attractive and coercive modality for the global terrorism to inflict long-lasting economic and environmental impact, let us turn our attention to some possible scenarios for maritime terrorist activity in the future and how we can estimate the consequences of such attacks. This examination will help us identify the security needs and required safety precautions to reduce the degree of possible impacts or prevent such events.

According to intelligence analysts and security experts, there are at least seven possibilities for terrorists to carry out significant attacks (Greenberg, Chalk, Willis, Khilko, & Ortiz, 2006): (1) Use of a commercial container ship to smuggle chemical, biological, or radiological (CBR) materials for an unconventional attach carried out on land or at a major commercial port such as Rotterdam, Singapore, Hong Kong, Dubai, New York, or Los Angeles, (2) use of a Trojan horse, such as a fishing trawler, resupply ship, tug, or similar innocuous-looking vessel, to transport weapons and other battle-related materiel, (3) hijacking of a vessel as a fund-raising exercise to support a campaign of political violence directed toward ethnic, ideological, religious, or separatist designs, (4) scuttling of a ship in a narrow channel in order to block or disrupt maritime traffic, (5) hijacking of an LNG carrier that is then detonated as a floating bomb or used as a collision weapon, (6) use of a small, high-speed boat to attack an oil tanker or offshore energy platform to affect international petroleum prices or cause major pollution, (7) directly targeting a cruise liner or passenger ferry to cause mass casualties by contaminating the ship's food supply, detonating an on-board or submersible improvised explosive device, or ramming the vessel with a fast-approach, small, attack craft. From these seven, at least 4 of them can target a port area or cause extensive disruptions in the port operations or can stem from the lack

of security measures in the port environment. From these seven scenarios, use of containers to smuggle or transport weapons of mass destruction needs more elaboration.

The container supply chain is ubiquitous, and container ships carry goods and commodities from hundreds of companies and individuals. These containers are often transported and received from inland warehouses. Every shipment involves many actors: the exporter, the importer, the freight forwarder, a customs broker, excise inspectors, truckers, railroad workers, dock workers, and the crews of feeder and ocean vessels (Willis & Ortiz, 2004). The involvement of many factors and individuals in the container shipping business creates many opportunities for terrorist infiltration. Whenever and wherever a container is handled during movement represents a potential vulnerability for the security and integrity of the cargo. Terrorists may exploit vulnerabilities to load/unload a container with a weapon or tamper with its contents. A highly possible scenario that is widely studied (Gordon, Moore, Richardson, & Pan, 2005) is the use of containers to smuggle a radiological dispersion device, a "dirty bomb". If such a device is detonated at a U.S. Port, it will contaminate a large area and may require the closure of significant parts of a large port for weeks or months, if not years. The attacks using the container shipping to sink a vessel has little to gain and very little chance of success, therefore, they mainly target the disruption of the global supply chain. However, if a bomb can scuttle a vessel in a narrow strait, choke points of the global trade, then there is a chance of inflicting huge damage by inhibiting the global trade. However, there are a few non-substitutable choke points such as the straits of Turkey connecting Black Sea to Mediterranean and the strait of Gibraltar.

To prevent tampering with the contents of shipping containers, seals and locking mechanisms can be used. Most of these mechanisms currently in use are very cheap and offer very little protection. The use of more secure and tamper resistant seals may cost up to several dollars each.

GPS transponders with Radio Frequency Identification Devices can be used to transmit data regarding the integrity of the container but these devices can cost up to hundred dollars and are not cost effective. As of now, there is no mandatory rule regarding the use of such devices.

Given the multiple modalities for a maritime terrorist attack can take place and the involvement of human factors to provide adaptability, it is a very tough task to estimate the consequences of such attacks. In this arduous task, the past maritime terrorist events provide the most direct means of estimating the consequences of future attacks. However, the number of such attacks is very low and cannot constitute a representative sample. Moreover, because of the adaptability involved, it is not possible to use the historical data for direct extrapolation to future events. These necessitate additional approaches to augment direct historical analysis. For injury and fatality analysis, the historical data of the terrorist attacks in non-maritime arenas can provide a measure. Modeling and simulation of the port/vessel operations can provide estimates of direct and indirect impacts of terrorism. Direct economic effects can often be easily estimated through modeling and simulation. Methods such as day-after games and scenario analysis can be used to elicit expert estimates of consequences and how firms and individuals will respond to terrorist events. For attacks that can cause infrastructure disruptions, historical data from non-terrorist related events can be used. Natural disasters like the Northridge Earthquake, Hurricane Andrew, and Hurricane Katrina provide case studies for large-scale regional disruption.

From these studies, the possible consequences of a maritime terrorist attack are classified and tabulated in Table 3.

Table 3 The Scope of Consequences of a Maritime Terrorist Attack (Greenberg, Chalk, Willis, Khilko, & Ortiz, 2006)

Affected Party	Human Consequences	Economic Consequences	Intangible Consequences
Individuals	Fatalities Injuries	Loss of salary Loss of property Loss of investments Loss of public services	Psychological consequences leading to changes in saving, earning and consumption preferences
Private sector		Destruction of property Ships Facilities Transportation infrastructure Products and raw materials Loss of data Life and injury compensation Short-term disruption of business cycle Immediate lag in delivery Loss of customers Loss of revenue business interruption Increased transport costs Internal diseconomies of scale Long-term transportation inefficiency Augmented security measures Increased insurance rates	Loss of human capital in the private sector Changes in consumption and investment preferences Reduces tolerance of risky investments Loss of future revenue streams Decreased foreign confidence Decreased foreign trade because of insecurity Shifts in stock market Decrease in tourism and resulting losses in revenue
Public Sector		Loss of revenue for government Destruction of public infrastructure Financing costs of response and recovery Increased government spending on counterterrorism	Political consequences Loss of human capital in the public sector

7.2 Vulnerabilities of Maritime Targets and Ports to Natural Threats

Similar to the previous sections, only the earthquakes will be discussed in this section to limit the scope of this study.

Earthquakes and the subsequent tsunamis create substantial damage to ports and surrounding supporting structures. These events can damage the port infrastructure, buildings, and cranes, also can create power outages requiring very high repair costs.

In addition to the repair costs of the infrastructures, another significant damage is the disruption of port operations. In several cases in the history, the port tenants left the port after a natural event and moved elsewhere creating irreparable damages. For example, Port of New

Orleans officials said that because they are unsure if departed tenants at the port will return, they have been reluctant to replace three severely damaged container cranes.

Damage to port infrastructure also include damages to their utility systems, including water, sewer and power. In the case of a power outage, port operations can become limited to daylight hours.

Some of the damages to the ports after an earthquake can be alleviated if the loading/unloading ships can be moved out of the port area before the tsunami strikes. Because the ships in the port area can become projectiles and cause extensive damage in the case of a tsunami. Therefore, early warning systems and port policies in place can contribute significantly to the port resiliency.

Similarly, emergency supplies in terms of power and water can minimize the disruption of the port operations and can keep the tenants in place preventing the long term damages.

8. REVIEW OF THE EMERGING TECHNOLOGIES IN MARITIME AND THEIR POTENTIAL USE IN THE IMPLEMENTATION OF ISPS CODE

8.1 Use of Technology in Increasing Port Resiliency and Implementation of the ISPS

In today's turbulent environment with various terrorist and natural threats, early detection of hazards and timely sharing of accurate information have the utmost importance for avoiding the costly consequences or at least ameliorating them.

For early detection of hazards, emerging technologies such as advanced High Frequency (HF) Radars, Passive Radar Systems, Automated Radar Target Recognition, Satellite Based Detection and Communication Systems, Active/Passive Acoustic Detection Systems, Automated Identification System (AIS), Port Security and Scanning Systems, and various container monitoring and tracking systems can be very useful. Fusion of these systems to provide Maritime Domain Awareness (MDA) in large geographical scales is a very popular topic (Wilkens, Gemelas, & Bruno, 2011).

When the amount of data collected from various information sources described above is considered, the problems associated with the organization of this huge amount of information to make sensible decisions can be recognized. This information and intelligence must be processed, fused, and interpreted, often in real-time, before disseminating effective assessments, actionable intelligence, and relevant knowledge to appropriate stakeholders in usable formats. The concept of "cognitive ports" has been proposed that learns and implements the rules and policies for information sharing, processing, and automated decision making (Mostashari, Nilchiani, Omer, Andalibi, & Heydari, 2011). Similar to the ISPS implementations, these cognitive mechanisms

have to be periodically examined and updated in the light of newly acquired information and intelligence.

In the following subsections, some of these emerging technologies and port operation modalities will be described in detail and their possible adoption in the implementation of ISPS Code and in the efforts to increase port resiliency will be discussed.

8.1.1 High Frequency (HF) Radars for Over the Horizon Vessel Monitoring

Radar, radio detection and ranging, is based on transmitting radio waves and collecting the echoes from various objects in the radar range. By measuring the delay and frequency offsets of the waves bounced off of various objects, information about the position and speeds of the objects can be obtained. Similarly, the radar return signals from the ocean in the HF frequency band contain important information about the surface currents which can be used for search and rescue operations (Corredor, et al., 2011) and tracking the movement and breaking of the ice shelves in the Arctic Region (Eicken, et al., 2011).

Unfortunately, the radio waves tend to travel in straight lines and this fact generally limits the detection range of radar systems to objects within the horizon. Because of the curvature of the earth, a radar with a height of 10m can detect objects up to 13 km of range. For this reason, airborne and satellite based radars have provided unprecedented ranges compared to terrestrial radar systems. (Wikipedia HF Radar Article, 2011)

High Frequency (HF) radar systems operating in the 3-30 MHz frequency range, overcome this range limitation due to curvature of the earth in two ways. These systems also called Over The Horizon (OTH) systems can either utilize the atmospheric reflections to reflect the targets beyond the horizon, or adopt ocean surface waves that utilize the high conductivity of the salty

sea water to create a virtual waveguide for electromagnetic waves to reach beyond the horizon. With such systems, incoming friendly/unfriendly vessels can be detected and tracked for over a few hundred nautical miles increasing the early detection capability of several threats.

Although the HF radar systems present many advantages such as the OTH detection and tracking capability, there are several challenges to overcome for worldwide deployment of such

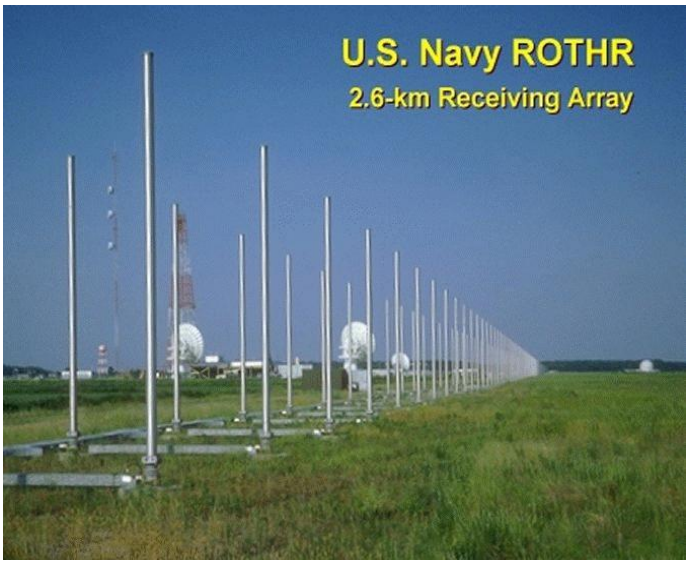


Figure 11 US Navy Over-the-Horizon Radar station (Milcom Monitoring Post)

technologies. The first and most obvious challenge can be seen by examining Figure 11 which depicts a typical HF radar installation. Because the unique frequency range of 3-30 MHz that allow OTH capability, the transmit/receive antennas of the radar systems tend to be large (Comparable to the 10-100m wavelength of the electromagnetic waves in this band). Arrays of multiple antennas need to be used with large separation distances to achieve high azimuth resolution considering the very long detection ranges of these radars. These requirements such as the deployment of very large antenna arrays (several km long) including the support structures and ground preparation render the deployment of HF radar systems very expensive (Because of the large coastal real estate requirements) and time consuming behavior (building the long

structures). Because of the associated costs and preparation requirements, portability or HF radar installations for small ports are infeasible and these installations have been limited to military applications so far.

On the other hand, several research groups are working on making the very promising HF radar technology portable and affordable by conducting research on small antennas operating in the HF band, deploying these radars on steep terrains instead of the flat coastal areas, and even installing these radar systems on floating platforms (Iskander, Yun, Celik, Youn, Omaki, & Baker, 2011). A prototype small antenna and its possible deployment scenario on floating platforms are illustrated on Figure 12 and Figure 13 respectively.

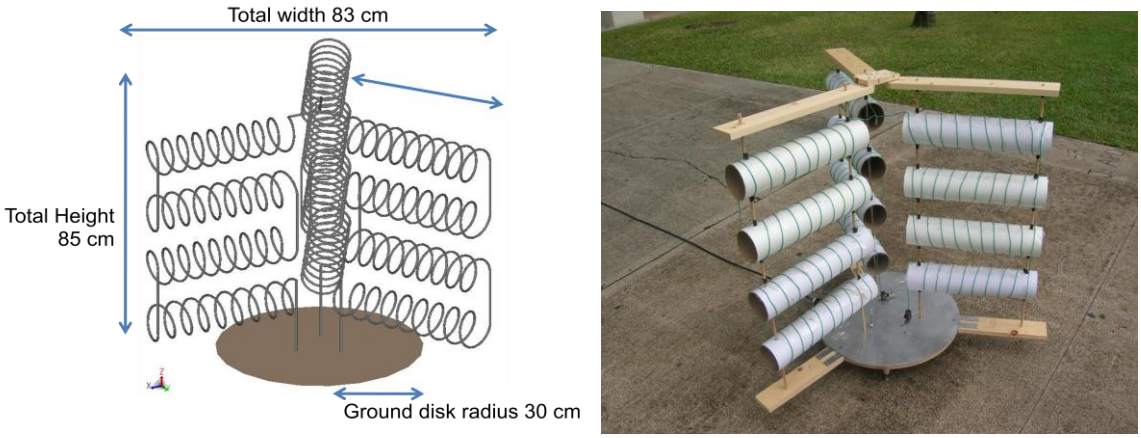


Figure 12 The compact HF Antenna (Iskander, Yun, Celik, Youn, Omaki, & Baker, 2011)

Once the technological bottlenecks that prohibit the wide deployment of HF radars for civilian and port operations can be overcome, this promising technology can be used to detect and track ships at a large distance as well as looking at the wave heights to detect tsunamis and can be augmented with the other information sources to create a resilient port environment.

The challenges to overcome include, addressing the challenging electromagnetic propagation environment modeling, accounting for the platform motion effects in target detection, providing higher resolution in terms of azimuth and range.

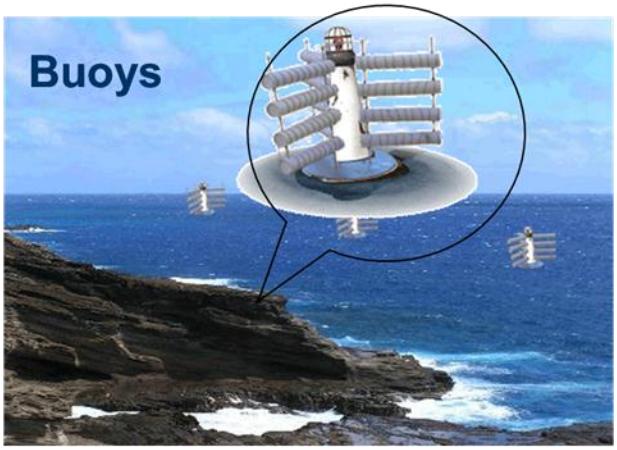


Figure 13 Possible deployment scenario of HF radars on floating platforms (Iskander, Yun, Celik, Youn, Omaki, & Baker, 2011)

8.1.2 Passive Radar Systems

HF Radar systems are very good in providing detection capabilities in the long range, but they have limited resolution and are active systems. Being active, in other words transmitting the radar signal, serves as a beacon for the adversaries to be aware of the existence and location of such radar systems and take the necessary precautions. To avoid this problem and use the crowded band of spectrum for radar operations, the passive radar concept is proposed (Wikipedia Passive Radar Article). The passive radar system operates covertly by using the existing radio signals in the environment such as the TV and radio stations, therefore, becomes invisible to adversaries.

As seen in Figure 14, passive radars operation involves the use of at least three broadcast stations for accurate triangulation of the target position using the direct and reflected paths. In this effort, higher broadcast bandwidths lead to increased detection accuracy. Along these lines, digital

terrestrial broadcast systems with their high bandwidths allow range accuracies in terms of a few meters (Iskander, Yun, Celik, Youn, Omaki, & Baker, 2011).

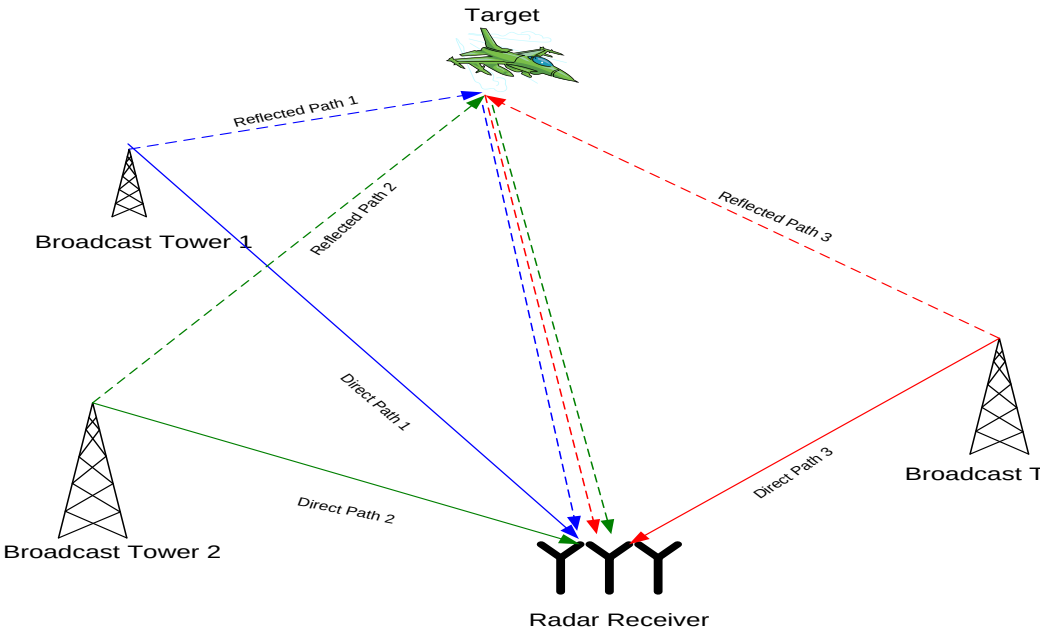


Figure 14 The passive radar operation (Iskander, Yun, Celik, Youn, Omaki, & Baker, 2011)

8.1.3 Satellite Based Detection Systems

Satellites, because of their very high altitudes offer higher observation ranges and increased resolutions. Roughly speaking, satellites can be classified into two major categories, geo-stationary and satellites on polar orbits. Geo-stationary satellites, as the name indicates, are stationary with respect to the earth and illuminate the same region. Because of this unique property, they are mainly used for broadcasting and telecommunications purposes. Satellites on polar orbits on the other hand scan the earth with periods ranging from several hours to a day. Because of their motion with respect to the earth's surface, they can utilize the Synthetic Aperture Radar (SAR) algorithms for obtaining high resolution images including the wakes of vessels and even submerged submarines.

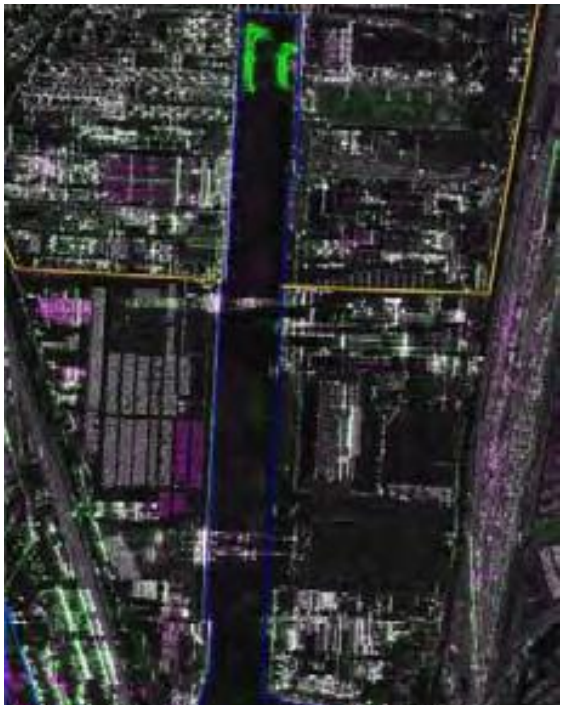


Figure 15 High resolution SAR image of Port of Livorno, Italy

(A MULTILEVEL APPROACH TO CHANGE DETECTION FOR PORT SURVEILLANCE WITH VERY HIGH RESOLUTION SAR IMAGES Francesca Bovolo, Carlo Marin, Lorenzo *Bruzzone*). (Bruno, et al., 2011)

With the advanced image processing algorithms, it has become possible to even count the number of new containers as indicated by the purple color in Figure 15. The resolution of the SAR images can be used to classify ships, detect changes in the port environment, and count the number of containers (Multilevel approach to port surveillance).

A major drawback of the satellite imagery systems is the waiting time needed for a satellite to pass over a specific region to detect the changes. This necessitate the fusion of many information sources to compensate for the periods when the satellite is not available (Bruno, et al., 2011)

8.1.4 Acoustic Detection Systems

All of the detection systems discussed so far either utilize the radio waves or the visual information which is not capable of penetrating the water. As discussed previously, terrorist attacks can be sourced from underwater such as divers, underwater delivery vehicles, or submarines etc. (Bruno, et al., 2011). For such threats coming from underwater sources within the port, acoustic surveillance systems are needed. Acoustics, namely the sound waves, can travel long distances underwater unlike the radio waves, and can be used in a similar manner to radar (consider the bats) for detection and direction finding. Active sonars have been used in

submarines for a long time but similar to active radar carry the risk of being detected by the adversaries. For this reason, several research efforts are in place for passive detection and classification using multi-static arrays of hydrophones (Gebbie, Siderius, & Allen, 2011) (Bruno, et al., 2011).

Similar to the radar systems, acoustic systems have reached such an accuracy that objects such as divers with re-breathers, shrimps, and other acoustic sources can be detected and classified even in the noisy environments of the ports.

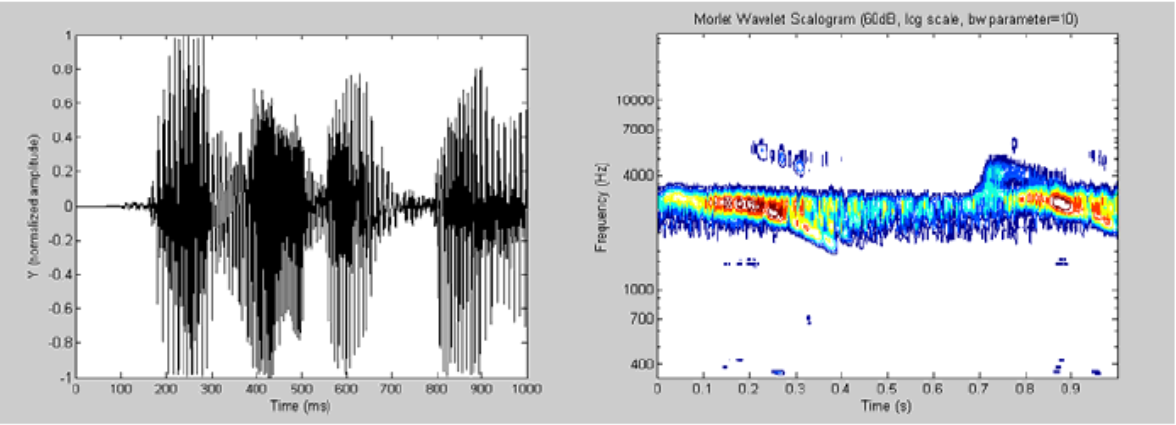


Figure 16 Classification of Ship-harbour signal (Intechopen)

8.1.5 Automated Target Recognition and Classification

With the development of high speed processors to keep up with the computational requirements of the advanced digital signal processing algorithms, automated target recognition and classification has become a reality. Radar and sonar systems with multiple sensors placed on various geographical locations can provide information about the target from many aspect angles similar to looking at an object from various angles (Bruno, et al., 2011). This information can be fused together with other sensor information and processed with advanced digital signal

processing algorithms to extract multiple target related features that can be used in autonomous classification algorithms. Evolutionary methods such as genetic programming have been used to classify the ground penetrating radar signatures of several objects (Koza, 1992) (Kobashigawa & Iskander, 2011). Companies such as Lockheed Martin has devoted a lot of efforts on automatically identifying and tracking ships from SAR, on board imaging cameras placed on several ships, and coastal surveillance data as seen in Figure 17.

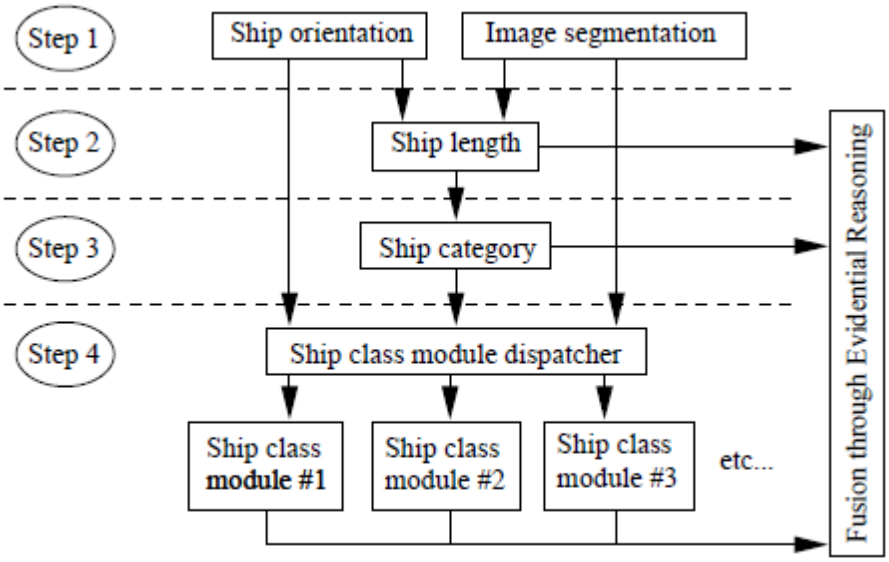


Figure 17 Hierarchical ship classifier design under study at LM Canada (V. Gouaillier)

8.1.6 Automatic Identification System (AIS)

Automatic Identification System (AIS) is an automated radar like tracking system used on ships for identifying and locating vessels by electronically exchanging data with nearby ships and Vessel Traffic Services (VTS) stations. AIS information augments marine radar for the purposes of collision avoidance. AIS on board a ship presents the bearing and distance of nearby vessels in a radar-like display format. For ground stations, the ship information can be displayed real-time on a map as shown in Figure 18.

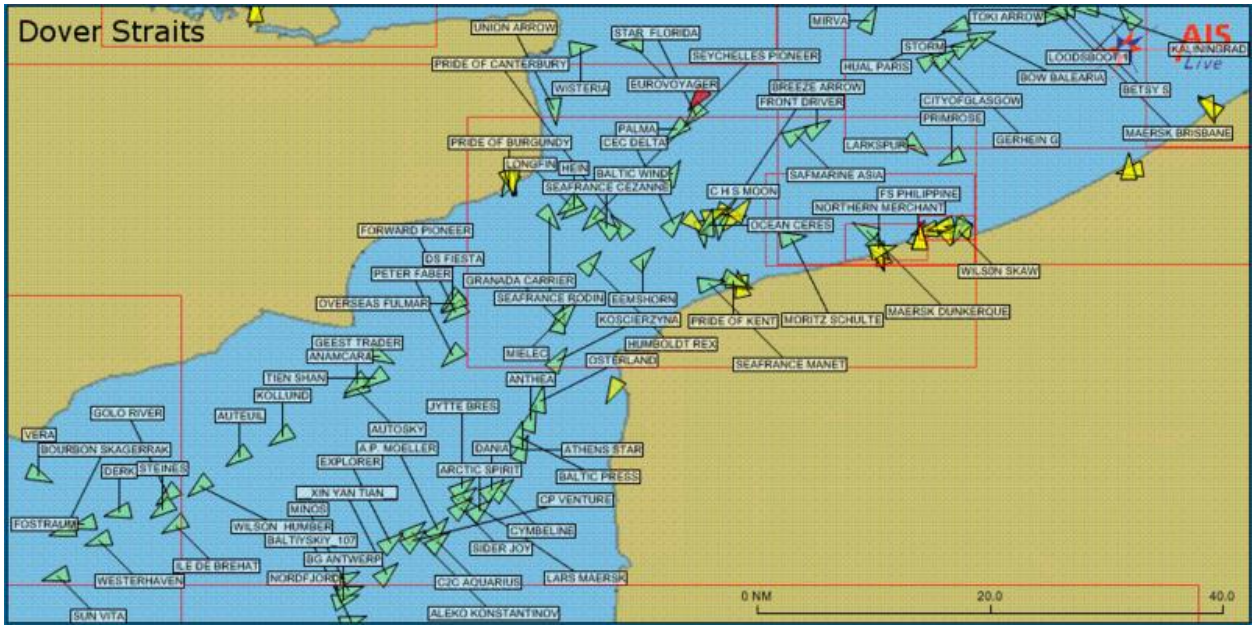


Figure 18 A graphical display of AIS data on board a ship (Wikipedia AIS Article)

Information provided by AIS equipment can assist the watch-standing officers and maritime authorities to track and monitor vessel movements and detect unidentified vessels.

Current SOLAS requirements mandate AIS to be fitted aboard international voyaging ships with gross tonnage of more than 300 tons and all passenger ships regardless of size. Therefore, the AIS system does not diminish the threats from small vessels such as fishing trawlers and require augmentation of other sensors such as high resolution Radar for detection and classification of small vessels.

8.1.7 Port Security/Scanning Systems

The land-sea interfaces of the ports are the ingress/egress nodes which can introduce the threats to the maritime environments. Because of this important fact, the security scanning systems at port interfaces have utmost significance in providing the port resilience.

As discussed previously one of the threats for the maritime environment is the introduction of radioactive devices to cause long term disruptions in the port operation. For this reason, nuclear weapons and radioactive materials are usually detected using passive gamma-ray using large area, high efficiency detectors such as the one in Figure 19 and Figure 20. These detectors allow high speed scanning while the container is in motion, therefore, do not disrupt or slow down the port operations. If the radioactive source is heavily shielded by dense, high-Z material, a complementary technique such as x-ray or gamma-ray radiography is needed. Also imaging technologies can help in this sense to verify that the contents match with the cargo manifest.

Because of the large amount of cargo volume handled daily at ports, automated identification of the container and truck is essentially needed. For this, mature technologies such as automated license plate readers and cargo container identification (OCR) can be easily adapted as seen in Figure 21.

ICIS (Integrated Container Information System) developed by SAIC (Science Applications International Corporation) integrates the information from various sensors from the port interface and provides a graphic display of the integrated data. (Orphan, Muenchau, & Gormley)

Figure 19 Gamma Scan (Orphan, Muenchau, Gormley, & Richardson, Advanced Cargo Container Scanning Technology Development)

Figure 20 Radiation Detector (RPM) (Orphan, Muenchau, Gormley, & Richardson, Advanced Cargo Container Scanning Technology Development)

Figure 21 OCR (Orphan, Muenchau, Gormley, & Richardson, Advanced Cargo Container Scanning Technology Development)

8.1.8 Container Tracking Systems

For automated container tracking and GPS location, Radio Frequency Identification (RFID) systems have been proposed (Savi Technology). This system involves very small, low-cost tags that can be attached to containers and interrogated when information is needed. RFID technology is used in all kinds of supply chain operations such as inventory management, and cargo tracking.

With the development of container intrusion detection systems together with RFID, any tampering to the contents of a shipping container when the ship is at a port can be detected and authorities can be automatically warned.

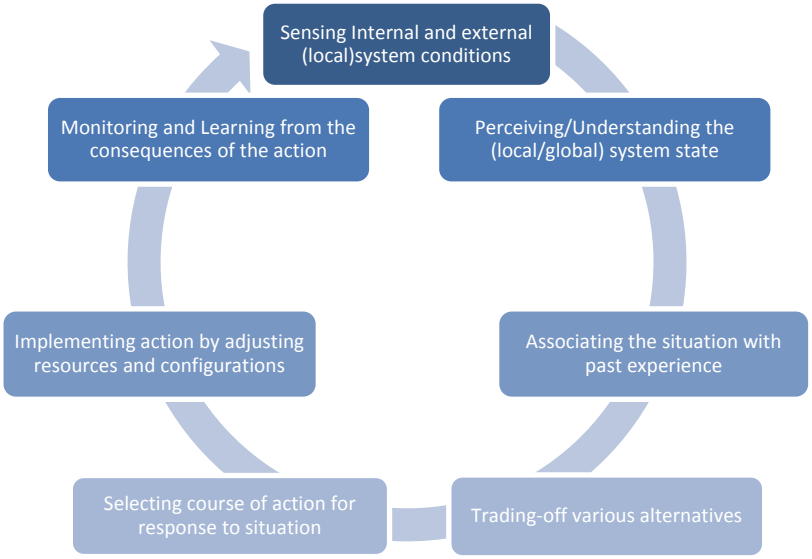
However, because the shipping containers are built using metals, RFID sensors can be placed outside the containers making it impossible to track individual objects within a container. To overcome this problem, acoustic methods for container interrogation are studied. (Spearhead Innovations) (Kundu, 2005)

8.2 Information Fusion to Create Maritime Domain Awareness; Path to Cognitive Ports

All of the technologies discussed above have their respective advantages and limitations. For example, the HF radars have long range but lack the resolution for automated target detection. This necessitate the use of X-band or passive radars in the near range for target identification. In this scenario, the HF radar will detect and track targets at long range and the ones that represent threats will be examined with other sensors at various ranges to detect the threats as early as possible.

Similarly, radio signal based detection systems do not work underwater, so acoustic systems need to be integrated into the security infrastructure. As discussed above, the huge amount of information coming from the sensors in a port environment or even on a national scale has to be collected, analyzed, digested, and displayed in such a format that lends itself to quick decision making. If left unattended, this huge volume of information will not be processed until the threat already takes place at the port.

For this purpose, cognitive port frameworks are proposed that use artificial intelligence methods (Mostashari, Nilchiani, Omer, Andalibi, & Heydari, 2011) for automated decision making. These artificial intelligence methods proposed in the work are iteratively updating the decision rules according to the outcomes of the decision history and available information.



(Mostashari, Nilchiani, Omer, Andalibi, & Heydari, 2011)

Figure 22 Cognition-centric system capabilities (based on Mitola,2006)

A conceptual diagram showing how a cognitive system works is illustrated in Figure 22. This chart shows that in the case of an event, or a threat, the most important thing is understanding the state of the system and conveying this information to the related stakeholders. Then, the system state is identified based on the past experiences automatically and the best decision alternative is selected and forwarded to the related parties. According to the outcome of the action, the past experiences and possible decisions are updated to minimize the consequences of the threats to the port resiliency.

In implementing such a system, the first task is the identification of the key performance and key environmental parameters as shown in Figure 23. This task is very similar to the risk analysis mandated by the ISPS in which event trees are developed according to the operations and interrelations of the multiple components of the port system. Therefore, most of this approach is

already implemented during the implementation of the ISPS code. Similarly, the scenario analysis and the decision making approaches shown in Figure 24 are already part of the security plans in the ISPS.

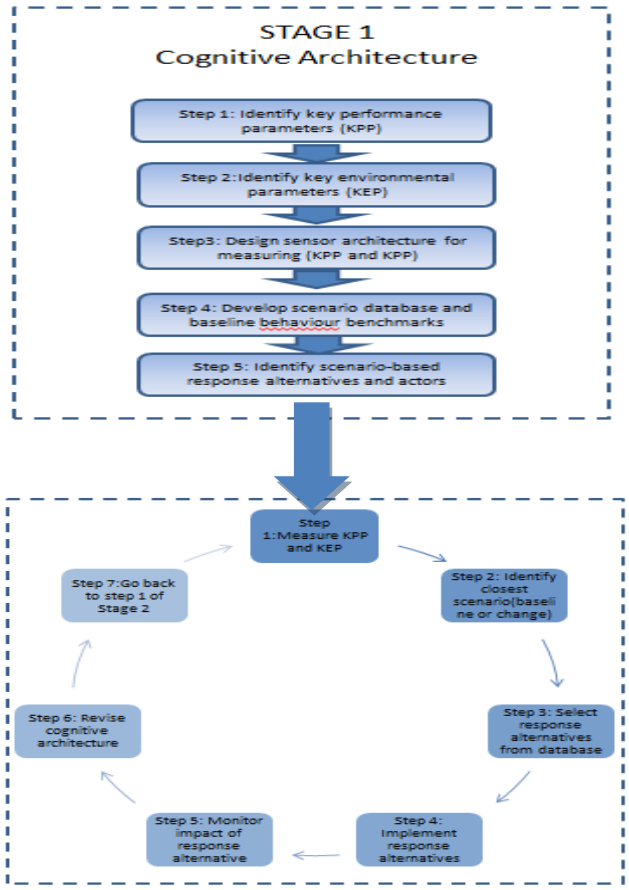


Figure 23 The proposed Cognitive Port Architecture Framework

At the end of this study, a sample response is developed or all possible scenarios as shown in Table 4. From these responses, the contributions of various emerging technologies into providing the port resiliency is very clear. We will discuss this in detail in the next section.

Table 4 Sample response alternatives-scenario-matrix

Scenario	Response Strategy	Actors Involved
S1	Continue monitoring	CG, law enforcement, TSA, etc.
S2	Use databases to identify vessel	CG and law enforcement
	Communicate to vessel for identification	
	Send Coast Guard vessel to investigate	
	Continue monitoring	
	Etc.	
S3	Intercept vessel and disarm	CG, other DHS,U.S. Air Force, etc.
S4	Search and rescue	CG, etc.

CG, Coast Guard; DHS, Department of Homeland Security

(Mostashari, Nilchiani, Omer, Andalibi, & Heydari, 2011)

9. DISCUSSION AND CONCLUSIONS

In the previous section, I have identified several technologies aimed at early detection of threats, alteration of the container contents, or smuggling of radioactive devices into ports. In addition, there are several technologies aimed at reducing these threats that are still conceptual or in the development phase. Once these technologies become mature enough to be commercially available, increased port resiliency can be achieved at affordable costs. However, it is still an unanswered question as to who will be responsible for handling the financial burden of these improvements and additional security measures at the ports. There are several research projects aimed at addressing these but given the complicated relationships of the stakeholders and government organizations involved, it is a very difficult question to answer. Similarly, the ISPS Code does not include any specific body responsible for providing the finance for the implementation .If this financial burden is reflected in the port fees to load them on to the customers, the volume of cargo incoming to a port can significantly decrease as the customers will choose a cheaper port.

Another problem that is discussed is the handling of information coming from multiple sensors and their formatting to arrive at useful decision aids. If left unaddressed, the huge volume of data coming from various technological devices will be very hard to process and will not be any useful for rapid decision making. This will render all the costs paid for these technologies unuseful. The concept of cognitive ports and the use of information technology tools become very important in this sense for rapid processing and dissemination of the data for timely decision making. Using artificial intelligence tools and sensor fusion, the incoming information can be classified into a few categories and sample responses for each category can be developed. As an example, the sample response alternatives of Figure 24 show different responses for

several scenarios. For example, the scenario S1 can correspond to an unidentified target detected by the HF radar system, and in this case the involved actors continue to monitor this target until it gets into the range of other detection systems. The scenario S2, can correspond to the threat target within the range of passive or X-Band radars, in this case the automated classification algorithms can be used to identify the vessel, AIS can be used for information interrogation, or if the threat is too high, the coast guard can intercept the ship before it gets into the vicinity of the port.

In the light of the above paragraph, the radar systems and AIS can be used to detect the vessels and intervene before they get too close to the port to cause any damage, therefore, contribute significantly to the port resiliency. Similarly, for the threats stemming from underwater, acoustic systems with automated target identification can be used to detect the threat locations, types and decide on the type of action to intervene.

For radioactive threats that can be smuggled into the ports from the land-sea interface, several technologies such as radiation scanning, container recognition, and gamma-ray scanning, or ultrasound can be used to check the container contents and identify the trucks and compare against the cargo manifests. Implementation of a fusion of these technologies such as the ICIS can be very useful in reducing the risk associated with radioactive attacks which is one of the significant cases considered by national security experts.

For earthquake and the resulting tsunami threats, HF radar systems can be used as early warning systems to detect the incoming tsunami and to take the necessary precautions. For example, the port of Hawaii sends all the ships out of the port area in the case of a tsunami to minimize the amount of infrastructure damage.

Perhaps, the most important technology component contributing to the resiliency of a port is the information technology infrastructure and the associated artificial intelligence for meaningful information fusion and abstraction. When the amount of information created by all the sensors operating in all kinds of modalities is considered, manual processing of this data becomes infeasible. Therefore, intelligent and adaptive systems are needed to relate all this information to a specific set of scenarios and determine the actions for each scenario and each threat level (Mostashari, Nilchiani, Omer, Andalibi, & Heydari, 2011). This is termed as the cognitive port structure, and also involves a communication infrastructure connecting all the related stakeholders involving the government, military, industry, and port officials.

Lastly, the recent natural disasters and terrorist threats have proven that the port infrastructures are a key component of the global supply chain generating a substantial amount of income for the government economies. The dangers of a prolonged disruption of port operations are too significant and long lasting that elimination of them require strong collaboration, operational changes and information sharing of many organizations at all levels including governments, port authorities, industry representatives, and port workers.

References

(2008). *Building a Resilient Nation.* The Reform Institute.

Wikipedia HF Radar Article. (2011). Retrieved September 12, 2011, from Wikipedia: http://en.wikipedia.org/wiki/Over-the-horizon_radar

Babins, L. T. (2006). *Measuring the Impacts of Increased Security on Ports and Shipping in the Caribbean Basin.* (Master's Thesis).

Bruno, M., Sutin, A., Chung, K. W., Sedunov, A., Sedunov, N., Salloum, H., et al. (2011). Satellite Imaging and Passive Acoustics in Layered Approach for Small Boat Detection and Classification. *Marine Technology Society Journal*, 77-87.

Campell, T., & Gunaratna, R. (2003). *Maritime Terrorism, Piracy and Crime.* Singapure: Eastern Universities Press.

Christopher, K. (2009). *Port Security Management.* Boca Raton,FL: Auerbach Publications Taylor & Francis Group.

Christopher, M., & Peck, H. (2004). Building a Resilient Supply Chain. *The International Journal of Logistics Management*.

Corredor, J. E., Amador, A., Canals, M., Rivera, S., E., C. J., Morell Julio M., G. S., et al. (2011). Optimizing and Validating High-Frequency Radar Surface Current Measurements in the Passage. *Marine Technology Society Journal*, 49-58.

Eicken, H., Jones, J., Meyer, F., Mahoney, A., Druckenmiller, M. L., Rohith, M., et al. (2011). Environmental Security in Arctic Ice-Covered Seas:From Strategy to Tactics of Hazard Identification and Emergency REsponce. *Marine Technology Society Journal*, 37-48.

Gebbie, J., Siderius, M., & Allen, J. S. (2011). Passive Acoustic Array Harbor Security Applications. *Marine Technology Society Journal*, 103-110.

Georgia Tech. (n.d.). Retrieved April 24, 2011, from Geoquake@gatech: http://www.geoquake.gatech.edu/Scratch/downloadable%20pics/Fig2_a.jpg

Gordon, P., Moore, J. E., Richardson, H. W., & Pan, Q. (2005). *The Economic Impact of a Terrorist Attack on the twin Ports of Los Angeles-Long Beach.* Los Angeles,CA: Center for Risk and Economic Analysis of Terrorism Events,University of Southern California.

Greenberg, M. D., Chalk, P., Willis, H. H., Khilko, I., & Ortiz, D. S. (2006). *Maritime terrorism: Risk and liability.* Santa Monica,CA: RAND Corporation.

Herbert-Burns, R. (2005). Terrorism in the Early 21st Century Maritime Domain. In J. Ho, & C. Z. Raymond, *The Best of Times, The Worst of Times:Maritime Security in the Asia-Pasific* (pp. 155-178). Singapure: World Scientific.

IMO. (n.d.). Retrieved May 10, 2011, from www.imo.org: http://www.imo.org/ourwork/security/instruments/pages/ispscode/aspx

Institute, V. T. (2008). *Evaluating Transportation Resilience.*

Intechopen. (n.d.). Retrieved July 23, 2011, from http://www.intechopen.com/source/pdfs/15115/InTechUnderwater_acoustic_source_localization_and_sounds_classification_in_distributed_measurement_networks.pdf

Iskander, M. F., Yun, Z., Celik, N., Youn, H., Omaki, N., & Baker, J. M. (2011). High-Frequency and Passive Radar Designs for Homeland Security Applications. *Marine Technology Society Journal*, 111-119.

Jackson, B. A., Dixon, L., & Greenfield, V. A. (2007). *Economically Targeted Terrorism:A review of the literature and a framework for considering defensive approaches.* Santa Monica, CA: RAND Corporation.

Kobashigawa, J., & Iskander, M. (2011). Comparison between genetic programming and Neural Network in classification of buried unexploded ordnance (UXO) targets. *Antennas and Wireless Propagation Letters*.

Koza, J. R. (1992). *Genetic Programming.* MIT Press.

Kristiansen, S. (2005). *Maritime Transportation:Safety Management and Risk Analysis.* Oxford: Elsevier Butterworth-Heinemann.

Kundu, T. (2005). *Ultrasonic nondestructive evaluation: engineering and biological material Characterization.* CRC Press.

Maritime Terrorism. (n.d.). Retrieved May 15, 2011, from Maritime Terrorism Research Center: http://www.maritimeterrorism.com/definitions/

Masters, D. C. (2008). *Safe ports: A global issue*. Retrieved July 20, 2011, from Homeland Security Innovation Association: http://www.hlsia.org/

Mazaheri, A. (2008). *How the ISPS Code effects Ports and Port Activities.* (Master's Thesis).

Milcom Monitoring Post. (n.d.). Retrieved June 16, 2011, from http://mt-milcom.blogspot.com/2007/08/forces-surveillance-support-center.html

Monstersandcritics. (n.d.). Retrieved May 03, 2011, from http://www.monstersandcritics.com/news/africa/features/article_1434085.php/In_photos_Somalia_- _Pirates_Hold_Ukrainian_Ship

Mostashari, A., Nilchiani, R., Omer, M., Andalibi, N., & Heydari, B. (2011). A Cognitive Process Arcgitecture Framework for Secure and Resilient Seaport Operations. *Marine Technology Society Journal* , 120-127.

Orphan, V., Muenchau, E., Gormley, J., & Richardson, R. (n.d.). *Advanced Cargo Container Scanning Technology Development.* Retrieved August 4, 2011, from The Transportation Research Board of National Academies: onlinepubs.trb.org/onlinepubs/archive/Conferences/MTS/3A%20Paper.pdf

Parker, R. (2010). Security Challenges Beyond 2010: Building Resilience. *The Journal of Defence and Security, Vol.1,No:2*, 145-153.

Pitera, K. A. (2008). *Interpreting Resiliency: An Examination of the Use of Resiliency Strategies within.*

Rice Jr, J. B. (2003). *Supply Chain Response to Terrorism:Creating Resilient and Secure Supply Chains.*

Richardson, M. (2004). *A Time Bomb for Global Trade: Maritime-Related Terrorism in an Age of Weapons of Mass Destruction.* Singapure: Institude for Southeast Asian Studies.

Rodrigue, D.-P. (2008-2012). *THE GEOGRAPHY OF TRANSPORT SYSTEMS*. Retrieved May 10, 2011, from Hofstra University: http://people.hofstra.edu/geotrans/eng/ch3en/conc3en/modaltransportcosttonmile.html

Rodrigue, D.-P. (2011). *THE GEOGRAPHY OF TRANSPORT SYSTEMS*. Retrieved May 11, 2011, from Hofstra University: http://people.hofstra.edu/geotrans/eng/ch5en/conc5en/globaltradeenvironment.html

Savi Technology. (n.d.). Retrieved 2011, from Savi Technology: http://www.savi.com/

Soo Yong, L., Zhengqing, Y., Baker, J., Celik, N., Hyoun-sun, Y., & Iskander, M. (2009). Propagation Modeling and Measurement for a Multifloor Stairwell. *Antennas and Wireless Propagation Letters, IEEE*, 583.

Spearhead Innovations. (n.d.). Retrieved September 13, 2011, from Spearhead Innovations: http://www.spearheadinnovations.com/html/pass.htm

Ung, S.-T. (2010). Current Status of Maritime Security Risk Assessment. *International Forum on Maritime Security* , (pp. 227-236).

USS Cole Bombing. (n.d.). Retrieved May 03, 2011, from Wikipedia: http://en.wikipedia.org/wiki/USS_Cole_bombing

V. Gouaillier, L. G. (n.d.). Retrieved June 19, 2011, from http://www.google.com/url?sa=t&rct=j&q=lockheed%20martin%20ship%20recognition&source=web&cd=1&ved=0CB4QFjAA&url=http%3A%2F%2Fciteseerx.ist.psu.edu%2Fviewdoc%2Fdownl

oad%3Fdoi%3D10.1.1.41.8222%26rep%3Drep1%26type%3Dpdf&ei=4d-4TuPgDubViALT8eTtBA&usg=AFQjCNFZ

Wikipedia AIS Article. (n.d.). Retrieved June 20, 2011, from http://en.wikipedia.org/wiki/Automatic_Identification_System

Wikipedia Passive Radar Article. (n.d.). Retrieved November 03, 2011, from Wikipedia: http://en.wikipedia.org/wiki/Passive_radar

Wilkens, R., Gemelas, T., & Bruno, M. (2011). In Search of Transparency in the Maritime Domain:An Introduction. *Marine Technology Society Journal*, 7-10.

Willis, H. H., & Ortiz, D. S. (2004). *Evaluating the Security of the Global Containerized Supply Chain.* Santa Monica,CA: RAND Corporation.

Yossi, S. (2005). *The Resilient Enterprise.* Cambridge, Massachusetts: The MIT Press.