THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION VOLUME 7 NUMBER 10

APRIL 2009
MARITIME AND PORT SECURITY

Contact: CIPP02@gmu.edu
703.993.4840

In this month's issue of The CIP Report, we take a look at maritime and port security. As the news focuses on the recent events involving Somali pirates taking an American hostage, the importance of maritime security becomes increasingly evident. We present articles that focus on the different aspects of maritime and port security.

GEORGE MASON UNIVERSITY
School of Law
CENTER for INFRASTRUCTURE PROTECTION

The Naval Postgraduate School (NPS) provides an article about the National Security Institute's Maritime Defense and Security Research Programs. The program's research focuses on maritime defense and securing our nation. NPS describes some of the research efforts. The second article, from Old Dominion University, discusses hazardous cargo that comes into U.S. ports and the safety issues involved. The next article provides an overview of the Marine Transportation System and the ongoing efforts to enhance its reliability and resiliency. Another article, from the Commonwealth Homeland Security Foundation (CHSF), explains the importance of port security and the work CHSF is doing in this area. The U.S. Coast Guard (USCG) provides an interesting look at the Hampton Roads Command Center and their role in keeping an important part of our critical infrastructure safe.

This month's Legal Insights discusses the Maritime Transportation Security Act. We also include a reminder of the upcoming 3rd National Conference on Security Analysis and Risk Management that CIP is co-hosting. Lastly, we present the abstract of a regional risk analysis paper recently posted on CIP's website.

We hope you enjoy this issue of The CIP Report as well as find it useful and informative. Thank you for your support and feedback.

Mick Kicklighter

Mick Kicklighter
Director, CIP
George Mason University, School of Law

Research Programs Contribute to U.S. Maritime CIP

by Naval Postgraduate School National Security Institute's Maritime Defense and Security

The Naval Postgraduate School (NPS) National Security Institute's Maritime Defense and Security Research Programs (MDSRP) are a community of researchers, practitioners, and policy developers whose focus is dedicated to advancing the maritime defense and security of our nation. Its organizational objective is to conduct and coordinate maritime defense and security research, experimentation, and information exchange between partner universities; federal, state, and local agencies; national laboratories; maritime industry; and international partners through the National Security Institute. Participants and co-sponsors of its diverse programs include the Office of Naval Research, Under Secretary of Defense of Homeland Defense and America Security Affairs, Department of Transportation, Lawrence Livermore National Laboratory, Stevens Institute of Technology, Marina Police Department, Office of Global Maritime Situational Awareness, Department of Justice, Stanford Research Institute, and many others. Contributions to the nation's maritime transportation system critical infrastructure span the scope of the MDSR programs. Specific research programs include multiple at-sea experimentation programs; basic physical, atmospheric, and sensor research; multiple initiatives related to maritime domain awareness; and red cell and education activities. Highlighted in this article are two specific research examples: the SEAWEB network experimentation program and the West Coast Port Operations modeling efforts, followed by a summary of the collaborative Maritime Information Sharing Taskforce (MIST) program.

The first research example, the SEAWEB network experimentation program, evaluates tactical acoustic sensors for port defense. It is applied research that is producing state-of-the-art undersea acoustic networked communication/navigation technology for application to Intelligence, Surveillance, Reconnaissance (ISR) and the Global War on Terrorism (GWOT). During February 2008, NPS led a two-week undersea sensor networking experiment in the Port of Long Beach, CA. This experiment represented the initial field work for a new-start NPS initiative called "SEAWEB Port Surveillance." The experiment confirmed the applicability of NPS through-water acoustic networking technology to support real-time monitoring of vulnerable waterside areas in a major domestic port. It further demonstrated the portability of this technology, as the SEAWEB equipment and personnel were deployed from a medium-size truck. As this project evolves, networked underwater sensors will be integrated with terrestrial and national surveillance systems for environmental measurements, intruder detection, and rapid response by security agencies to facilitate the protection of critical infrastructure.

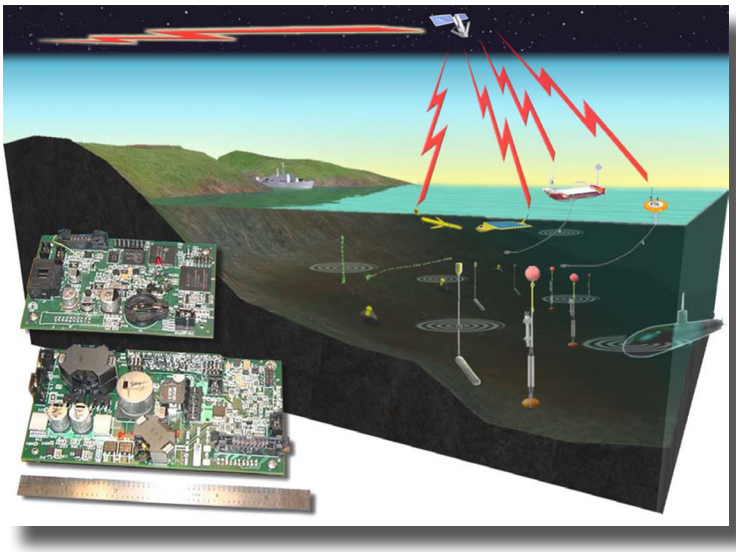
Experimentation is also underway to develop a capability for SEAWEB networks to self-organize following ad hoc deployment, node failure, and node addition. This work has been undertaken to meet a requirement for unconstrained deployment and automatic networking of SEAWEB nodes in maritime operations, creating a more reliable system for detecting threats to critical infrastructure in or around the maritime environment.

Future plans include another SEAWEB experiment, BAYWEB, to be deployed for seven days in the San Francisco bay area around Angel Island in late spring, 2009. This experiment's purpose will be to obtain long-term continuous measurements in a port environment, using through-water networked acoustic

(Continued on Page 3)

NPS *(Cont. from 2)*

Figure 1. Representation of SEAWEB network experimentation program



communications for sensor telemetry. The goal is to provide near real-time data dissemination and address issues of working in an environment of extreme currents. This experiment will seek to demonstrate collaboration among the scientific, environmental, security, commerce and academic communities to capitalize on capability and perspective to surface and address potential challenges.

The second research example highlights how operation of the major container ports on the U.S. West Coast is critical to ongoing commercial and security activity. The researchers built a simulation model of the seven major west coast container ports to study their productivity, and especially to measure system-wide consequences, were one or more ports to be taken out or degraded due to a natural or human-caused event.

Modeled are individual container vessels starting with their Notice of Arrival 96 hours out in the Pacific. Vessels then travel to their intended port or to an alternate port if the intended port is closed. In the case of closure of the intended port, an alternate is chosen in accordance with the shipper's own economic self-interest, with an eye toward minimizing time and cost to the ultimate destination. Once at a port, either intended or diverted, the vessel unload time is accounted for, and the shipment is broken into ten pieces bound for each one-digit ZIP code in the continental United States. These landside shipments then travel to the destination ZIP code.

Data were collected on all aspects of the model to ensure validity. This includes data on vessel arrival patterns by intended port, unload time, port capacities (berths), landside travel times, and various costs, including demurrage costs for freight.

Alternate versions of the model were built and exercised using or applying the modeling of several different scenarios of port incidents. Researchers built models both with and without the proposed port at Punta Colonet, Mexico, to see how the presence of that port might help maintain operations in the face of U.S. port closures. The model was run for a one-year time span with thousands of replications to establish statistical precision due to the stochastic nature of this model (and of the system it simulates). The model has been streamlined to be general and scalable in the number of ports and an animation was developed to help with model verification and credibility establishment. Figure 2 (on page 15) is a screenshot of the model (done in Arena simulation software) to illustrate both the logic (the flowchart on the top) and the animation at the bottom.

In spite of preventative efforts, it is always possible that one of the West Coast container ports will have to shut down temporarily due to either a natural catastrophe or a deliberate attack. In that event, both incoming and outgoing traffic will have to be rerouted to other ports and delays will inevitably ensue. Research is being conducted to assess the magnitude of that delay and whether it can be reduced by changes in either infrastructure or policy.

These efforts follow two directions. The main effort includes a Monte Carlo simulation called WCPORT that incorporates decision rules that imitate the decisions of incoming ship captains when they are informed that their intended port has shut down. Statistics are collected about delays to ships and containers as they wind their way to their original destinations. In the simulation, each port is essentially a queue with two parameters: the number of container berths and the number of cranes. This simulation

(Continued on Page 15)

Protecting Workers and Infrastructures in Hazardous Cargo Trades

by Sara Russell, Instructor
Maritime and Supply Chain Management, Old Dominion University

Among the many requirements of a seaport terminal manager is the responsibility to protect personnel from injury and protect terminal facilities from damage. Simultaneously, the manager must maintain efficient operations that meet the requirements of all port users. These tasks will become increasingly more complex: the U.S. Department of Transportation (DOT) projects that by 2020, total freight moved through U.S. ports will increase cargo volumes by more than 50 percent from 2001. The terminal operator will be challenged to quickly handle larger volumes of cargo quayside and landside to meet supply chain and time requirements. An important consideration when handling hazardous cargoes is the extreme volume coupled with faster operations that potentially could lead to increased risk for accidents, spills and explosions. Among the two billion tons of cargo handled by U.S. ports, hazardous materials, chemicals, and other products, if spilled or released, would cause delays within and among key maritime infrastructures including navigable channels, terminals, interstate and rail systems, as well as pose terminal safety issues within maritime infrastructures.

Improper stowage onboard vessels, vessel collisions, unsuitable handling and transfer of products quayside, and accidents inside warehouses or transit sheds can potentially lead to spills or explosions at terminals, thus damaging or destroying key components of the maritime infrastructure. Vulnerabilities beyond the terminals' gates include our inland port infrastructure. The Association of American Railroads states that 1.8 million carloads of hazardous materials are moved annually.[1] Safe handling procedures must be adopted and maintained to prevent disastrous consequences of improper handling and subsequent damage to the quay, the yard or rail systems. Without such procedures, the ensuing damage to these infrastructures not only results in excessive repair costs for terminal owners and operators but can also negatively impact U.S. commerce if cargo is delayed or rerouted.

Hazardous chemicals, when mixed with water or come in contact with air, or when combined with other chemicals, can result in fires, creation of toxic vapors and pollution to humans and marine life. To prevent such disasters, unique handling requirements and safety regulations accompany these products during transportation and transfer operations. For example, liquid natural gas (LNG), a primary energy resource, cooled to -260°F and at atmospheric pressure, travels via specially designed and insulated tankers. Eight LNG import terminals in the U.S. receive cargo from Asia, Africa and the Caribbean. In the event of a spill onboard the vessel, the hazards are dependent upon the size and location of a hole in the ship's structure. If spilled, the cargo is vaporized. And with a viable ignition source, the cloud can ignite and burn, thus damaging the vessel and nearby superstructures, and possibly injuring or killing workers. Ultimately, safety is the priority. The Federal Energy Regulatory Commission, the U.S. Coast Guard, the U.S. DOT and state and local governments have combined efforts to assure enforcement of safety transportation and storage processes for LNG cargoes. In addition to agency regulations, the International Ship and Port Security Code (ISPS) addresses safety plans and responses onboard the vessel and quayside. With strict handling requirements, attention to training activities, and monitoring of operations by all organizations, only four LNG accidents have occurred in the U.S. since 1944.

Chlorine represents another potentially dangerous product. In 2006, the U.S. exported 39,481 metric tons of chlorine for product

(Continued on Page 5)

[1] Boyd, J. D. (2009, March 23). Railroads, Shippers Struggle over Chlorine. *Journal of Commerce*.

Hazardous Cargo *(Cont. from 4)*

use including poly vinyl chloride (PVC) plastics, water treatment, paper bleaching, and various consumer products including detergent, dyes, and insecticides. Fires and explosions result if chlorine, transported as a liquid gas or in a gaseous state, is spilled and reacts with other chemicals. These noxious fumes irritate human skin, eyes and respiratory systems, causing burns, frostbite, and ulcerations. If chlorine is stored on terminal premises, it should be sealed in appropriately labeled containers and separated from combustible products such as gasoline, alcohols and ammonia. The U.S. Occupational Health and Safety Administration (OSHA) recommends personnel handling chlorine be trained in compressed gas handling and safety operations and be equipped with personal safety gear which can include safety suits and respirators.[2] And in the instance of a spill, marine terminals require immediate evacuation to prevent the inhalation of fumes and vapors by workers and residents of surrounding communities.[3]

Chlorine spills are damaging as evidenced by the 2005 Norfolk Southern (NS) train wreck in Graniteville, SC. On January 6, 2005, a train heading towards Columbia carrying tanks of chlorine, liquid sodium hydroxide and liquid cresol missed a switch and collided with a stationary locomotive, spilling 40 tons of chlorine and creating a cloud of chlorine within a one mile radius. Evacuation and cleanup measures were implemented. Nine people died from vapor inhalation and hundreds more sought medical care for respiratory irritations. After 24 days, NS resumed train operations.[4] Not only does this accident demonstrate the effects of hazardous cargo spills and the need for evacuation measures, but it highlights the need for improved supply chain management and alternative cargo routes when infrastructures are disrupted.

Hazmat safety is important whether cargoes are onboard vessels, quayside or landside. Following the 2006 explosions on board the Hyundai Fortune, mis-declaration of hazardous cargo and consequent improper stowage became important issues for shippers, transportation providers, and terminal operators. The International Maritime Organization (IMO) Secretariat published the results of a year-long study involving 25,284 containers of dangerous goods in Belgium, Canada, Chile, Italy, South Korea, Sweden and the United States. Analysts found that 27% of the boxes were improperly placarded and marked, 19% had structural deficiencies, 15% had documentation problems, and 7% had deficiencies in stowage and securing.[5] In an attempt to lower insurance and shipping costs, many importers and exporters fail to take the required safety precautions to ensure safe handling procedures. Not only during the ocean voyage might these shipments be at risk, but once the cargoes reach land, are stored on terminal, and move throughout our maritime infrastructures, they pose a potential hazard.

Various safety protocols exist to facilitate proper transportation procedures. The IMO's Formal Safety Assessment (FSA) is one tool available for facilities proactively instituting safety measures to protect maritime infrastructure and superstructures. FSA, a five-step process, can be used to establish safety regulations or to analyze and update existing regulations. First, organizations must identify hazards by analyzing the types and volumes of cargoes and the transport vessels that access their facilities. Next, they assess damages resulting from these hazards, including the potential for cargo spills. Third, they create plans[6] to control the hazards;

(Continued on Page 12)

[2] *Chlorine.* (n.d.). Retrieved April 2, 2009, from U.S. Department of Labor, Occupational Health and Safety Administration: http://www.osha.gov/SLTC/healthguidelines/chlorine/recognition.html.

[3] Fingas, R. L. (2001). Perspectives on Specific Substances: Chlorine. In M. Fingas, *The Handbook of Hazardous Materials Spills Technology*, p. 19. New York: McGraw-Hill.

[4] Jerry T. Mitchell, A. S. (2005). *Evacuation Behavior in Response to the Graniteville, South Carolina, Chlorine Spill*. University of South Carolina.

[5] Bonney, J. (2007, February 5). What's in the Box? *Journal of Commerce*, p. 1.

[6] *Formal Safety Assessment*. (n.d.). Retrieved April 1, 2009, from International Maritime Organization: www.imo.org/Safety/mainframe.asp?topic_id=351.

Preface to the National Strategy for the Marine Transportation System

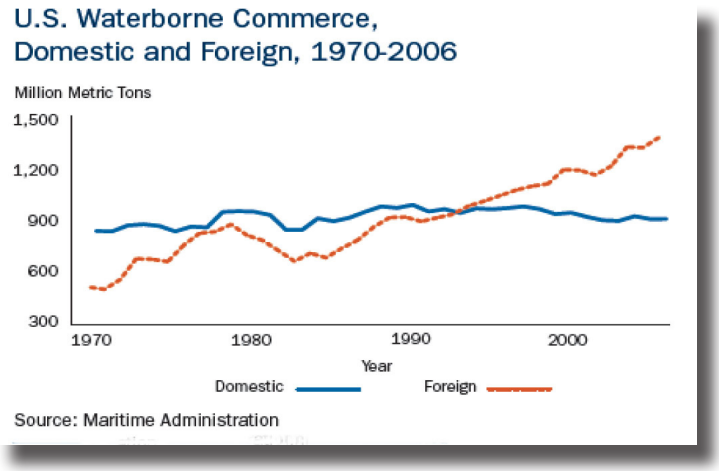
by Mary E. Peters, Former Secretary of Transportation

"As one of the world's leading maritime and trading nations, the United States relies on an effective and efficient Marine Transportation System (MTS) to facilitate commerce and protect our national security."

Introduction

America's Marine Transportation System (MTS) is critical to our national security and economic prosperity. Each year this robust system is responsible for providing the transportation network access to 95% of the goods (by weight) imported or exported from our country resulting in enormous national economic impacts. According to a study based upon data from 2006 the maritime industry contributes nearly $2 trillion annually to the economy and accounts for more than 8 million American jobs[1]. The accompanying graphic, shown in a recent Maritime Administration report[2], demonstrates the extent to which waterborne commerce originating abroad has increased over the past four decades.

The U.S. Marine Transportation System's importance requires all levels of Government and marine industry to focus on insuring its reliability under all hazards and resilience during disruptions. This article summarizes ongoing efforts to further enhance the reliability and resilience of the MTS. Three 2008 major marine disruptions - two hurricanes and a marine collision - are described to highlight the vulnerability of the MTS and to highlight the U.S. Coast Guard's role in responding to them. It briefly describes ongoing Department of Homeland Security efforts to further enhance MTS resiliency and reliability. Finally, it highlights the experience of the Ports of the Lower Mississippi River and the trade resumption and resiliency planning process to address future disruptive events as an example of how our nation's ports are actively improving its capabilities to deal with potential threats and vulnerabilities.



Section I: Waterway Disruptions

Hurricanes IKE and GUSTAV - 2008

Two major category-2 hurricanes struck the United States Gulf Coast in 2008. On September 1st the center of Hurricane GUSTAV made landfall in the United States along the Louisiana coast near Cocodrie. Just two weeks later, on September 13th, Hurricane IKE made landfall on Galveston Island. IKE's enormous size and 12 foot storm surge wreaked havoc from Galveston Island eastward into southern Louisiana. These two storms destroyed many of the Aids to Navigation (ATON) markers used to guide ships through the channels to the ports. With the

(Continued on Page 7)

[1] Martin Associates (n.d), *United States Port-Sector Economic Impacts*, retrieved from: http://aapa.files.cms-plus.com/PDFs/Port%20Sector%20Economic%20Impacts%20Chart.pdf.

[2] U.S. Department of Transportation, Maritime Administration, *America's Ports and Intermodal Transportation System – January 2009.*

Transportation *(Cont. from 6)*

navigation system effectively destroyed, combined with other critical infrastructure issues, the Coast Guard Captain of the Port closed the channel to all vessel traffic pending the repair of these vital services.

Following their planning doctrine the Coast Guard began to surge assets toward the affected area even before the storm's landfall to be positioned to quickly respond to the potential damage and environmental issues, and to provide for assistance to mariners. A primary component of this surge included the entire gulf-coast fleet of six Coast Guard Inland Construction Tenders, which are used to drive piles used for fixed ATON structures[3]. These two storms caused more than 1,200 ATON failures in the waterways along the inland and coastal areas. And of these discrepancies, 334 occurred to fixed ATON structures where only Coast Guard Inland Construction Tenders had the inherent capabilities and supplies to immediately effect repairs.

As a result of this massive surge of operational resources, the Coast Guard rapidly restored the most critical components of ATON system. Working in conjunction with other federal agencies and local port partners, all major waterways were reopened to vessel traffic within just four days of the hurricanes' landfall. Restoring the navigation system leading to the port of Houston was a critical first step in this recovery. As the nation's second largest port area, the ports of Houston-Galveston are responsible for moving 212 million short-tons of commerce each year. The economic impact of a single day of closure for this port has been estimated at $322M[4].

Mississippi River Oil Spill - 2008

This U.S. Coast Guard photo shows some of the more than 100 vessels anchored waiting to enter the port of Houston-Galveston.

On July 24th, 2008, the tugboat *Mel Oliver* pushing a loaded fuel barge collided with the tank vessel *Tintomara*, resulting in an oil spill that closed a 100-mile stretch of the Mississippi River near the port of New Orleans. The collision was so severe it broke the barge in half, causing about 276,000 gallons of fuel oil to be spilled, about 60% of the cargo carried at the time of accident. Cut nearly completely in half, the stern section of the barge sank 100 feet to the river's bottom, significantly complicating recovery operations. As the oil proceeded downriver it involved over 1,000 vessels. Oil product was found throughout the water column, and with the river's height falling, oil clung to many vessels and local infrastructure.

In response to this accident the Coast Guard Captain of the Port of New Orleans restricted all river traffic to ensure marine safety by focusing on the simultaneous challenges of both responding to the sunken barge and ensuring that vessels would not spread contamination throughout the river system. Part of the recovery strategy included establishing cleaning stations that removed oil from vessels within the contaminated zone. Additionally, concerns about exacerbating ongoing cleanup efforts were addressed through the implementation of a safety zone in the vicinity of the sunken barge.

The four day river closure to address the spill caused a back-up of more than 200 ships waiting to enter port. Although this closure was temporary, it still had significant impact on the local, national, and

(Continued on Page 20)

[3] The ATON system generally consists of floating buoys and fixed structures marking channel limits and obstructions.

[4] http://www.portofhouston.com/busdev/tradedevelopment/economicimpact.html, accessed on March 28, 2009.

Port Security in an All-Hazards World

by L. Scott Lingamfelter*

The Vulnerability of Critical Infrastructure

When the United States was attacked on September 11, 2001 by al-Qaeda-inspired terrorists, Americans and our allies around the world witnessed first-hand the vulnerability that is inherent in an open and free society, two critical attributes necessary for the vital free enterprise environment that many citizens take for granted. Since that attack, the United States has made progress in better coordinating national and international efforts to combat terrorism. However, the critical infrastructure of the Nation — 80 percent of which is in private hands — is largely unprotected against coordinated and well-placed attacks by terrorists who seek to disrupt our way of life and weaken our will to resist.

A Compelling Economic Need to Secure Our Vulnerable Ports

Our critical infrastructure is arguably the economic "center of gravity" in the United States. A key component of that center of gravity and our economic system is the commercial and military maritime port infrastructure across the Nation and throughout the world as well as the critical supply chain that links maritime centers to the heartland. Eighty percent of the world's trade travels by water, making ports the linchpin to our national commerce. The U.S. and world economy depend on commercial shipping as the most reliable, cost efficient method of transporting goods. Currently, U.S. ports handle approximately 20 percent of the maritime trade worldwide. Shipping through American ports generates $8.7 billion each day for the U.S. economy, or about 29 percent of the daily gross domestic product. Our ports are irreplaceable in the movement and performance of a critical supply chain that, if interrupted, will cripple the economy of our Nation and much of the free world. Some recent examples clearly illustrate how a disruption impacts the economy.

- In 1995, the earthquake in the Kobe, Japan had a major impact on the world economy, requiring the diversion of more than 100 ships that were en route to other ports in Japan and an economic loss approaching $50 billion.

- In the fall of 2002, a port strike on the West Coast resulted in an 11-day disruption in the movement of goods. Ships were left at anchor from Los Angeles to Taipei with a $19 billion loss of revenue to the U.S. economy.

- In July of 2008, the Port of New Orleans was shut down for six days following an oil spill that stranded 200 ships.

The impact of an attack on a major maritime port facility and the critical supply chain is hard to exaggerate. If the Mississippi River were blocked for an extended period of time, the cost to the Nation could approach $275 million per day. While the examples above were not caused by terrorists, an attack resulting in the disruption of the critical supply chain associated with the maritime system (mainly major ports) can severely hamper trade and potentially cripple the global economy by hundreds of billions, if not trillions, of dollars. We must take effective action to better secure our port facilities.

Consider the facts. The two largest container ports in the world, Hong Kong and Singapore, together handle more than one million 40-foot ocean containers each month. A large container ship can discharge over six million pounds of freight in an hour. Daily, more than 15 million containers are moving by sea, rail, or road around the world. In 2002 eight million containers and 59,995 vessels entered 3,700 terminals and 301 ports in the United States. Today, it is estimated that 9 to 11 million containers move through our Nation in a year. Indeed, close to 90 percent of the world's general cargo moves by containers. When they cease to move, the effects impact the core operations of Wal-Mart, Lowes, Home Depot, Ford, General Motors, and Chrysler, not to

(Continued on Page 9)

Port Security *(Cont. from 8)*

mention the millions of small businesses that form the backbone of the American economy. The movement of products from ports is impressive. Yearly, 310 million tons of raw materials and agriculture products are transported on the Mississippi River. An excess of 90 percent of America's imported and exported goods are sent to South America, Europe, Africa, and Asia by sealift.

Likewise, the Hampton Roads port region is a vital commercial center for Virginia and the Nation. One of the world's largest harbors, our port region sits only 18 miles from the open ocean and is easily accessible to shipping lines and shippers alike while serving as the home to the Virginia Port Authority (VPA) and AMP/Maersk. For example, the VPA alone affects 345,000 jobs in Virginia while generating $41 billion in business revenues and $1.2 billion in State and local taxes per year. Moreover, with the future development (beginning in 2017) of the Craney Island Marine Terminal by the Port of Virginia, the capacity of the Hampton Roads region to service cargo will increase by 1.5 million TEUs (twenty-foot equivalent unit) while making Virginia home to the most modern deep water terminal on the East Coast. Currently such companies as Wal-Mart, Target, Home Depot, Family Dollar, QVC Network, Cost Plus, Dollar General, Kohls, Sysco, as well as a wide range of food producers and energy providers transit the port facilities in the Hampton Roads region. All of them depend on uninterrupted access to the port to sustain their critical supply chain. An extended closure of the port region by a man-made or natural disaster would devastate these industries and countless jobs.

The Real Threats That We Confront

The ideological and terrorist forces that seek to disrupt and destroy our way of life understand that our economic viability is an essential component to maintaining that way of life. Ports, their infrastructure, and the intermodal connectivity to them are obvious targets. Port terminals and the millions of cargo containers they handle can be exploited to carry out terrorists' plans. Shipping containers provide a vehicle for terrorists to smuggle destructive devices into the United States, including nuclear, chemical, or biological material that could be configured as a "dirty bomb" ready to explode at the port or elsewhere.

Terrorists know the potential of improvised explosive devices (IED) in combat and may be contemplating a new generation of IEDs to attach to ships as they enter ports and terminal facilities. Refineries, ship building and maintenance facilities, power plants, and sensitive national defense-related sites are routinely found in our major ports and specifically in Hampton Roads. They are all targets for our enemies who are determined to deploy the next generation of IEDs, some of which may use nuclear material to create a dirty bomb.

Likewise, terrorists know that a well-timed sinking of a major commercial ship in a critical channel could halt shipping for an extended period of time. Similarly, rail and road networks are vulnerable to dirty bombs that when detonated could destroy tunnels, bridges, and rail yards, bottling up economic activities at a port.

Our inability to effectively and reliably detect, deter, and disrupt such threats in a layered and sophisticated way could result in extended closure of a maritime facility until the port and region could be rendered safe. This inability is well known by our enemies and we must address it.

Innovative Solutions to Mitigate Risks

While no solution will ever make our ports and the critical supply chain immune from attack, we must devise effective strategies that will mitigate the risk of disruption to an acceptable level while planning for sufficient resiliency in port infrastructure to help those facilities resume normal operation as soon as possible in the wake of a man-made or natural disaster. The key to success is not an impenetrable cordon around our ports and its infrastructure, but rather a balanced and risk-focused strategy that incorporates the best practices and necessary technologies to detect, deter, and disrupt hostile acts against the most likely vulnerabilities before they happen, while also — in the event of an

(Continued on Page 16)

United States Coast Guard Sector Hampton Roads Command Center Joint - The Living and Breathing Port of Hampton Roads

by Brittani Lashaway, LTJG, USCG

The Port of Hampton Roads can be described as the commercial heartbeat of the Mid-Atlantic. Like every form of life, the Port of Hampton Roads continues to grow and become more efficient with every passing year. According to the Port of Virginia port statistics, in 2007, the Port of Hampton Roads had over 3,000 vessel calls and was the third largest U.S. East Coast container and general cargo port[1]. In 2008, the port handled approximately 1.2 million containers. Virginia's sheltered, ice-free harbor encompasses 25 square miles of easily accessible waterways and is located just 18 nautical miles from the open sea. It offers ships carrying the heaviest cargoes the ease of steaming in and out of 50-foot-deep, obstruction-free channels. With these opportunities come challenging situations, such as drug trafficking, terrorist threats, and the need for environmental protection. The port security challenges force the Coast Guard and its Federal, State, and private industry partners to work together to maintain "life" within the port.

The basis for every DNA strand in a port is the definition of the Captain of the Port (COTP) found in Title 33 of the Code of Federal Regulation (CFR) Part 6. The COTP regulates all law enforcement activity. A few of the responsibilities listed in 33 CFR 6 for the COTP are as follows: guarantee all commercial vessels coming into the port are screened; protection and security of vessels, harbors, and waterfront facilities; possession and control of vessels while in the port; and the issuance of documents and employment of persons aboard U.S. vessels. The COTP Zone for Hampton Roads is found in Title 33 CFR 3.25-10 and has these boundaries: the southern border is the Virginia/North Carolina state line; the northern border is the Chesapeake Bay of the Virginia/Maryland state line; the northern border for the Atlantic side of the Eastern shore is the Maryland/Delaware state line; the western boundary is the western portion of the Virginia state line; and the eastern boundary is out 200 nautical miles from the baseline (see Figure 1). Another important strand of the DNA is the Regulated Navigation Area (RNA) found in Title 33 CFR 165. This area defines the navigational equipment required onboard commercial vessels to protect the port from what the U.S. believes to be possible shortfalls that other foreign countries might have in regards to navigational equipment. The RNA begins 12 nautical miles seaward with the remainder of its perimeter defined by the James River Bridge, the West Norfolk, I-64 High-rise, and Campostella Bridges which cross various tributaries of the Elizabeth River, and an imaginary line from Hampton, Virginia across the Chesapeake Bay to Cape Charles, Virginia on the eastern shore. The final and most important strand of the DNA is the Coast Guard's Notice of Arrival (NOA) requirement. It requires commercial vessels to submit an electronic notice to the National Vessel Movement Center (NVMC). This notice is put into a database to inform U.S. ports of the vessel's last ports of call, size, cargo, flag, and crewmembers' names and nationalities.

Figure 1. Sector Hampton Roads Area of Response is defined by the red line.

(Continued on Page 11)

[1] http://www.portofvirginia.com/development/port-stats.aspx.

USCG *(Cont. from 10)*

The brain, or information management center, for the Captain of the Port is the Sector Command Center-Joint (SCC-J). Within the SCC-J, there are cameras to view the port, and communication is conducted via marine radios. The SCC-J has nine different watch positions; seven of them are manned twenty-four hours a day, seven days a week, and 365 days of the year. The jobs the SCC-J watch standers complete are diverse and are the vanguard of port security. The Command Duty Officer (CDO) is a twenty-four hour watch position. During the watch period, the CDO is the direct representative of the COTP, and oversees the other eight individuals on the watch floor. Operational Unit Controller (OUC) is the first line of response for search and rescue cases, marine casualty cases (onboard commercial vessels), pollution spills, and suspicious/actual terrorist activity within the COTP zone of Hampton Roads. Two individuals man the OUC desk twenty-four hours a day, standing twelve hour watch shifts. This position is an essential part of the SCC-J. Just as the brain directs the muscles to move and react to various situations, the OUC directs Coast Guard assets from seven boat stations and five patrol boats, and coordinates between Federal/State agencies to launch for emergency situations. OUCs not only direct assets to launch, they also gather essential information and enter it into a central database to ensure the entire Coast Guard is aware of all known facts for each case. Two people stand the Communications Unit (CU) watch each twelve hour period. The CU watch standers monitor the Sector's marine radios for distress calls or other abnormalities that come across the radios. They then pass this information to the OUC who begins to prosecute the case. The Vessel Arrivals Desk (VAD) is manned seven days a week for nine hours a day. This position screens all commercial vessels coming to the COTP zone based on the information provided in the Notice of Arrival (NOA). Each vessel is evaluated based on its last ports of call, cargo, flag, nationality of crew, and size, and then, in totality, assessed and assigned a level of risk associated with its arrival to the port. Depending on the risk assessment, it may have to be boarded before entering, or it may transit without any further investigation by the Coast Guard. The VAD also schedules vessel examinations to ensure compliance of safety and security standards. The Situation Unit (SU) watch stander is stood by one person in twelve hour shifts and maintains overall situational awareness of all watch positions. The SU watch stander is responsible for double checking all commercial vessels that the VAD has evaluated to ensure accuracy, keeps track of all aids-to-navigation discrepancies within the COTP zone, and assists with the tracking of all radar contacts of commercial vessels either entering or transiting through the Port of Hampton Roads. The Enforcement Duty Officer (EDO) is in the SCC-J eight hours a day during the work week and is on call the remainder of the time. The EDO is the primary point of contact for drafting COTP orders that coordinate High Interest Vessels (HIV) movements. HIVs are vessels that wish to enter the Port of Hampton Roads, but due to some elevated level of risk require additional security measures prior to entry. The final position in the Command Center is the Sensor Manager (SM) watch stander. This position is staffed by United States Navy personnel who keep track of all vessels that wish to enter the Regulated Navigation Area within the Port of Hampton Roads. SM watch standers track vessels in the Port using Radar, Automated Identification System (AIS), and cameras that are strategically placed throughout the port. AIS is a required tracking system for all commercial vessel 300 gross tons or larger, and uses a radio transponder to provide a real time positions of vessels in the area. The SM watch standers work closely with the Virginia and Maryland Pilots to ensure all vessels entering/transiting through Hampton Roads comply with safety and security regulations and are cleared to enter/transit. The Coast Guard/Navy relationship is the reason that Hampton Roads is designated as a Sector Command Center-Joint, one of only four in the entire Coast Guard.

To truly experience the heartbeat of Hampton Roads, imagine working this actual scenario that a CDO experienced in the SCC-J.

On Thursday morning November 8, 2007 at exactly 0600 in the morning, as I entered the Command Center, the sliding glass door opened up from the

(Continued on Page 17)

Hazardous Cargo *(Cont. from 5)*

this step can include establishing handling procedures, conditions for unloading/loading cargo, and training requirements. Fourth, operators create a cost-benefit assessment of the damage and create action plans for the institution and maintenance of the safety plans. This proactive approach to hazard identification mitigates the effects and costs of such incidents.

Within the hazardous cargo arena, numerous regulations complement facility operations and plans. One example is the International Maritime Dangerous Goods Code (IMDG Code) which establishes universal rules for maritime transport of dangerous goods. It includes protocols for packaging, labeling, classification, stowage, segregation and emergency response action for all interested parties including manufacturers, shippers, and intermodal transport providers and port authorities. It then becomes the port users' responsibility to adopt and follow such measures. However, most port safety protocols differ from port to port and local factors contribute to the disparities. These factors include individual jurisdiction of terminal property and the types and volumes of cargo handled, which in turn influence the activities performed on terminal property, combined with physical location issues from tidal changes, wind speeds, and temperatures. Core elements addressed by all safety procedures include the responsibilities of port authorities, terminal operators, and employees with regard to air pollution; transportation, storage and handling of harmful goods; proper equipment usage; maintenance and training policies; emergency and first aid plans; and general yard operations. For port authorities, failure to adopt, maintain, and update safe handling procedures can lead to employee illness claims and damage to infrastructure.

Direct and indirect costs resulting from worker injuries account for an economic loss between 4-5 percent of the Gross Domestic Product.[7] Direct costs include hospital-related expenses, physicians, drugs, health insurance administration and worker compensation costs, whereas indirect costs include loss of wages, costs of fringe benefits, employer retraining, workplace disruption costs (damages to equipment, tools and materials and required overtime), increased insurance premiums and loss of company goodwill.

The American Society of Safety Engineers (ASSE) states that indirect costs associated with safety failures can continue to impact organizations and are potentially 20 times greater than direct costs.[8] Negative publicity, an automatic result from workplace accidents and health scares, manifests a cost associated with the inability to attract potential employees. Other costs include workers' inability to reach productivity levels following a traumatic event, or the costs of counseling stemming from traumatic events. Therefore, by instituting a plan, the organization not only saves and improves productivity, but society perceives it as a well-respected corporate citizen.[9] Management organizations realize the negative impact of ignoring worker safety, which often translates into costly downtimes and high fines. Additionally, equipment malfunctions can result not only in worker accidents but also in delayed vessels and fewer vessel calls. For example, in January 2008, the Southampton Container Terminal experienced such delays and reduced productivity when a crane collapsed onto a berthed ship.[10] As a result, five cranes of similar design were pulled from quayside operations for inspection, thus necessitating over a dozen ships to reroute their cargo. The port experienced a 40% decline in business due to the down cranes. As investigations continue into the cause of the accident, the terminal loses business as ships and cargo are rerouted to neighboring ports. Therefore, ports and maritime facilities must assess their risk to such hazards by analyzing the types of cargoes, volumes of cargoes and handling methods to mitigate risks including spills, corrosion, and explosions that could seriously damage maritime infrastructure. ❖

[7] *Occupational Health.* (n.d.). Retrieved July 26, 2008, from the World Health Organization: www.who.int/occupational_health.
[8] Engineers, A. S. (2002). *White Paper: The Return on Investment for Health and Environmental Management Programs.*
[9] Russell, S. E. (2008). Port Workers and Safety. In W. K. Talley, *Maritime Safety, Security and Piracy,p. 20. London: Informa.*
[10] Porter, J. (2008, February 19). Ships steer clear of Southampton. *Lloyd's List*.

Legal Insights

The Maritime Transportation Security Act of 2002

by Timothy P. Clancy, JD, Senior Program Manager, Cyber/IT

One of the most important pieces of federal homeland security legislation is the Maritime Transportation Security Act (MTSA). Passed by Congress in 2002, MTSA sets out a series of policies and procedures to better secure U.S. ports and waterways from acts of terrorism. This legislation and its corresponding regulations have had a dramatic and far-reaching influence on security practices across the complex international system of maritime transportation and commerce.

In the United States, government security responsibilities for the maritime sector — as in many CI/KR sectors — have been shared traditionally by a complex mix of Federal, State and local authorities. Port authorities are chartered primarily by State or local government entities and are a mix of private sector, quasi-government and government entities. Traditionally, seaports have been subject to limited federal regulation — such oversight and regulation was largely left to the States and localities.

The events of September 11 changed this regulatory paradigm dramatically. In the months following, there was a great deal of concern raised in Congress and internationally about the vulnerability of ports and waterways to potential terrorist attacks. As a result, Congress and the Executive Branch acted swiftly to radically alter port security practices.

MTSA and its corresponding regulations were central to this radical new era of U.S. maritime security. MTSA and subsequent homeland security laws established broad federal authority to regulate and police maritime activities in the United States both on land and in domestic waters.

There is no question that the federal government has the power under the Constitution to assume this authority and responsibility. Security of navigable waterways in the United States has always been the responsibility of the federal government, carried out by the United States Coast Guard. The federal government also has the constitutional authority to regulate interstate and foreign commerce and consequently has wide powers to regulate port practices.

An important feature of the U.S. maritime and port security regime under MTSA is that it closely tracks to international port security standards. Also adopted in the aftermath of September 11, the International Ship and Port Facility Security Code (ISPS) was promulgated by International Maritime Organization (IMO) under the authority of the International Convention for the Safety of Life at Sea (SOLAS).

The ISPS Code is a two-part document providing measures and procedures to prevent further acts of terrorism which threaten the safety of ships and the security of passengers and crews. The ISPS Code is intended to provide guidance while allowing individual countries to adopt their own security measures and procedures based on the Code.

These international standards entered into force in July, 2004, the same time as many of the key provisions of MTSA. While ISPS is a mixture of mandatory regulations and voluntary guidance, however, MTSA makes all ISPS provisions mandatory and gives the Coast Guard and DHS strong authority to enforce MTSA provisions.

The goal of MTSA is to establish a more consistent security regime for ports across the U.S. to better identify and deter threats. The Act is built on a risk-based methodology and is focused on

(Continued on Page 14)

Legal Insights *(Cont. from 13)*

elements of the maritime sector that pose significant risk to life and property, such as tankers, large passenger vessels, offshore oil and gas facilities and other seaport facilities that handle hazardous materials or cargo. The legislation requires both vessels and port facilities to conduct vulnerability assessments. Vessels and facilities must also develop and implement certain security plans. These security plans may include passenger, vehicle and baggage screening procedures; security patrols; establishing restricted areas; personnel identification procedures; access control measures; and/or installation of surveillance equipment.

Another important aspect of MTSA is its provisions that encourage the sharing of information on threats and vulnerabilities across layers of government and the private sector. These provisions seek to shield certain sensitive and classified security information about critical port facilities from public disclosure. Indeed, as was discussed in the May 2007 CIP Report, these MTSA provisions were used as a template for similar information protection provisions in the Chemical Facility Anti-Terrorism Standards (CFATS) legislation. MTSA also created certain mechanisms at each port — Area Maritime Security Committees, for example — to include key private-sector port stakeholders as well as State and local law enforcement to enhance coordination and information sharing.

MTSA and its subsequent law, the SAFE Port Act, have not been without controversy. The implementation of the Act's requirements for a national maritime worker biometric identification card for access to vessels and critical port facilities has been contentious. DHS has begun enforcement of the new Transportation Worker Identification Credential™ (TWIC) requirement this month, while giving some ports in the South and West regions some leeway for full implementation of TWIC. Once TWIC is implemented, all port workers must display biometric TWIC credentials for unescorted access to secure areas of the ports.

MTSA is a landmark example of homeland security legislation. Crafted in cooperation and in concert with international security standards organizations, it swept away a patchwork security regime for the maritime sector. By making most international guidelines mandatory, the United States led by example in greatly strengthening maritime security practices globally. The Act has also had an impact on other CI/KR sectors: subsequent legislative attempts to more tightly regulate certain sectors have used MTSA as a template for a risk-based methodology and improved information sharing.

The Federal government has taken a much stronger role in regulating and policing the nation's ports and maritime transportation system since September 11. MTSA represents the core of this effort. ❖

NPS *(Cont. from 3)*

has been the subject of a thesis by Edward Pigeon, and work is ongoing.

The other effort consists of an analytic model called PORTZ whose purpose is to determine optimal dispatching rules. The queue is treated analytically in PORTZ, but only in equilibrium; that is, the delay is assumed to be indefinite. The intention is that WCPORT and PORTZ will be complementary, with PORTZ suggesting modifications to the dispatch rules of WCPORT, and with each serving as a verification tool for the other.

Optimum port security will require collaboration between all key parties. MIST is addressing the collaboration requirements for maritime domain awareness and security. It is currently sponsored by the Naval Postgraduate School's MDSRP and the Department of Transportation's Maritime Administration (MARAD). MIST was stood up in the summer of 2008 as a prototype program to help the federal maritime domain awareness effort incorporate the input of the private sector into the sharing of maritime threat information. The National Maritime Security Policy, the Intelligence Reform and Terrorism Prevention Act of 2004, and the National Strategy for Information Sharing have all called for increased participation by the private sector in improving maritime domain awareness. The MIST effort supports this call for action by facilitating cooperation between local, private sector stakeholders and federal stakeholders. Leveraging the private sector to enhance information sharing could result in a potential increase of resilient response to emergencies and disasters affecting critical maritime infrastructure.

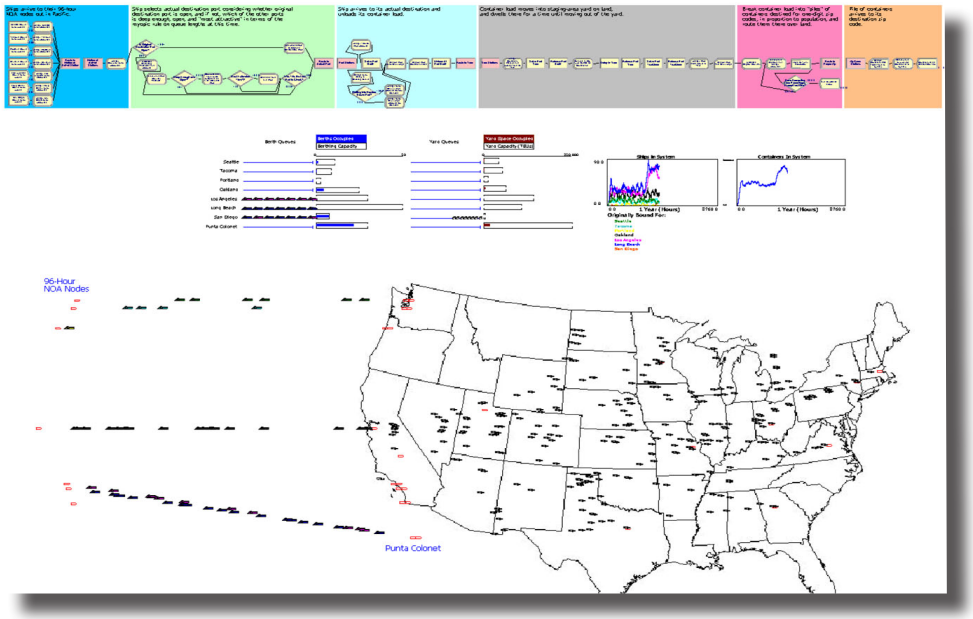


Figure 2. Screenshot of Arena simulation logic model (top flowchart) and animation (bottom) of west coast container-port operations. At the time of this screen shot, both the ports of Los Angeles and Long Beach were closed, so vessel traffic was being diverted to other ports, mostly the proposed port in Punta Colonet, Mexico.

Conceived as a multi-agency response, MIST worked closely in 2008 with the U.S. Coast Guard, MARAD, the Office of Global Maritime Situational Awareness (OGMSA), Global Maritime and Air Intelligence Integration (GMAII), Customs and Border Protection (CBP), and state and local government agencies to conduct a pilot workshop with private sector shipping at the Port of Long Beach/Los Angeles (LA/LB). The goal of the workshop was to prototype a process for uncovering private sector issues and solutions related to the sharing of threat information at the local level. The workshop was well received and provided actionable information regarding the general needs of the private sector. For example, the workshop delivered useful data about how to align private sector incentives with national strategy, leverage key local practices, streamline government interactions, collaborate with communities of interest, and improve information quality.

In May of 2009, MIST will look to address information sharing coordination and best practices in the Seattle/Tacoma maritime region. It will do so by replicating

(Continued on Page 18)

Port Security *(Cont. from 9)*

attack — instituting and installing measures that enhance resiliency, response, and rapid recovery. All of this contributes to port security while positively impacting the risk exposure to industry and those that insure them.

The CHSF Grant Approach

The Commonwealth Homeland Security Foundation (CHSF), using an innovative public-private approach, desires to contribute to the development and implementation of solutions that significantly improve the security of the commercial and military maritime port facilities in Hampton Roads against man-made or natural disasters. In particular, the protection and sustainability of the critical supply chain, intermodal facilities, and the workforce associated with the port region are key concerns.

To this end, the CHSF plans to award a series of grants to its university consortium members — George Mason University, Old Dominion University, The College of William and Mary, The University of Virginia, Virginia Commonwealth University, and Virginia Tech — to identify, develop, and implement effective and affordable solutions to enhance port security and the associated critical supply chain.

The CHSF is appealing initially to industry located in Virginia or others with interests in the Hampton Roads port security to fund the initial strategy grant. This should include the insurance industry that has a distinct interest in approaches that reduce the exposure of the port and its associated industry to terrorist attacks.

The initial grant will focus on optimal strategies to secure the Hampton Roads port region in a comprehensive manner. In developing those strategies, the CHSF will employ the research and development capacity of its university consortium members to work with stakeholders in the Hampton Roads region — including all industry sectors, maritime and related, as well as Federal, State, and local government — to craft a range of viable strategies to address port security.

When this is accomplished, the CHSF will assemble all stakeholders to further refine and "down select" the most achievable strategy and begin the process of follow-on grants to focus on the specific application of optimal solutions, including best practices and technologies, to secure the port of Hampton Roads, its critical supply chain, intermodal facilities, and its workforce from disruption. In doing so, the CHSF will serve as a strategic match-maker between Federal and State dollars and funding from the private sector to deploy strategies in a coordinated public-private partnership, thereby leveraging the resources, talent, and insight of those entities with a major interest in the security of the Hampton Roads port.

The strategies that the CHSF envisions pursuant to the initial research should draw on selected top-level strategic objectives for maritime security as outlined in *The National Strategy for Maritime Security*, September 2005. They include:

1. Preventing terrorist attacks and criminal hostile attacks;
2. Protecting maritime-related population centers and critical infrastructure; and
3. Minimizing damage from attacks and ensuring expedient recovery.

Conclusion

The vulnerabilities, risks, and consequences of an attack on our vital ports and critical supply chain — particularly on the Commonwealth's premier resource in Hampton Roads — are real, present, and dangerous to our economic well-being. The need for a public-private approach offered by the CHSF is essential to the development of a comprehensive strategy incorporating the best practices and available technology to secure our critical supply chain in and near maritime port facilities. Government lacks the funding to secure the critical infrastructure that largely resides in private hands. Private industry cannot afford a disruption in the flow of the critical supply chain and neither can governments — at all levels — that depend on industry and business viability.

(Continued on Page 18)

USCG *(Cont. from 11)*

communications room, "Mr. Rooney, I hear Sector North Carolina talking to a cruise ship that is taking on water and just ran aground in the Inter-Coastal Waterway (ICW)!" I remember thinking it was going to be a very busy day for North Carolina! As I walked over to the Command Duty Officer desk, I heard a radio transmission on channel 16 from North Carolina, "Captain, how many people are onboard your vessel?" The master replied "65 both crew and passengers total." I remember thinking the master seems very calm and under control. As I continued my walk to the CDO desk, I heard Sector North Carolina request the vessel's GPS position. Immediately, I noticed position as the master passed it to North Carolina. My thoughts were once North Carolina gains control of the situation, I will call and offer assistance or support. Before I could sit down and log onto the computer, I heard Mr. Rooney say, "Sir, the position they just passed plots in our Area of Responsibility." I immediately got up and walked over to him, "Where?" He replied, "Pungo, Virginia Beach area of the ICW." My first thought was, "How in the world, are we going to get 65 people off of that ship?" My adrenaline started to pump and I wondered if the other watch standers could hear my heart beat. I looked at Mr. Rooney and said, "Call District and request a helo and direct Station Portsmouth to launch." I remember thinking we needed to get someone on scene and quick! I immediately returned to the CDO desk and initiated the Critical Incident Communications (CIC) conference for a major marine casualty. The conference call for the CIC brief included personnel from Coast Guard Atlantic Area and Pacific Area Command Centers, and Coast Guard Headquarters Command Center, located in Washington, D.C. I briefed the case, "This morning at 0600 a cruise ship hit an object and is taking on water in the Inter-Coastal Waterway in the vicinity of Pungo which is in Virginia Beach, VA. Once the master noticed that he was taking on water at a rapid rate, he deliberately ran the ship aground. At this time, the Inter-Coastal Waterway is partially blocked to commercial and recreational traffic and there are 65 people onboard including the crewmembers. We have launched Air Station Elizabeth City to deliver pumps, as well as Station Portsmouth to control vessel traffic. The master of the vessel reports no injuries and the vessel is stable at this time." The Headquarters Command Center replied, "Sounds good, I want another brief in thirty minutes." Immediately I hung up the phone and briefed my Chain of Command. I discussed the possibility of a possible terrorist attack. Utilizing the Captain's COTP authorities, I directed a safety zone be established around the vessel, sent Coast Guard personnel on scene to interview the master of the cruise ship, and notified the Navy, Air Force, and Army of the incident. Once the first of the Coast Guard assets from Station Portsmouth arrived on scene, I directed them to get the passengers and non-essential crewmembers off of the cruise ship and to establish a 200 yard safety zone around the vessel. Shortly, marine units arrived on scene from Virginia Beach, Chesapeake, and Virginia Marine Police. Station Portsmouth crewmembers interviewed the master of the vessel and determined that this incident was not a deliberate attack. For the safety of the public and first responders, the Inter-Coastal Waterway was closed by the Captain of the Port from Alligator River Swing Bridge in Tyrrell County, NC, to the Great Bridge Locks in Chesapeake, VA. Once the safe evacuation of all passengers and crew was complete, the focus shifted to containing and stopping the pollution and finally un-grounding and repairing the cruise ship. After three days of conducting pollution clean-up, temporary repairs were made to the hull of the cruise ship and the vessel was re-floated at high tide and towed to a shipyard for permanent repairs. Less than a day later, the Army Corp of Engineers discovered a large submerged object in the channel that the cruise ship struck causing the vessel to take on water.

However many similarities there are between the human body and the SCC-J, there is one major difference: The SCC-J is not given time to recover from a long exhausting case, but must rebound instantly to be ready for the next maritime situation and response. The SCC-J must balance all port information and maintain maritime domain situational awareness at

(Continued on Page 18)

Port Security *(Cont. from 16)*

Insurance companies know, as they experienced after 9-11, that a major disaster confounds their ability to offer insurance products to businesses. This cooperative public-private partnership venture proposed by the CHSF to identify the right strategy to secure our ports is the best way to ensure that our security requirements for critical supply chain are addressed.

Moreover, when the Federal Government takes note of the commitment of this public-private venture, they will see the efficacy of the concept and will be more likely to bring Federal dollars to the application of effective solutions.

In the end, the CHSF approach to this problem provides a "win-win" strategy for both the public and private sectors while, most importantly, making it all the more difficult for our enemies to disrupt the economic viability so essential to our way of life. ❖

* *L. Scott Lingamfelter is the President of the Commonwealth Homeland Security Foundation (CHSF). After 28 years of active service with the U.S. Army, he retired as a Colonel in 2001. That same year, he entered another phase of public service as an elected member of the House of Delegates of the Virginia General Assembly, where he currently serves on the Appropriations Committee, the Education Committee, and the Militia and Public Safety Committee.*

NPS *(Cont. from 15)*

the workshop process from LA/LB, enhancing the social network tool hosted by MARAD on MarView, and completing a field study to capture "a day in the life" of a facility security officer working in the private maritime industry as it relates to information sharing. The notion of MIST is that a better understanding of the private sector network and perspective on maritime security, paired with a more solid bridge for communication and collaboration with government, will result in a more resilient port environment.

This article highlights only a small sampling of the more than 25 different Maritime Defense and Security Research Programs currently on-going at NPS. In addition, the MDSRP publishes a monthly e-newsletter, the SITREP, which is a collaborative venue to highlight not only NPS research, but maritime-related research of all agencies, research labs, industry, and other stakeholders interested in Maritime Defense and Security issues. If you wish to receive the SITREP, or have any questions regarding this article, please contact Ms. Rita Painter at rpainte@nsp.edu. ❖

USCG *(Cont. from 17)*

all times. The Operational Commander uses the SCC-J as a command and control platform to coordinate missions to achieve operational effectiveness and strive to guarantee port safety and security. ❖

Upcoming Conference Reminder

The CIP is co-hosting, with the Security Analysis and Risk Management Association (SARMA), the 3rd National Conference on Security Analysis and Risk Management from June 16-18, 2009, in Arlington, VA.

Confirmed Keynote Speakers include:

- Mr. Peter F. Verga, Principal Deputy Under Secretary of Defense for Policy
- Ms. Tina Gabbrielli, Director of the Office of Risk Management and Analysis, U.S. Department of Homeland Security
- Mr. Roger W. Cressey, President of the Good Harbor Consulting Group and former Director for Transnational Threats on the National Security Council

For additional information, to include Agenda, Early Bird Registration (ending May 1st), Sponsor and Exhibitor prospectus, please visit http://sarma.org/events/pastevents/3rdannualconferenc/.

Release of Paper on Regional Risk Analysis

Complementing CIP's efforts on risk, to include co-hosting the Security Analysis and Risk Management Association's annual conference and past publication of a risk monograph, CIP recently posted a paper on its website addressing the topic of regional risk analysis. Authored earlier this year by Liz Jackson of the Federal Emergency Management Agency's Office of National Capital Region Coordination (NCRC), William McGill of The Pennsylvania State University, and Chris Geldart of the URS Corporation and former Director of NCRC, "Regional Risk Analysis: A Coordinated Effort" discusses the analysis of homeland security risk in a multi-jurisdictional environment and offers insight on key considerations of strategic risk analysis. The paper abstract is below.

Risk assessments are being conducted more frequently as localities seek to enhance their preparedness and mitigate and manage risk with regard to all-hazard events. In the National Capital Region (NCR), a risk analysis was recently conducted that built on previous assessments and further contributes to a regional risk picture. This paper describes the development of the 2008 NCR Strategic Hazards Identification Evaluation for Leadership Decisions (NCR SHIELD) regional risk analysis, which includes both a risk assessment and strategic approach to risk management. It begins with a discussion of the difficulties that must be overcome to ensure executive decision makers align their thinking and pursue a common goal of assessing regional risk to inform their decision-making processes and, in turn, how they mitigate and manage risk at the strategic level. The paper concludes with information on the conduct of NCR SHIELD and outlines a stakeholder-engaged process for further developing a multi-jurisdictional approach to risk management.

The full paper is available on the CIP website at http://cip.gmu.edu/research/Regional_Risk_Analysis.php.

Transportation *(Cont. from 7)*

international maritime commerce. The total estimated cost of this closure was $500M - $1B.

Section II: Trade Resumption/ Resiliency Plan (TR/RP) - Building Resiliency into the MTS

Examples such as the 2008 Hurricanes and the Mississippi River oil spill previously discussed illustrate the importance of immediate response and recovery operations to support an effective recovery of the MTS. It also illustrates the role that contingency planning plays in preparing for these high-consequence events. Considering the economic costs and the unpredictable nature of waterway and port closures, it is of vital importance to the economic security of the United States that alternatives to this transportation segment are analyzed and appropriate response and planning doctrines developed.

A security program focused on layered initiatives, programs, and cooperative work with stakeholders throughout the international supply chain provides the greatest flexibility and support to reduce the chances of a breach in the security network. A holistic supply chain strategy can help reduce the risk of disruptions at the marine ports, or even while the vessel is at sea where it can be vulnerable to pirate attacks or other incidents prior to reaching its destination. An important component of a holistic risk management framework is the development and implementation of a Trade Resumption/Resiliency Plan (TR/RP), as well as other strategic risk management plans and response and recovery programs.

The TR/RP is an important component of the DHS Port Security Grant Program (PSGP) that is designed to identify initiatives that would aid the preparedness of regional port communities by adding resiliency in the basic systems that support port commerce and trade. The TR/RP supports and complements other strategic maritime regional planning activities, including the Area Maritime Security Plan (AMSP), the Area Contingency Plan (ACP), and the Strategic Risk Management Plan (SRMP) and others as highlighted in the figure below.

The goal behind these initiatives is to build resiliency into the MTS by identifying gaps in security, authorities, capabilities, capacities, competences and partnerships across the security continuum of awareness, prevention, protection, response and recovery. These efforts can enhance the system's ability to operate under normal conditions, and improve its capability to address a Transportation Security Incident (TSI) or an Incident of National Significance (INS).

As Figure 1 below highlights, following a TSI or an INS, performance of the port (i.e. measured by container throughput or other productivity measures) will be impacted during the immediate response stage as well as in the early recovery stages. Response and immediate MTS recovery is usually led by government entities, such as the U.S. Coast Guard's efforts previously mentioned, with the assistance of the private sector and begins within 1-3 days of the event and last for 90 days or longer. Resumption of trade is primarily a function of the private sector who

(Continued on Page 21)

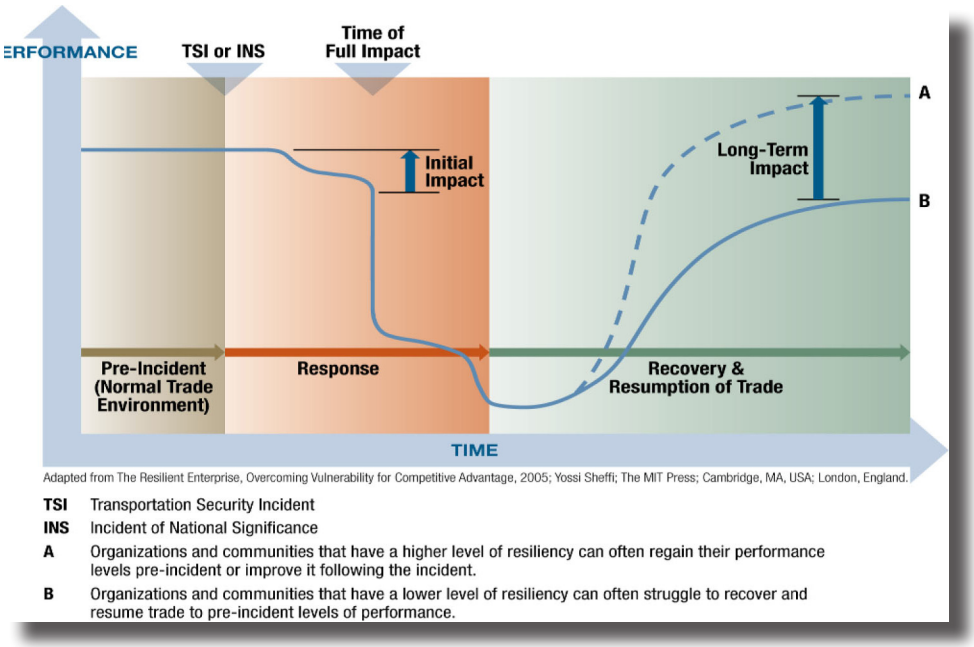


Figure 1. Conceptual Framework for Response and Resumption of Trade Following a TSI or INS

Transportation *(Cont. from 20)*

own most of the assets and can take months to years.

Section III: The Experience of the Lower Mississippi River (LMR)

Evidence of the implementation of this national strategy can be found in the planning work recently completed in the Lower Mississippi River (LMR). The Ports in the LMR[5] are a critical gateway for imports and exports for the United States, especially for food products, petroleum products, and chemicals. To increase the resiliency of the LMR MTS, which extends from Baton Rouge to the Gulf of Mexico, the LMR Ports joined forces to form the Port-Wide Strategic Security Council (PSSC). The PSSC has launched some important initiatives to increase its preparedness position and collaborate on security grant applications. One of the activities the PSSC has commissioned is a Trade Resumption and Resiliency Plan (TR/RP) to identify gaps in the current LMR operating environment and to identify respective capital investments and initiatives that can help to address the critical institutional and planning, waterway, and landside issues in the region.

With the support of DHS, the Ports of the LMR, and others across the U.S., are increasing coordination with regional, local, and federal agencies and the private sector to enhance its capabilities to protect the MTS. Under the leadership of the U.S. Coast Guard, local law enforcement agencies, and other key sector stakeholders, it is also enhancing system-wide situational awareness and communications capabilities to detect, deter, mitigate, respond, and recover from disruptive events such as the ones discussed in this article or other high consequence events.

As the nation prepares to implement the American Recovery and Reinvestment Act 2009 Projects, it will be important for the MTS stakeholders to continue to coordinate closely so that competing demands don't distract resource allocation and attention from the critical infrastructure and key resources essential for trade and the economic well-being of our nation. The focus for future transportation investments needs to be on smart infrastructure that leverages technology and adds redundancy, capacity, flexibility, and control into the transportation system to ensure the nation's competitiveness, as well as safe and secure supply chain operations. ❖

Figure 2. Ports of the Lower Mississippi River (LMR)

[5] The LMR Ports includes the Port of South Louisiana, Port of New Orleans, the Greater Baton Rouge Port, the Plaquemines PHT District, and the St. Bernard PHT District.

The Center for Infrastructure Protection works in conjunction with James Madison Univerity and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems, and economic processes supporting the Nation's critical infrastructure. The Center is funded by a grant from the National Institute of Standards and Technology (NIST).

If you would like to be added to the distribution list for *The CIP Report*, please click on this link:
http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1