Ensuring Maritime Commerce: GAO Reviews of Resilience and Ports

Stephen L. Caldwell
Director, Maritime Security Issues
U.S. Government Accountability Office

Ensuring a Resilient Maritime Transportation System
The Transportation Research Board
National Academies of Science
Washington, DC, June 24, 2014

AGENDA

- Background
- National Level
- Department Level
- Port Level
- Facility Level
- Questions & GAO Contact

BACKGROUND

Importance of U.S. Ports

- Ports contain many types/sectors of critical infrastructure
- More than 95% of non-North American foreign trade arrives through U.S. ports
- Ports are major centers for chemical and petroleum production activities
- There are 17 strategic ports necessary for major military deployments
- Many ports feature important national symbols (e.g., the Statue of Liberty)
- Recreation is a central feature of many ports

BACKGROUND

Vulnerability of U.S. Ports

- Ports are extensive in size, and are accessible by water, land, and air
- Many ports are intertwined with major urban areas
- Ports process a large volume of cargo, passengers, and hazardous materials
- Ports are a hub of activity for multiple transportation modes
- Many vessels move through ports with relative anonymity
- Cargoes move quickly due to just-in-time delivery systems

BACKGROUND

Port Threats and Possible Scenarios

- Generally no known, credible threats in US, but overseas attacks have occurred:
  - USS Cole attack, Yemen
  - Limberg Attack, Yemen
  - Ferry Attack, Philippines
  - Khawr Al Amaya Oil Terminal, Iraq
- Possible U.S. Threats Include:
  - Entry point for terrorists or dangerous contraband (e.g., WMD)
  - Waterside facilities or port infrastructure could be attacked via small boat, or other means
  - Possible targets include cruise ships, passenger ferries, military vessels and infrastructure

BACKGROUND

Legislation

- The Maritime Transportation Security Act (MTSA) of 2002, passed to protect the nation's ports and waterways by requiring a wide range of security improvements, many led by U.S. Coast Guard (USCG):
  - Conducting vulnerability assessments for port facilities and vessels
  - Developing Area Maritime Security Plans to identify and mitigate risks
- The SAFE Port Act of 2006, modified existing legislation and created and codified new programs and requirements:
  - Addition of Salvage Response Plans to clear waterways and reestablish port commerce to Area Maritime Security Plans

BACKGROUND

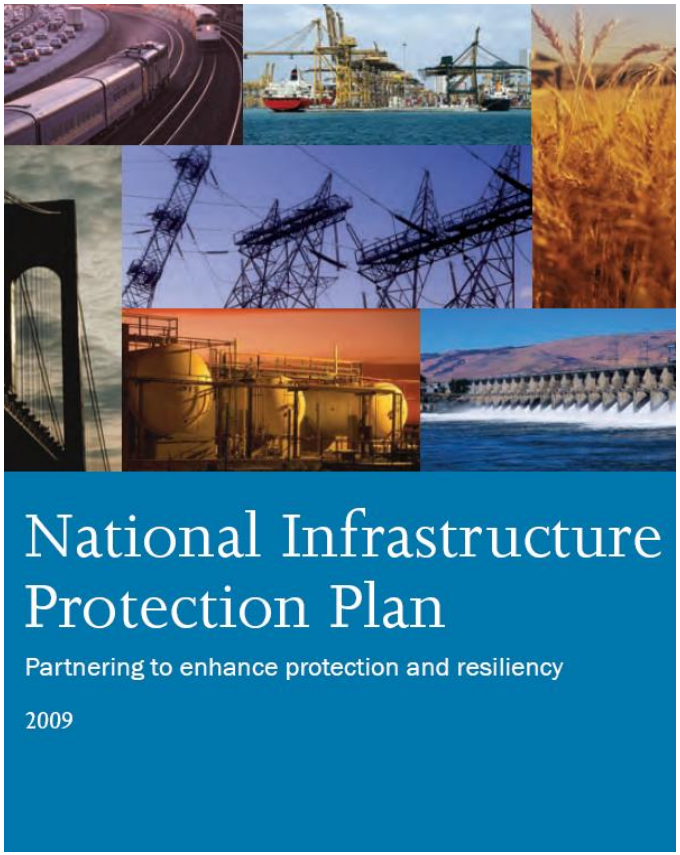
U.S. Government Accountability Office (GAO)

- GAO is an independent, nonpartisan agency that works for the U.S. Congress
- The GAO mission is to support the Congress in meeting its oversight responsibilities and to help improve the performance and ensure the accountability of the federal government
- GAO evaluates how the federal government manages programs and spends funds.
- Regarding maritime issues, since 9/11, GAO has issued over 75 reports on maritime and supply chain security

NATIONAL LEVEL

National Infrastructure Protection Plan (NIPP)

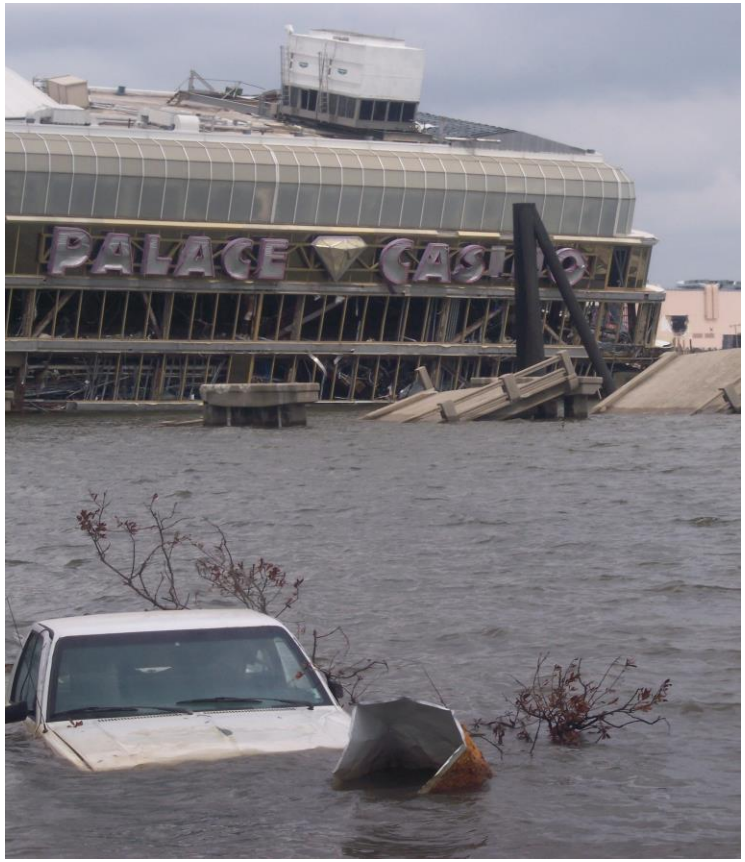
- The NIPP provides the framework for developing and implementing a coordinated national effort to manage the risk to critical infrastructure
- The NIPP outlines the roles and responsibilities of security agencies and partners, including DHS and State
- The NIPP designates 16 critical infrastructure sectors and assigns a Sector Specific Agency (SSA)—a federal department or agency—to each sector responsible for leading CISR activities
- The 2009 NIPP defined resilience as the ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions



NATIONAL LEVEL

GAO Review of Resilience in National Planning

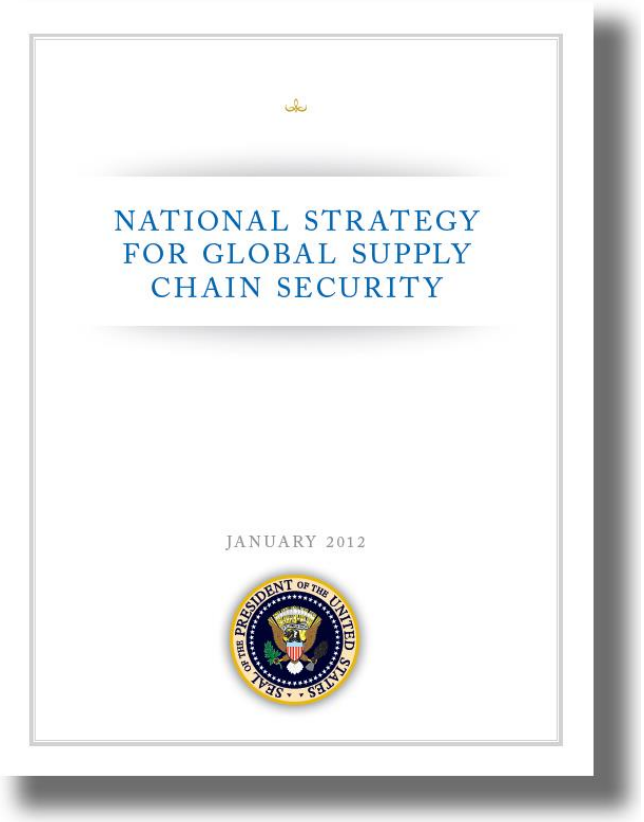
- GAO reviewed the NIPP and efforts to define and promote resilience of critical infrastructure (GAO-10-296)
- The NIPP increased its emphasis on resiliency and treated resiliency as a separate concept on par with protection
- The emphasis on resilience was to encourage system-based sector and cross-sector activities on a broader set of risks (terrorism + natural disasters)
- DHS provided guidance on how SSAs were to update their sector plans to integrate DHS's all-hazards approach to protection and resilience
- GAO found that both the national plan and some sector-specific plans had been revised to incorporate resilience



NATIONAL LEVEL

National Strategy for Global Supply Chain Security

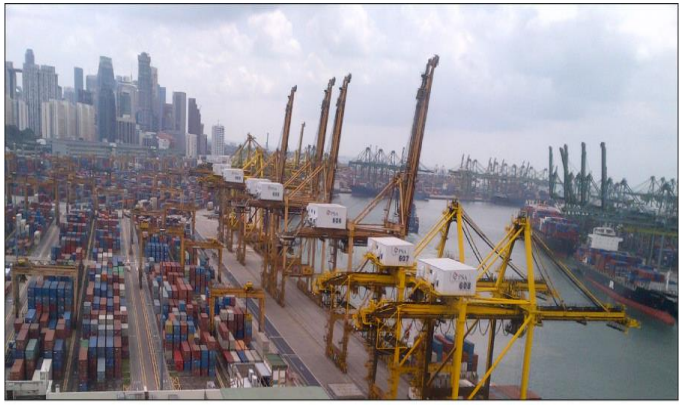
- Released in January 2012 by the White House, the Strategy establishes the nation's policy to strengthen the worldwide systems that sustain the movement of goods
- The second of the two goals is to foster a resilient supply chain by:
  - developing a resilient supply chain that is prepared for and can recover rapidly from all-hazards
  - a risk-informed approach for DHS's cargo security programs across all modes of transportation



NATIONAL LEVEL

GAO Review of The Global Supply Chain Strategy

- GAO reviewed the strategy, including CBP's Container Security Initiative (CSI) that uses U.S. officers in foreign ports to identify and examine cargo container shipments that could pose a high risk such as WMD (see GAO 13-764)
- GAO found that CBP has not regularly assessed the risks of foreign ports to the U.S. to compare to its CSI global footprint in ports (it had not done so since 2005)
- GAO found that CSI did not have presence at half of the ports considered high risk, and one fifth of existing CSI ports were low risk
- GAO recommended that CBP periodically assess the supply chain security risks from foreign ports and use the results to inform future expansion of or changes to CSI ports



Source: GAO.

DEPARTMENT LEVEL

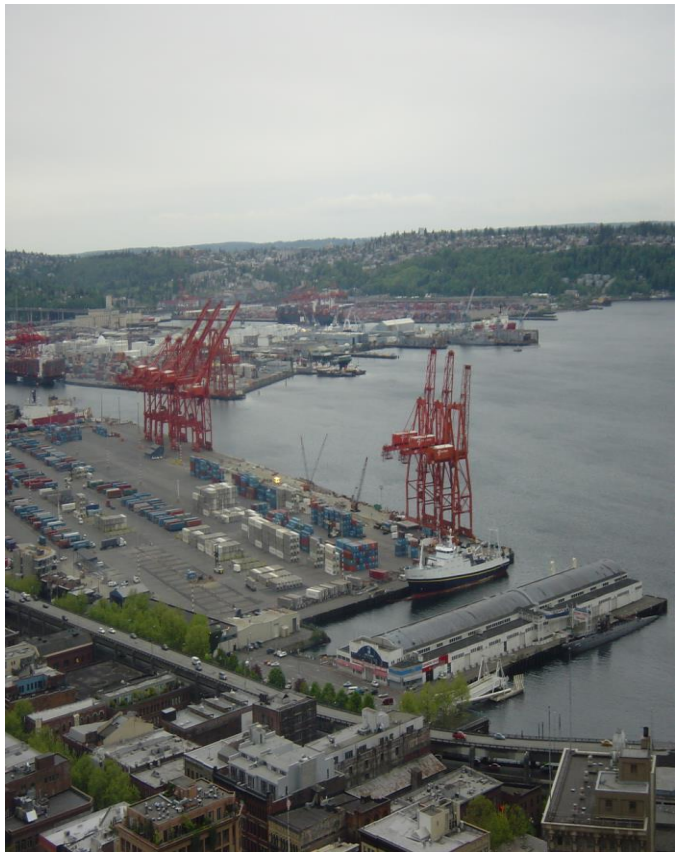
DHS Resilience Efforts

- Since 2009, DHS has emphasized resilience by developing a resilience policy, and creating two internal entities—the Resilience Integration Team (RIT) in 2010 and the Office of Resilience Policy (OPR) in 2012
- Officials state the policy provides agencies with a single, consistent, department wide understanding of resilience
- RIT develops and disseminates resilience initiatives, through coordination with subject matter experts and all resilience related components
- ORP coordinates and promulgates resilience strategies throughout the department

DEPARTMENT LEVEL

GAO Review of DHS Resilience Efforts

- GAO reviewed DHS's coordination of resilience efforts across ports and other infrastructure (GAO-13-11)
- DHS high-level documents promote resilience, and DHS developed a resilience policy
- However, DHS officials could not provide details on how its components might implement the resilience policy
- GAO recommended DHS develop an implementation strategy that defines goals, objectives, and activities could help ensure consistency, efficiency, and shared prioritization in the adoption of the policy, as well as, promote concrete steps and accountability by components



DEPARTMENT LEVEL

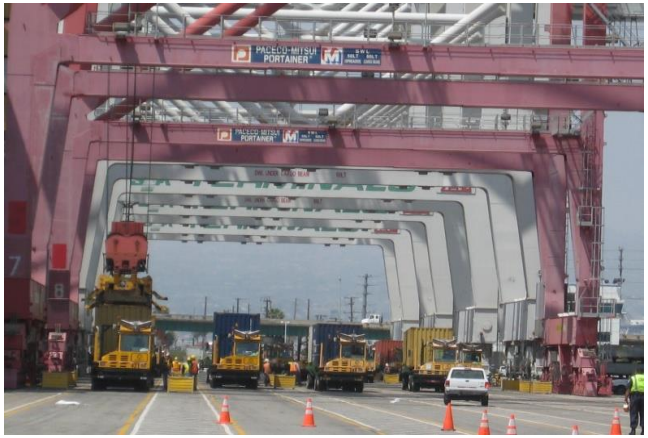
Regional Resiliency Assessment Program (RRAP)

- RRAP consists of assessments, conducted by DHS officials, that allow for an analysis of infrastructure clusters and systems in various regions
- This program has included ports as part of a transportation system or larger regional system, but has not focused on just a port
- GAO reviewed the RRAP (GAO-13-616) and found that DHS was not measuring whether resiliency had improved for individual assets that participate in RRAP
- GAO recommended that DHS develop a mechanism to measure whether asset owners and operators who participate make improvements based on the RRAP

DEPARTMENT LEVEL

GAO Review of DHS and Port Resilience

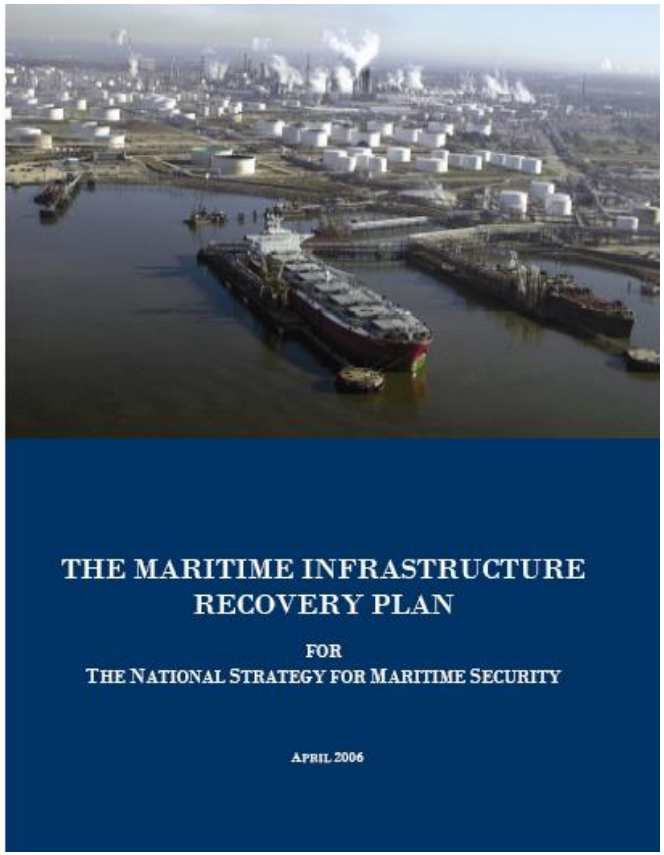
- GAO reviewed DHS's coordination of resilience efforts across ports and other infrastructure (GAO-13-11)
- DHS component agencies, such as the Coast Guard, have opportunities to collaborate and leverage existing tools to assess port resilience
- GAO found that the Coast Guard and IP work with stakeholders to address some aspects of resilience but they could take additions actions to promote portwide resilience
- GAO recommended Coast Guard and IP could leverage the RRAP approach to develop assessments of the overall resilience of one or more specific port areas



PORT LEVEL

U.S. Coast Guard Planning for Recovery

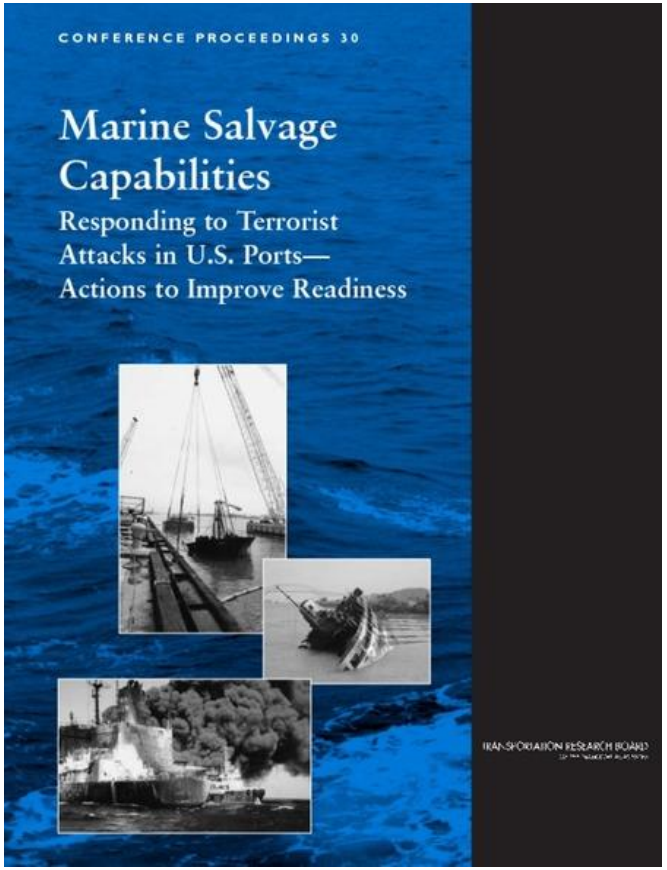
- In addition to the MTSA and SAFE Port Act, the Coast Guard Authorization Act of 2010 further reinforced the need for response and recovery planning and protocols in Area Maritime Security Plans
- Coast Guard provides recovery planning guidance to ports within the Maritime Infrastructure Recovery Plan on:
  - Identification of recovery priorities
  - Development of pre-incident baseline data and development and dissemination of Essential Elements of Information
  - Establishment of maritime transportation system recovery units



PORT LEVEL

U.S. Coast Guard Planning: Salvage

- As mandated by the SAFE Port Act, Area Maritime Security Plans must include a Salvage Response Plan to ensure salvage activities and to identify available resources to support clearing of waterways and restoration of commerce flow
- Coast Guard provides salvage planning guidance to ports on:
  - Roles and responsibilities of federal, state, and local partners
  - Recovery-specific tasks to identify salvage response needs
  - Identification of local marine salvage providers for use when needed



PORT LEVEL

Marine Transportation System Recovery Unit (MTSRU)

- An MTSRU is a collection of maritime personnel, led by the Coast Guard, established during a transportation security incident to provide support
- MTSRU is responsible for tracking and reporting status information, understanding critical recovery pathways, recommending courses of action, serving as a venue for input to the local response organization, and recommending recovery priorities
- The specific responsibilities of a MTSRU can vary by port area, as some port areas are more able to leverage information-sharing abilities of established collaborative bodies

PORT LEVEL

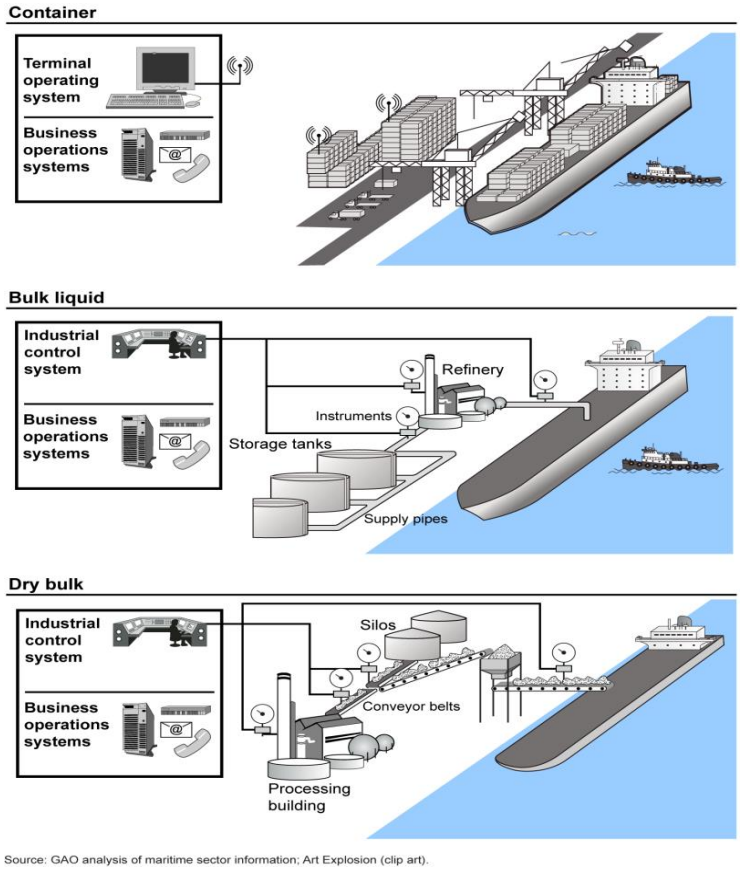
GAO Review of USCG Port Recovery and Resilience

- GAO reviewed USCG port recovery planning (GAO-12-494R)
- GAO found port level recovery planning met key requirements of the SAFE Port Act and USCG guidance, such as establishing MTSRUs, identifying essential elements of information, setting priorities, and developing salvage response plans
- But recovery is just one aspect of resiliency, and USCG authority under MTSA is limited to shore side facilities and infrastructure
- In a follow-up report (GAO-13-11), GAO recommended development of a resilience implementation strategy, and increased collaboration among DHS port security components

FACILITY LEVEL

Cybersecurity as an Emerging Resiliency Issue

- Critical infrastructure has become increasingly interconnected with and dependent on cyber-systems
- The operation of ports are supported by information and communication systems.
- The NIPP and Presidential Directives-7 & 21 set forth frameworks to address the risks posed by cyber threats
- USCG is responsible for maritime security and the assessment of maritime security risks



Source: GAO analysis of maritime sector information; Art Explosion (clip art).

FACILITY LEVEL

Cyber Threats: Actors and Types

- Threats come from a wide array of sources:
  - Bot-network operators
  - Business competitors
  - Criminal groups
  - Hackers
  - Insiders
  - Foreign Nations
  - Phishers
  - Spammers
  - Spyware or malware authors
  - Terrorists
- These types of cyber threats may can adversely affect information and communications networks:
  - Denial of service
  - Distributed denial of service
  - Phishing
  - Trojan Horse
  - Virus
  - Worm
  - Exploits affecting the information technology chain

FACILITY LEVEL

Port Cybersecurity Incident in Europe

- In June 2013, Belgian and Dutch authorities reported that drug smugglers had employed professional hackers to conduct criminal operations
- The criminal group successfully smuggled 1,044 kilos of cocaine and 1,099 kilos of heroin through the port of Antwerp on to the Netherlands
- The hackers emailed trojan horses and installed key stroke logging devices to capture passwords, allowing them to gain control of the port computers and terminal operating system
- The criminals were then able to monitor “their” container, and unload it at a time and location of their choosing, avoiding normal port staff

Europol Public Information

EC3 EUROPOL

The Hague, June 2013
Intelligence Notification 004-2013

CYBER BITS

Hackers deployed to facilitate drugs smuggling

What happened?

On 17 June Belgian and Dutch authorities reported on arrests made in a drugs investigation. The members of the criminal group smuggled drugs through the harbour of Antwerp to The Netherlands. A dozen suspects have been arrested and 1 044 kilos of cocaine as well as 1 099 kilos of heroin have been seized. What's interesting is that the criminal group used hackers to access the computer systems of harbour companies and container terminals.

How does it work?

Using hackers, the criminals took control of the computers of two container terminals and of a harbour company. The approach was twofold:

- Classic intrusion by sending mails with attachments containing Trojans to staff members;
- Breaking into offices to install key logging devices to capture passwords.

Once the computers were under their control, the group could follow "their" container and upon arrival, unload it to a location and at a time of their choosing. This in return enabled the criminal group's drivers to access the container before the normal harbour staff would.

The investigation discovered that the intrusion mails were sent from a Dutch IP address. The stolen data were forwarded to a server owned by the criminal group.

Why do you need to know?

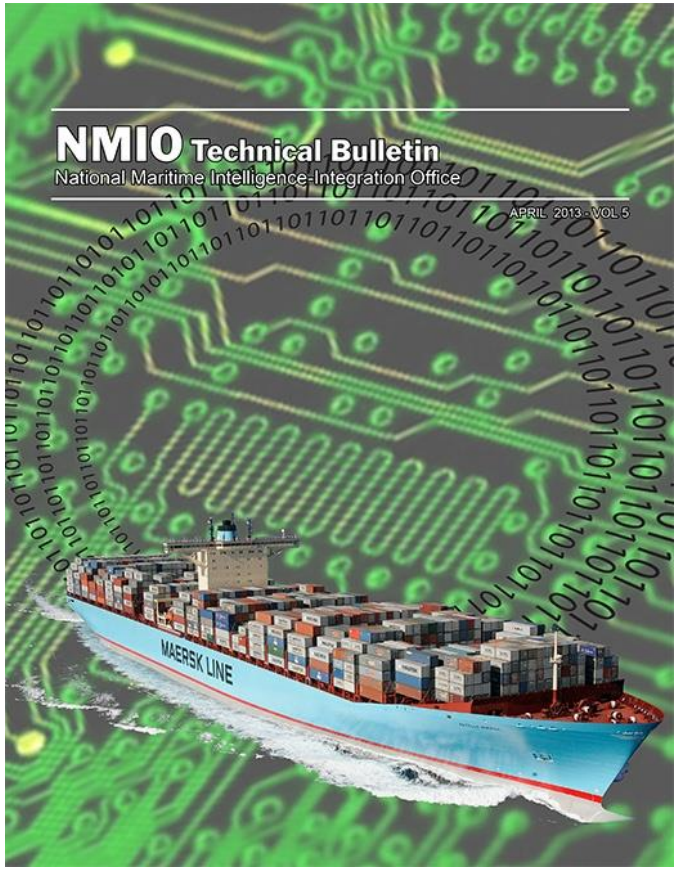
- It's one of the first times this modus operandi has been revealed;
- The criminal group was professional and well-connected as demonstrated by the amounts of drugs seized. It can be assumed that their modus operandi has been shared with other criminal groups who will try to do the same in other ports and airports;
- Europol currently has no view on the cyber resilience of cargo companies and container terminals in harbours. We suggest evaluating the cyber security situation for the various companies involved in cargo handling, especially in the big harbours. The focus should be on the risks and vulnerabilities of the different actors involved. Awareness has to be raised that for instance signs of a burglary should not be ignored. The use of short term contractors from different companies might also increase the risk of infiltration.
- EC3 would welcome reactions on this note. Please mail to O31@europol.europa.eu.

1

FACILITY LEVEL

GAO Review of Port Cybersecurity

- GAO reviewed federal maritime cybersecurity efforts (GAO 14-459)
- GAO found DHS and other federal stakeholders only took limited steps
- The National Maritime Strategic Risk Assessment (2012) & Area Maritime Security Plans did not address cyber
- USCG had some mechanisms for sharing security-related information, but the use of these mechanisms for cybersecurity-related information varied
- GAO recommended that USCG assess cyber related risks, and use this to inform its maritime security regime
- Other studies raised similar concerns about the maritime industry in USA, Europe, Australia (see backup slides)



QUESTIONS AND GAO CONTACT

Questions?

Stephen L. Caldwell, (202) 512-9610, email: caldwells@gao.gov

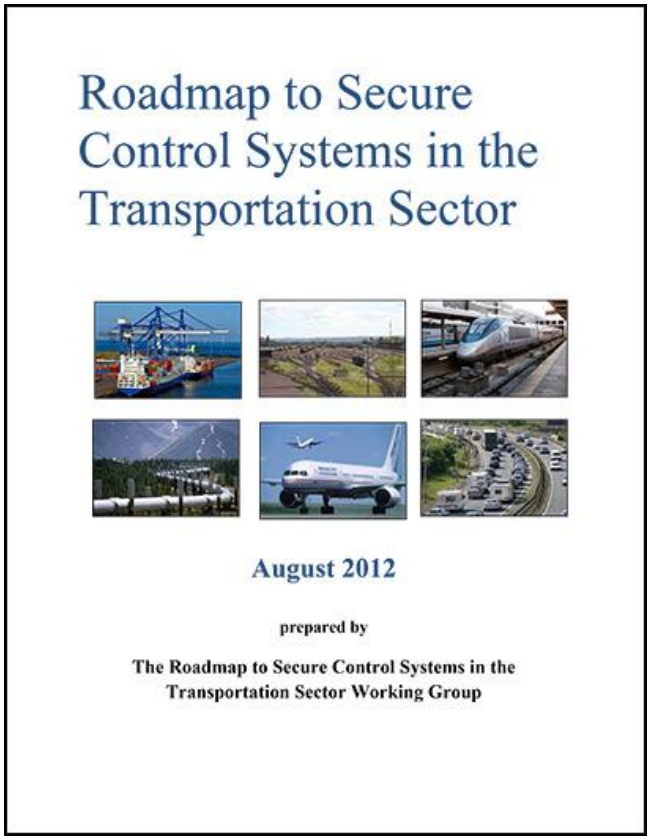
GAO website: www.gao.gov

COPYRIGHT

CYBERSECURITY THREATS

U.S. Roadmap to Secure Control Systems

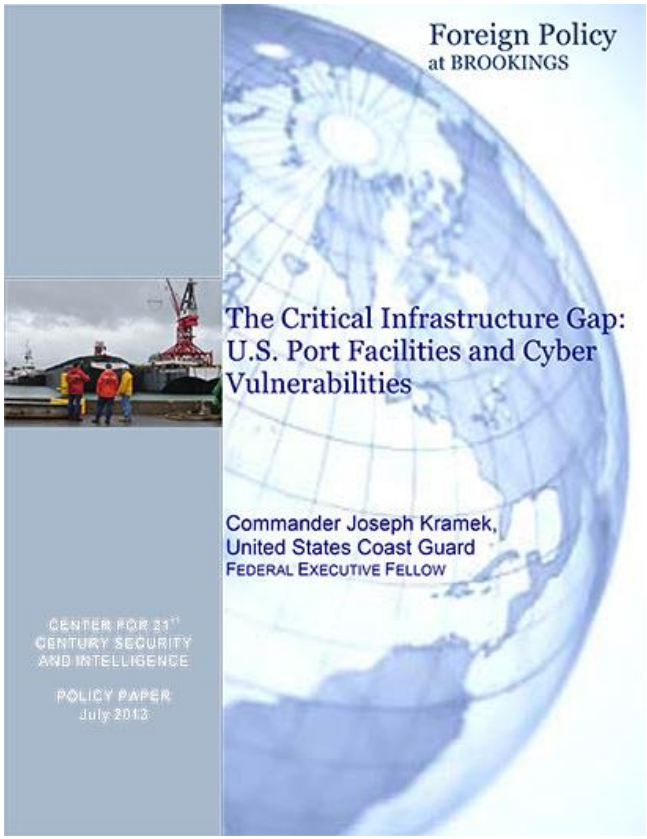
- *Roadmap to Secure Control Systems in the Transportation Sector*, Aug. 2012
- Working group facilitated by DHS, National Cybersecurity Division, Control Systems Security Program
- Maritime terminal security involves the use of types of systems for communications, sensors, and command and control
- Pipelines, probably more than any other mode of transportation, is reliant on control systems for its operations
- Industry is migrating toward a more connected control infrastructure and is thus increasingly vulnerable to attacks on its control systems



CYBERSECURITY THREATS

Brookings Institute Policy Paper

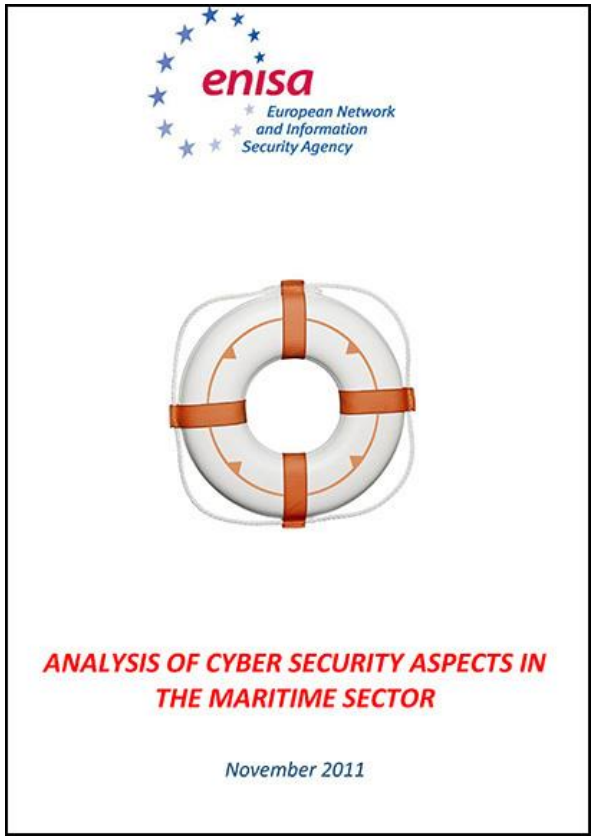
- *The Critical Infrastructure Gap: U.S. Port Facilities and Cyber Vulnerabilities*, July 2013
- Brookings Institution, Center for 21st Century Security and Intelligence
- The level of cybersecurity awareness and culture in U.S. maritime facilities is relatively low; cybersecurity hygiene is not being practiced
- Complex networked logistics management systems undergird the global flow of maritime commerce
- Recommendations, including to industry re: vulnerability assessments and response plans



CYBERSECURITY THREATS

European Analysis

- *Analysis of Cyber Security Aspects in the Maritime Sector*, Nov. 2011
- European Network and Information Security Agency (ENISA)
- Maritime activity increasingly relies on info communications and technology to optimize navigation, propulsion, and traffic control
- Cyber threats a growing menace, potentially "disastrous consequences" for EU ports
- Awareness on cybersecurity needs in the maritime sector is low to non-existent
- Current maritime governance considers only physical security, and is fragmented
- Recommendations on governance & cooperation



CYBERSECURITY THREATS

Australian Government Inquiry

- *Offshore Oil and Gas Resources Sector Security Inquiry*, June 2012 (pages 107-110)
- Department of Infrastructure and Transport, Office of the Inspector of Transport Security
- Cyber security… an increasingly serious issue for offshore oil and gas facilities
- Cites attackers targeting global oil, energy, and petrochemical companies, with intent to steal sensitive info such as operational details
- Reliance on external supervisory control of facilities creates new and additional threats, which need to be understood and mitigated
- Recommendations on cyber security governance and practices