Comparing Results of Maritime Cybersecurity Studies from Selected Countries

Stephen L. Caldwell
Former Director, Maritime and Supply Chain Security Issues at the U.S. Government Accountability Office

CCICADA Maritime Cybersecurity Conference
Rutgers University, NJ / March 2-3, 2015
AGENDA

• Background
• Cyber Systems
• Cyber Threats
• Cyber Studies
• Comparing Studies
• Questions & Contact Info
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 about 100 reports on maritime and supply chain security
- Stephen L. Caldwell was the director in charge of the maritime and supply chain security portfolio from 2006-2015
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 by U.S. Coast Guard (USCG) and industry.

Presidential Policy Directive (PDD) 21, sets forth a unified strategy to address the all-hazards risks posed to critical infrastructure.

The National Infrastructure Protection Plan (NIPP) set up a framework to address cyber risks, information sharing, and development of sector plans.

Executive Order (EO) 13636 requires enhanced information sharing with the cyber private sector, prioritization of cyber security actions, and identification of cyber risks.
CYBER SYSTEMS
Importance of Cyber Systems

• The NIPP, PPD, and EO place increasing emphasis on addressing both physical and cyber protection of infrastructure in an integrated fashion

• Maritime critical infrastructure has become increasingly interconnected with and dependent on cyber systems

• The operations of ports are supported by information and communication systems, such as
  • Terminal Operating Systems (slide 6)
  • Business Operations Systems (slide 6)
  • Industrial Control Systems (slide 7)
  • Access Control and Monitoring Systems (slide 8)
CYBER SYSTEMS
Terminal and Business Operating Systems

- Terminal operating systems are information systems used by terminal operators to control container movements and storage.
- Business operation systems are information and communications technologies used to help support the business operations of the terminal, such as communicating with customers and preparing invoices.

Source: GAO analysis of maritime sector information; Art Explosion (clip art).
Industrial control systems are automated systems used to control industrial processes such as manufacturing, product handling, production and distribution. These systems are used to operate motors, pumps, valves, signals, lighting, and access controls, and to facilitate the movement of goods throughout maritime terminals using conveyor belts or pipelines.
Access control and monitoring systems are information and communication technologies that support physical security operations. These systems include camera surveillance systems that can be connected to information system networks to facilitate remote monitoring of port facilities, and electronically enabled physical access control devices.
CYBER THREATS
Cyber Threat Actors

- 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 adversely affect information and communications networks:

- Denial of service
- Distributed denial of service
- Phishing
- Trojan Horse
- Virus
- Worm
- Exploits affecting the information technology chain

For expanded view of this graphic, see GAO-07-705, p.6
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.

By the Transportation Sector Working Group (TSWG), created by DHS, National Cybersecurity Division, Control Systems Security Program

Approach: government and industry experts developed goals, objectives, metrics and milestones to measure cybersecurity posture in the transportation sector over 10 years

Scope: limited to all U.S. transportation modes, therefore few specifics on maritime (which are generally descriptive of that mode)

Recommendations: to implement the roadmap through buy-in, action plans, prioritize actions, and communicate results
• Title: *The Critical Infrastructure Gap: U.S. Port Facilities and Cyber Vulnerabilities*, July 2013

• By the Brookings Institution, Center for 21st Century Security and Intelligence

• Approach: case studies using interviews with variety of stakeholders, analysis of grant programs and funding, and literature review

• Scope: included 6 diverse ports in U.S., focusing on port facilities; not vessels

• Recommendations: to Congress, DHS, USCG, FEMA and industry re: assessing requirements and resources, determining vulnerabilities, and developing response plans
Title: Maritime Critical Infrastructure Protection: DHS Needs to Better Address Cybersecurity, June 2014

Joint by GAO’s Information Technology and Homeland Security and Justice Teams

Approach: used MTSA, PDD, EO and NIPP as criteria to assess DHS progress

Scope: port facilities covered by the U.S. MTSA statute; also included Port Security Grant Program; did not include vessels

Recommendations: to USCG and FEMA regarding risk assessments, threat information sharing, and expertise used to assess grants
Title: *Analysis of Cyber Security Aspects in the Maritime Sector*, Nov. 2011

By the European Network and Information Security Agency (ENISA)

Approach: conducted desk research of literature, review of regulations, conducted interviews and questionnaires, and held a validation workshop

Scope: the maritime sector in Europe, such as port facilities (and possibly vessels), with some review of international governance issues

Recommendations: to raise awareness, develop strategies, define roles and responsibilities, develop standards, conduct training, consider regulations, harmonize international & EU actions
CYBER STUDIES
Australian OITS Government Inquiry

• Title: Offshore Oil and Gas Resources Sector Security Inquiry, June 2012 (pages 107-110)

• By Dept. of Infrastructure and Transport, Office of the Inspector of Transport Security (OITS)

• Approach: review of international and Australia legal and regulatory regimes, interviews with government and industry, including site visits to offshore facilities (and U.S., U.K., and Norway)

• Scope: examined Australia’s maritime oil and gas sector (focusing on offshore infrastructure); cyber was only one of many components examined

• Recommendations: (re: cyber) training at both the executive and operational level, conduct exercises, and examine other improvements
COMPARING STUDIES
Making Comparisons and Common Themes

• It is difficult to make direct comparisons due to differences in the studies’ purpose, scope, methodology and organization
• However, they have common themes that reinforce areas of concern and needed action:
  • Maritime operations are growing more automated and interconnected
  • Stakeholder awareness of cyber threats and their cyber hygiene has been weak
  • Vulnerabilities exist, with potentially harmful consequences to ports
  • Risk assessments to date have generally focused on physical (not cyber) security
  • Threat information sharing is ad hoc and needs to be improved
COMPARING STUDIES
Maritime Environment

- Maritime operations are growing more automated and interconnected
  - Complex networked logistics management systems undergird the global flow of maritime commerce (Brookings)
  - Maritime activity increasingly relies on info communications and technology to optimize navigation, propulsion, and traffic control (ENISA)
  - SCADA systems are used to control all operational aspects, including remote operations, of ship-to-shore and rail-mounted gantry cranes, at marine ports and terminals (TSWG)
  - Current maritime governance is fragmented among various stakeholders (ENISA)
COMPARING STUDIES
Awareness and Hygiene

• Stakeholder awareness of cyber threats and their cyber hygiene has been weak
  • The level of cybersecurity awareness and culture in U.S. maritime facilities is relatively low (Brookings)
  • Cybersecurity awareness in the maritime sector is low to non-existent (ENISA)
  • Cyber support services are contracted out without consideration of the security of foreign owned contractors (TSWG)
  • FEMA has not consulted cybersecurity SMEs to inform the review of cyber-related grant proposals (GAO)
  • Basic cybersecurity hygiene is not being practiced (Brookings)
COMPARING STUDIES
Vulnerabilities and Potential Consequences

• Vulnerabilities exist, with potentially harmful consequences to ports
  • Industry is migrating toward a more connected control infrastructure and is thus increasingly vulnerable to attacks (TSWG)
  • Security at terminals also involves the use of types of systems for communications, sensors, and command and control (TSWG)
  • Attacks specific to cyber systems can have impact extending into the physical, business, human and environmental systems to which they connect (TSWG)
  • Attackers have targeted global oil, energy, and petrochemical companies, with intent to steal sensitive information such as operational details (OITS)
  • Cyber threats are a growing menace, with potentially “disastrous consequences” for European ports (ENISA)
COMPARING STUDIES
Risk Assessments

- Risk assessments to date have generally focused on physical (not cyber) security
  - Many Industrial Control Systems used today were designed for availability and reliability during an era when security received a low priority (TSWG)
  - Current maritime governance considers only physical security (ENISA)
  - Of 6 ports, only 1 had conducted a cyber vulnerability assessment, and none had developed a cyber response plan (Brookings)
  - The last National Maritime Strategic Risk Assessment did not address or provide any information on cyber risks (GAO)
  - Without an assessment of cyber-related risks, USCG and its stakeholders will be less able to plan and allocate resources to protect maritime transportation (GAO)
COMPARING STUDIES
Threat Information Sharing

- Threat information sharing is ad hoc and needs to be improved
  - Information exchange platforms should be considered and developed to identify major and upcoming cyber threats (ENISA)
  - At offshore oil and gas companies, both executives and operators must be able to identify the information most critical to business integrity and continuity (OITS)
  - The degree which U.S. information-sharing mechanisms were adequate and shared cybersecurity information was mixed (GAO)
  - The absence of an adequate national-level mechanism to maintain awareness among all maritime stakeholders at various locations reduces opportunities to mitigate cyber-based threats (GAO)
QUESTIONS AND CONTACT INFO

Questions?

Stephen Caldwell, (301) 602-0794, email: stephencaldwell1000@gmail.com

For access to referenced GAO reports, see GAO website: www.gao.gov