Acquisition Directorate

Research & Development Center

Report No. CG-D-07-16

Maritime Cyber Security University Research

Phase I - Final Report Appendices

May 2016

Homeland Security

N O T I C E

This document is disseminated under the sponsorship of the Department of Homeland Security in the interest of information exchange. The United States Government assumes no liability for its contents or use thereof.

The United States Government does not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the object of this report.

Bert Macesker
Executive Director
United States Coast Guard
Research & Development Center
1 Chelsea Street
New London, CT 06320

Technical Report Documentation Page

1. Report No. CG-D-07-16	**2. Government Accession Number**	**3. Recipient's Catalog No.**
4. Title and Subtitle Maritime Cyber Security University Research: Phase I - Final Report Appendices		**5. Report Date** May 2016 **6. Performing Organization Code** Project No. 8501
7. Author(s) USCG Research and Development Center, Dennis Egan et al., Rutgers University, Nicole Drumhiller et al., American Military University, Adam Rose et al., University of Southern California; Milind Tambe, University of Southern California		**8. Performing Report No.** R&DC UDI # 1623
9. Performing Organization Name and Address	U.S. Coast Guard Research and Development Center 1 Chelsea Street New London, CT 06320	**10. Work Unit No. (TRAIS)** **11. Contract or Grant No.** N/A
12. Sponsoring Organization Name and Address COMMANDANT (CG-FAC) US COAST GUARD STOP7501 2703 MARTIN LUTHER KING JR AVE SE WASHINGTON, DC 20593		**13. Type of Report & Period Covered** Final **14. Sponsoring Agency Code** Commandant (CG-FAC) US Coast Guard Stop7501 Washington, DC 20593
15. Supplementary Notes The R&D Center's technical point of contact is Judith R Connelly, 860-271-2643, email: judith.r.connelly@uscg.mil		
16. Abstract (MAXIMUM 200 WORDS) Appendicies of the Maritime Cyber Security University Research: Phase I - Final Report: Modern maritime systems are highly complex digital systems to ensure the safety and efficient operation of the shipping traffic so vital to the global economy. The vulnerabilities associated with reliance on digital systems in the maritime environment must be continuously examined. System protections must be ever ready to monitor vulnerabilities and secure maritime traffic system. The U.S. Coast Guard must ensure the integrity of the entrances to our "digital ports" and work to develop practical cyber security solutions to protect the nation's maritime infrastructure.		
17. Key Words Cyber security, MTS, Risk Management, Threats, Vulnerabilities	**18. Distribution Statement** Distribution Statement A: Approved for public release; distribution is unlimited.	

19. Security Class (This Report) UNCLAS	**20. Security Class (This Page)** UNCLAS	**21. No of Pages** 84	**22. Price**

TABLE OF CONTENTS

APPENDIX A. INFORMATION SHARING FOR MARITIME CYBER RISK MANAGEMENT

Information Sharing for Maritime Cyber Risk Management

Dennis Egan, Darby Hering, Paul Kantor, Christie Nelson, Fred Roberts

April 18, 2016

For further information: Dennis Egan, deegan@dimacs.rutgers.edu, or Fred Roberts, froberts@dimacs.rutgers.edu

Command, Control and Interoperability Center for Advanced Data Analysis

A Department of Homeland Security University Center of Excellence

Acknowledgements

The authors acknowledge vital discussions with CCICADA colleagues William Pottenger and Vanessa Kitzie in the course of this project. Special thanks go to our U.S. Coast Guard partners, in particular Mr. David Boyd, CAPT Michael Dickey, Dr. Joe DiRenzo III, LTJG Shanda Harper, LCDR Samuel Nassar, CAPT Andrew Tucci, CDR Brian McSorely, as well as the numerous U.S. Coast Guard and other government and private sector personnel whom we interviewed and are not specifically named. We would like to give a special acknowledgement to the two groups of reviewers who participated in the Working Meeting for Maritime Cyber Security, February 29 to March 2, 2016, and who contributed a number of new ideas and constructive criticisms that have been incorporated in the final version of this paper. CCICADA also gratefully acknowledges support from the Department of Homeland Security Office of University Programs, under award number 2009-ST-061-CCI002-07.

Options for Maritime Cyber Risk Management Information Sharing

Dennis Egan, Darby Hering, Paul Kantor, Christie Nelson, Fred Roberts

Table of Contents

1. Executive Summary

Effective and timely sharing of cyber risk management information among all stakeholders in the Maritime Transportation System (MTS) is vital to maintaining a safe, secure and resilient MTS. To develop information sharing protocols across this complex system, we must consider the layers of cyber risk management, including communication and technology, economic, and legal and regulatory aspects. Our research addresses the following questions: *What is the most appropriate role for the U.S. Coast Guard (USCG), and how does guidance for physical security relate to cyber risk management needs? What organizational systems could best support the needed sharing? What kinds of incentives could be used to encourage participation, particularly from private industry? What information needs to be shared, and when? What technologies could be used to enable and safeguard the information sharing?* In this white paper, we discuss the approach taken by the CCICADA-Rutgers team to address these topical questions. Our research process included interviews with experts, literature reviews, and taking a leadership role on the Port of New York and New Jersey Area Maritime Security Committee cyber subcommittee. We present our initial findings based on the interviews conducted and documents read, and we conclude with a set of recommendations related to each topical question.

2. The Background

At the March 2015 Maritime Cyber Security Symposium held at CCICADA/Rutgers University, one of the important themes was that the ability to share information in an effective and timely manner with all stakeholders in the MTS is essential in keeping the MTS safe, secure, and resilient. At the Symposium, VADM Charles Michel of the USCG laid out six research challenges. This paper deals with one of those challenges:

Information Sharing - How would a framework for network analysis be developed to support optimal information sharing with partners to address maritime cyber issues?

In June 2015, a Maritime Cyber Security Research Summit was organized at California Maritime Academy to investigate these six research challenges. Working groups were formed to address each of the challenges and this led to a report (Clark and Roberts 2015).

After the report, three more focused research questions were posed by USCG-FAC (Office of Port and Facility Compliance). This report deals specifically with the following one of those questions:

Information Sharing - Develop Information Sharing Protocols to meet the needs of industry and government.

To address this challenge, the CCICADA team set out to investigate methods to achieve rapid and useful information sharing in a way that both large and small players in the MTS can participate. In particular, how can we entice larger content providers to take the lead on information sharing within the MTS on cyber issues? We sought to explore ways to incentivize environments that are both transparent and candid in the sharing of information.

As part of the research, we also sought to investigate ways to categorize what information about the latest cyber threats and countermeasures should be shared and with whom. To answer this question we looked to understand the types of information that need to be shared rapidly as well as the types of information that do not impose an immediate threat. One example we set out to investigate is how and when to share reports on "near misses."

CCICADA also set out to understand what organizational structures for information sharing between government and industry in the MTS and between private sector MTS entities make the most sense to better understand:

- What information sharing leverage can be gained from existing organizations such as the Maritime Information Sharing and Analysis Center (M-ISAC) and Area Maritime Security Committees (AMSCs) or the National Cybersecurity and Communications Integration Center (NCCIC) or the International Maritime Organization (IMO) or NATO's Center for Combined Operations from the Sea (CJOS)?
- How is information sharing performed in other sectors such as those facilitating financial services, utilities, and oil and natural gas?
- Can we find good systems for use of real-time machine to machine interfaces such as the Security Information and Event Management (SIEM) software that can automatically collect, filter, correlate, vet, and distribute threat analysis and trends?

Finally, CCICADA sought to analyze the roles of the USCG in cyber risk management information sharing, roles such as developing standards for sharing systems, exchanging best practices, or enforcing sharing regulations. Can we learn a great deal from USCG reporting procedures for physical security risks, and translate those into good reporting procedures for cyber security risks?

This was an ambitious agenda for a project of a few months, and this paper reports on our preliminary findings and recommendations. There is a great deal that still needs to be done.

This report is organized into five topical areas:

- The role of the USCG and extending physical security to cyber security - cyber risk management
- Organizational systems for information sharing
- Motivation and barriers for sharing information
- What information to share, and what to share rapidly vs. slowly

- Technologies to support information sharing

A Comment on Terminology: In this paper, we use the terms "cyber security" and "cyber risk management" somewhat interchangeably. We tend to favor the latter terminology since we feel that management of cyber risk is a key to maximizing cyber security.

3. Context

In the maritime cyber security arena one may identify five kinds of adversarial threats or risks. One is TCOs (Transnational Criminal Organizations) which might disrupt cyber systems with goals such as hijacking, concealing contraband transport, or, potentially, hostage-taking. A second class of threats would originate with Violent Non-State Actors (VNSA) such as Al Qaida or ISIS/ISIL. While these might exploit some of the same technologies, they may have goals quite different from the essentially economic goals of TCOs[1]. Maritime cyber-systems are subject to attack by nation-states, either as part of a declared war, or part of an undeclared military contact, such as the encounters in the South China Sea. So-called "hacktivists," cyber specialists acting in extreme ways in support of a cause, may create havoc and cause damage to call attention to a social or political issue. Finally, there may be cyber attacks for purposes of corporate espionage. For each of these, the response requirements, both in terms of velocity, and of appropriate responding agents, may be quite different. And this, in turn will affect the architecture and technology, as well as the legal structure for information sharing. It should be emphasized that careless cyber behavior or misuse of cyber systems is a major cause of cyber system failures with potential consequences as serious as those of deliberate attacks, and information sharing abut the consequences of such behavior or misuse is also covered by our findings and recommendations.

3.1.Maritime Cyber Risk Management a Novel Challenge

The problem of information sharing for maritime cyber risk management has little in common with many marine security issues. Because of this, there are not strong analogies. One key issue of maritime safety and security is hull breach. The defense is waterproof bulkheads. But the analogous approach – shutting off cyber communications, removes their value completely. Whether the cyber system is GPS, or other computer controlled systems, their key contribution to maritime activity is their ability to bridge long distances, and maintain nearly instant situational awareness. Therefore nothing analogous to a "complete lockdown" seems feasible. As to the cause of hull breach, other than rare failures due to extreme weather, and those due to poor maintenance, the key cause is obstructions, which are more or less fixed in space. In contrast, cyberspace does not offer "chartable hazards," as bad actors can rapidly change their IP addresses or obscure them completely. The closest analogy to physical world hazards seems to be the notion of a "campaign," in which similarities in the specific technologies and messages serve to "locate" an attack in some abstract "ocean of possible attacks." Assembling information in terms of those characteristics seems to come closest to the historical approaches to maritime safety and security. Whether that abstract ocean of threats can be usefully presented remains to be explored.

1 http://www.sanctionswiki.org/TCO

3.2.Layers of Interaction

The problem of organizing for maritime cyber risk management seems to have three distinct aspects that must be considered. These arise because the players are of very different types: governments and their agencies, commercial shipping and cruise firms, the onboard captains and crew and the ports and associated personnel. Their coordinated efforts to advance Maritime Cyber Risk Management appear to involve at least three different "layers" of concern: communications and technology arrangements, economic considerations, and legal and regulatory matters.

Communication and Technology Arrangements

In the **communication and technology layer**, we find the problems of collecting information (about attacks and signatures) and of distributing warnings and remedies. The key considerations for this layer are of two kinds: technical capability, and architectural design. Technical capability limits the roles that individual parties may play. Architectural design asks questions such as: what channels should be used to communicate? Is the organization peer-to-peer or centralized? How does the architecture deal with varying levels of security and classification of information? What are the trust mechanisms?

The entire MTS comprises many players with outright conflicting interests, ranging from simple commercial competition to declared hostilities. How will access to shared information be limited (if at all) in consideration of these conflicts? Centralized control requires a trusted center. This can be accomplished for a single nation, but is much harder for a plurality of nations. Centralized control also puts "all the eggs in one basket" so that an attack on that control center can have widespread impact, worse than would be realized in a distributed or peer-to-peer system. There is some recent research on building decentralized systems that can enforce trust without putting all the eggs in one basket (Minsky, 1991; Minsky and Leichter, 1995; Minsky and Ungureanu, 2000).

Economic Considerations

The **economic layer** represents not only the fact that multiple players are in competition with each other, but also the sheer costs of being a participant. Many maritime activities work on a narrow economic margin, and the costs of being an effective participant in a sharing system may be out of reach. As soon as some players are excluded, however, the entire system loses much of its value, and the outcasts are ripe for an attack that could affect many players across the maritime system. From an economic perspective every organization must watch its "bottom line." As the SONY attacks[2] showed, the entertainment industry, which had felt that cyber-security concerns were limited to IP issues, can be harmed in other ways. It has been reported that since that attack, that industry as a whole has become more interested in information sharing.

In addition to the false confidence that one will not be a target, if a firm reports that it has been hacked, it may lose the confidence of the public and suffer overall harm much greater than was caused by the specific attack. Each corporation or business is asked to weigh the potential downstream benefit to all of its competitors against its immediate loss by revealing the attack. This layer brings us face to face with all the complexities of maintaining competitive advantage when the threat is ubiquitous and invisible.

2 Attributed to North Korea. See http://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html?_r=0

Legal and Regulatory Matters

A third layer is the **legal or regulatory layer**. In the United States (and many other countries), cooperation among firms, which might have the effect of reducing competition, and therefore raising consumer costs, is tightly regulated. Since cyber risk management is a cost, and cooperation or sharing will lower those costs, such sharing is in danger of falling under the regulations. While there are proposed (limited) legislative remedies (Burr, 2015), the problem is a significant one. Conceivably there may one day be an extension of the seafarer's obligation to assist persons, to an obligation to assist systems (Davies, 2003).

4. The Research Process

We drew information from several kinds of sources as we compiled findings and developed recommendations for this white paper. The process is described briefly below, and was aimed to organize and synthesize the information into specific recommendations for consideration.

4.1.Interviews

Our best sources of information were numerous interviews with experts. We reached out to all of the participants in Working Group Team #6 of the Maritime Cyber Research Summit held at the CSU Cal Maritime Safety and Security Center, June 16-17, 2015. A summary of Working Group 6's findings and recommendations can be found in Clark and Roberts (2015). That working group focused on Information Sharing, and many of its findings and recommendations led to the topic of the present white paper. We were able to interview a majority of the Working Group 6 participants, who in turn gave us additional contacts to interview. Besides that key set of sources, we interviewed other senior USCG officers specifically charged with developing cyber risk management policies and guidelines, as well as some people in the private sector with specific expertise in areas such as maritime law and Information Sharing and Analysis Centers (ISACs), and also representatives of other government agencies such as the FBI, port security, NYPD, and other law enforcement agencies.

In all we conducted approximately thirty interviews. Most interviews were conducted by a pair of project team members who used an interview guide, took notes and later combined their notes into a single interview summary. Since we did not ask permission of the interviewees to attribute specific quotes or ideas to them, in the following, we refer to (Interviews, 2015-6) when we present a finding based on one or more interviews.

4.2.Literature Review

We also reviewed selected documents related to cyber risk management information sharing. Some of these are listed in the Reference section of this white paper. These include relevant legislation and regulations, government reports, security guidelines, best practices and standards, and academic research on technologies, incentives and risk related to information sharing. The documents cited in the Reference section are a tiny fraction of the literature available on this topic.

4.3.Port of New York and New Jersey AMSC Cyber Subcommittee

Another source of information for the project was the knowledge and experience gained from our leadership role in the Cyber Security Subcommittee of the Area Maritime Security Committee (AMSC) for the Port of New York and New Jersey. This subcommittee, formed and officially chartered in 2015, is chaired by the USCG with Rutgers University/CCICADA as a co-chair along with Stevens

Institute/Maritime Security Center and the NYPD. Meeting and working with this subcommittee brought us into contact with numerous USCG personnel, commercial partners, and representatives of law enforcement concerned with maritime cyber risk management in the region surrounding the Port of New York and New Jersey. Through meetings and conversations we were able to begin to understand issues related to cyber risk management information sharing by commercial companies (some of whom are competitors with one another), planning for cyber risk management exercises, and cyber risk management training needs. Since a primary activity of each AMSC is to create a security plan (the AMSP), a natural part of the maturation process for AMSCs is to create a subcommittee to address cyber risks. At the time of this writing, about one-third of the AMSCs have chartered cyber security subcommittees (Interviews, 2015-2016).

4.4.Process for Organizing and Synthesizing Information

After gathering information by conducting interviews and reading relevant documents, the project team systematically worked to organize and synthesize the information. Project team members were asked to summarize major takeaways from the interviews and literature in bullet points, and to categorize these bullet points by placing them under one (or more) of the five substantive topics under information sharing that we used to organize our project. As mentioned in Section 2, the five topics are:

- The role of the USCG and extending physical security to cyber security – cyber risk management
- Organizational systems for information sharing
- Motivation and barriers for sharing information
- What information to share, and what to share rapidly vs. slowly
- Technologies to support information sharing

These clusters of bulleted items formed the basis of the findings in Section 5 of this report. Documents and/or interviews are cited in support of the findings. The findings in turn lead to the recommendations in Section 6.

5. Findings

In this section, we present selected findings that provide context for the recommendations given in Section 6. Throughout this section, we link the discussion points to the recommendation(s) they produce using the notation [**R** 6.x.y] to indicate relevance to recommendation 6.x.y, for example.

5.1. The Role of the USCG and Extending Physical Security to Cyber Security – Cyber Risk Management

The USCG has an extensive set of guidelines and regulations for physical security. Developing cyber security – cyber risk management guidelines for the MTS seems to be a natural extension of that role for the USCG. It was suggested in interviews that the USCG could develop cyber risk management guidelines for facilities similar to 33CFR105 and continue, similarly, to develop guidelines for vessels (Interviews, 2015-6; Maritime Security, 2010). Since there are many diverse players in the MTS, and they have competing interests, these guidelines should be written at a "high" level – specifying the characteristics of a cyber risk management plan, not detailed prescriptive requirements (Interviews, 2015-6).

5.1.1 Resources for Planning Cyber Risk Management

There are numerous resources for planning cyber risk management, but most were not developed specifically for the maritime sector. Examples include the NIST framework (NIST, 2014), the NIST 800 series (NIST, 1990-2015), the ISO/IEC series, the Center for Internet Security Controls for Effective Cyber Defense Version 6.0, and the BIMCO recommendations (BIMCO, 2016). The ISO/IEC 27,000 series provides international best practice recommendations on security management (ISO/IEC, 2013). The Center for Internet Security (CIS) Controls for Effective Cyber Defense Version 6.0 provides ways to defend against the most common and dangerous cyber attacks (CIS, 2015). The NIST 800 Series provides security guidelines, policies and procedures for federal government IT systems and organizations (NIST, 1990-2015). The BIMCO recommendations are specific to a segment of the maritime sector, and carefully address cyber security for onboard systems (BIMCO, 2016). [**R** 6.1.1, 6.1.2, 6.1.3]

The NIST guidelines are perhaps the most widely known, and provide an example framework of a process for developing cyber risk management plans (NIST, 2014), called the Cybersecurity Framework (CSF). The NIST Cybersecurity Framework was developed to support protection of critical infrastructure resources. It includes a list of steps to take (and repeat) to develop and refine a cybersecurity plan. Additionally the NIST Framework Core contains a list of "Functions, Categories, Subcategories and Informative References" that describe common cybersecurity activities. As described by NIST (NIST, 2016), "The goal of the framework is to minimize risks to the nation's critical infrastructure, such as the transportation, banking, water and energy sectors. The executive order directed NIST to work with stakeholders across the country to develop the voluntary framework based on existing cybersecurity standards, guidelines and best practices." In creating this framework, NIST was "extremely collaborative with the public sector" (NIST, 2016-2). However, even this framework is not a perfect document. CSF is referenced in several documents as a living document, and when requesting feedback on the framework through a response analysis, respondents felt that it needed frequent updating (suggested yearly), and that it should be done by either NIST or a neutral third party. It is important to note that CFR is "consistent with voluntary international standards" (NIST, 2015), which is important in the maritime international setting. If the USCG decides to issue guidelines for cybersecurity plan development, this could inform part of the guide.

The DHS Cyber Resilience Review (CRR) process uses the NIST guidelines. The CRR predates the NIST CFR, and although not a perfect matchup, closely aligns with the NIST framework. Included in the CRR self-assessment package is a document that maps the CRR to the CFR (DHS CRR).

ICS-CERT (Industrial Control Systems Cyber Emergency Response Team), operated through DHS, offers self-assessment tools as well. Though there are many of these tools available, the ICS-CERT Cybersecurity Evaluation Tool (CSET), is a free well supported option. DHS offers approximately 60 YouTube videos showing how to utilize this tool (CSET, 2015). CSET has several approaches for self-assessment: a questions based approach (recommended for most assessments), a standards based approach (for regulated industries, presenting requirements as they are written in the standards), and a cybersecurity framework based approach (a risk-based cybersecurity evaluation using a customized question set). This self-evaluation allows users to customize their assessment based on need: regulated industries have requirements available to assess built into the tool and there is also an option to select a desired security level (low, moderate, high, very high). Questions in the self assessment are based on 27

different categories such as access control, physical security, training, maintenance, etc., each with many subtopics.

5.1.2 Cyber Risk Management Audits

Guidelines that are for protocols for ports, companies, etc. should not become a basis for auditing individual approaches. But companies may welcome government guidelines. NIST could be one such starting point (BIMCO, 2016; Interviews, 2015-6). [**R** 6.1.1]

Because cyber risk management lacks a specific physical presence, there is little functional connection, beyond physically securing (e.g., requiring two-person authentication) access points to cyber-systems. None of our interviewees discussed issues such as physical protection against GPS spoofing, and other threat-specific physical measures. Therefore, it seems that physical security and cyber risk management might be better linked through audit systems currently in place or third party audits, and companies should not rely solely on external audits (Interviews, 2015-6; BIMCO, 2016). [**R** 6.1.4, 6.1.5]

One example of audits are those performed by the Bureau of Safety and Environmental Enforcement (BSEE). BSEE regulates and inspects all oil and gas operations on the outer continental shelf (if oil rigs are in transit, they are regulated by the USCG). BSEE does not write a company's hazards plan; it is developed by the operators themselves and is approved by a third-party. BSEE assesses how well the companies meet these plans. These plans focus primarily on physical security, but in the future they may include some cyber risk management as well. It is important to note that BSEE might be a reasonable entity to conduct cyber auditing for oil and gas operations. However, as of the time of our interview, BSEE had never conducted a cyber audit.

There are additional regulations, 33CFR Subchapter H (Maritime Security, 2010), relating to maritime vessels. These regulations focus on owner/operators of Mobile Offshore Drilling Units (MODU), foreign cargo vessels greater than 100 tons, US self-propelled vessels greater than 100 tons (except commercial fishing vessels), passenger vessels with more than 150 passengers, or other types of passenger vessels carrying more than 12 passengers when including at least one passenger for hire, and certain types of barges, tankships, and temporary assist vessels, but do not apply to warships. There are compliance audits for various types of security and safety topics including drills and training. Audits are performed through Vessel Security Assessments, and owners or operators must have a Vessel Security Plan. This is another area to which cyber components could be added. Amendments to the Vessel Security Plans are approved by the Marine Safety Center and may be added by the USCG or the vessel owner or operator. These regulations also apply to facilities. The regulations for facilities include access control, systems and equipment maintenance, handling cargo, training, drills and exercises required, monitoring, procedures for incidents. This is yet another area in which cyber regulations, training, drills, etc. could supplement the existing plans. Amendments to a Facilities Security Plan are approved by the Captain of the Port (COTP) and may be initiated by the COTP or the owner/operator. [**R**.6.1.4]

Although not designed for auditing, the BIMCO guidelines may also provide suggestions for components to integrate into these cyber risk management audits, assessments, trainings, and drills.

5.1.3 Metrics

Our interviews made it clear that all are concerned with the cyber-threat to the MTS. However, there are not currently any agreed-upon measures in place to assess "how secure" any part of the system is.

Similarly, there are no measures in place to assess "how insecure" or "at risk" parts or subsystems may be. Clearly there is need for metrics to determine the cyber secure status of ports, vessels, container handling systems, etc. The Maritime Resource Center in Middletown, RI provides one example of an organization that is beginning to develop such metrics, through their proprietary methodology for assessing vessel and marine terminal cyber risk management. The primary use of such metrics for that organization is for use in their educational programs for mariners. However, many other uses can be envisioned, for example in cyber risk management audits. The Department of Energy's Cybersecurity Capability Maturity Model (C2M2, 2014) provides a complementary approach focused on assessing an organization's implementation and management of cyber risk management practices. Information Sharing and Communication is one of ten cyber security domains for which an organization can use C2M2 to assess the maturity of its processes. An effort to develop performance-based standards and the metrics to measure achieving those standards focused on maritime cyber risk management could be very important. [**R** 6.1.5]

5.1.4 Training and Exercises

The 33CFR103.515 specifies the USCG role to coordinate with the Area Maritime Security (AMS) Committee to conduct and participate in exercises to test the effectiveness of the AMS Plan. The AMS Plan should include a cyber component, and exercises should increasingly include tests of the effectiveness of the cyber risk management plan. Strategies for incentivizing sharing (together with new technologies) could be tested at upcoming or future USCG cyber risk management exercises (Interviews, 2015-6). These exercises could be held in conjunction with physical security exercises since we know a cyber attack may be brought about by physical damage or vice versa. The AMS Committee for the Port of Pittsburgh held the first such exercise in 2013. Exercises can range in scope from tabletops and workshops to full-scale, simulated, coordinated cyber attacks. In the latter case, access to a cyber range may be useful (Interviews, 2015-16). [**R** 6.1.6, 6.1.7, 6.1.8]

Conventional education (in Technical Schools, Community Colleges, Colleges and Universities) moves slowly. Today, some don't even realize that cyber is a threat (Interviews, 2015-6). It may be that the national or international coverage of dramatic problems contributes more to the essential awareness of cyber-threats than does any formal program of education. Therefore educational efforts should be of two kinds: "Slow:" the development and dissemination of courses and training materials suitable for players at all levels from port managers to mariners, and "Fast:" effective media campaigns to build upon any major attacks (or near-misses) as they occur, to increase awareness, and motivate players to engage with the training materials, and/or the sharing organizations. Building awareness and capability requires training tailored to components of the maritime system (Interviews, 2015-6; BIMCO, 2016). The private sector and non-profit organizations have an important role to play in such training (Interviews, 2015-6). This might coincide with rolling out new cyber guidance from the USCG. [**R** 6.1.9, 6.1.10]

5.1.5 Collaboration with Other Government Agencies

The USCG has a unique position in the MTS as part of the U.S. Government. In developing guidelines and technical standards for cyber risk management information sharing, the USCG has the opportunity to collaborate with other government agencies (such as NIST, ODNI, Cyber Command, NavSea, and DHS CERT). In support of these opportunities for enhanced information sharing, strengthened by the USCG presence at the NCCIC described below in Section 5.2, further research is needed into the most appropriate role for the USCG in (1) *pushing* best practices for cyber risk management to the private

sector (versus just *posting* the information), and (2) developing regulations for sharing information about cyber attacks, vulnerabilities, and defenses with the private sector (Interviews, 2015-6). [**R** 6.1.11, 6.1.12, 6.1.13]

5.2.Organizational Systems for Information Sharing

The question of how to organize systems for information sharing had by far the richest source of information, as there are several model organizations, and there is a strong consensus that some combination of those models will form the basis for any effective program of cyber risk management for the MTS. Key findings seem to be that: (1) industry players, based on their resources, will play roles of varying intensity in the organizations that are developed; (2) to permit all needed kinds of cooperation some organizations should be non-governmental, while others are governmental and perhaps even multi-national; (3) issues of trade secrets, proprietary information, public embarrassment, lack of technical (IT) skills of even a basic nature, and national security will limit the willingness of players to share information, and must be countered with an array of incentives, as discussed in Section 5.3 below; (4) there are significant technical challenges in developing protocols for rapid sharing, and in coping with the expected flow of information, as participation expands to include all the parts of the MTS (see Section 5.5 below).

With such diverse organizations in the MTS, a range of organizational, technical, and incentive systems will be needed. To ensure timely dissemination to appropriate players, some of our interviewees emphasized the importance of a tiered approach to information sharing (Interviews, 2015-6). [**R** 6.2.2]

5.2.1. Enhancing USCG Presence at the NCCIC

Organizationally, partnering with effective national organizations can help the USCG to a running start. By increasing its presence at the NCCIC, the USCG would expand its opportunities to coordinate with NCCIC partners and report cyber risk management alerts, trends and mitigation strategies across the USCG, commercial partners, and other appropriate government agencies. We understand from interviews that the USCG currently has one member of the CG Cyber Command onsite at the NCCIC, and we are recommending this presence be extended to a 24x7 capability (Interviews, 2015-6). [**R** 6.2.1]

Through interviews and related research we learned that the NCCIC is able to receive and analyze Protected Critical Infrastucture Information (PCII),[3] a category of Sensitive but Unclassified (SBU) information that is protected from FOIA disclosure and regulatory use to encourage reporting of information important to the security of the nation's critical infrastructure. Furthermore, through the new DHS Automated Indicator Sharing (AIS)[4] program, the NCCIC is able to receive cyber threat indicators from private industry, perform automated analyses and tasks such as removing personally identifiable information (PII) or anonymizing the sender, and distribute the indicators to federal departments or private industry, as appropriate. This kind of two-way, machine to machine sharing accelerates the pace at which DHS, and therefore the NCCIC, is able to receive and provide cyber measures and signatures. Finally, the NCCIC works with a variety of DHS training and assessment tools available to Critical Infrastructure and Key Resources sectors. These tools include the previously mentioned Critical Resilience Review (CRR)[5] available as self-assessment or DHS-facilitated evaluation,

[3] https://www.dhs.gov/protected-critical-infrastructure-information-pcii-program
[4] https://www.us-cert.gov/ais
[5] https://www.us-cert.gov/sites/default/files/c3vp/crr-fact-sheet.pdf

and the National Cybersecurity Assessment & Technical Services (NCATS)[6] through which a variety of cyber assessment services (such as architecture reviews and red-team, blue-team penetration testing) are available at no cost to stakeholders. [**R** 6.2.1]

5.2.2. Re-developing the Maritime ISAC

Partnering with effective private sector organizations will be needed to bring competing firms and competing nations into an effective overall system. Relying solely on a governmental organization might limit information sharing among private sector partners (and international partners), and this leads to the idea of a re-development of the Maritime ISAC to provide an industry-focused community for information sharing (Interviews, 2015-6). [**R** 6.2.3]

Reflecting the economic layer of interaction, organizations differ in the resources they can direct to cyber risk management. Some interviewees suggested a Maritime ISAC with membership levels that provide and require different levels of information and capability (Interviews, 2015-6; FS-ISAC, 2015). A fast-acting ISAC is needed to complement periodic, face-to-face information sharing (supported by the AMSCs) since some cyber threats and attacks must be met in real time (Interviews, 2015-6). There seem to be variously: very tight agreements among small numbers of large players with major budgets (Interviews, 2015-6); more broad sharing, such as ISACS; and smaller players with low or no cyber budget or expertise. To include the full range of MTS stakeholders, some models are: ISACs; fusion centers; neighborhood watch as developed by the FBI Office in Los Angeles. Incremental development can start with key players and expand, perhaps using AMSC cyber risk management subcommittees as an initial step that the USCG is able to support immediately while industry partners evaluate the viability of developing and running an ISAC. (Interviews, 2015-6). [**R** 6.2.2, 6.2.3, 6.2.4, 6.2.7]

Reflecting both the economic and legal layers of interaction, sharing agreements may require: anonymity; authenticated messaging; and no FOIA access (FS-ISAC, 2015). The FS-ISAC model (particularly its technical systems guaranteeing submission anonymity) is a possible model for a new Maritime ISAC (FS-ISAC, 2015). [**R** 6.2.3]

Again at the legal layer, multi-national membership adds challenges. The FS-ISAC may provide a model. (FS-ISAC, 2015; Interviews, 2015-6). National laws on cyber vary greatly (Interviews, 2015-6). Since some important information is classified, it seems reasonable that a proposed Maritime ISAC ultimately be a cleared organization (Interviews, 2015-6; FS-ISAC, 2015). The ISAC could interface with other government agencies to ensure appropriate notification of organizations as part of the membership/access levels. [**R** 6.2.3, 6.2.4]

At the technical layer of interaction, shipboard systems and concerns are specialized, and, for example, legacy supervisory control and data acquisition (SCADA) systems and their network connections, in particular, need to be assessed for cyber risk (Konon, 2014). To have effective communication among those with true common interests, the ISAC or similar organization might maintain a subgroup focused on shipboard systems, perhaps guided by the BIMCO publication (BIMCO, 2016). [**R** 6.2.4]

Any industry-led information sharing platform (such as M-ISAC) and the USCG information sharing platform (such as a part of the NCCIC) must themselves share critical cyber risk management information regarding cyber threats. This leads to the idea that the M-ISAC maintain a presence at

[6] https://www.us-cert.gov/ccubedvp/federal

NCCIC, as is done by the FS-ISAC, the Aviation ISAC, the Multi-State ISAC, and others (Torres, 2015; FS-ISAC, 2015). [**R** 6.2.3]

5.2.3. Enhancing Cyber Incident Reporting Capability

As defined in 33CFR101.305, maritime security plans require that "activities that may result in a transportation security incident" be reported to the U.S. Coast Guard National Response Center (NRC). Some of our interviewees have suggested that the USCG either develop the capability or partner with an organization (such as the NCCIC[7]) to receive centrally information about cyber risk management incidents and suspicious activities (Interviews, 2015-6). The analysts at this organization could send relevant alerts to the affected maritime community members (Interviews, 2015-6) establishing a regulated two-way path and ensuring the USCG has all relayed information. In the mean time, we heard in interviews with port officials that there is confusion regarding whom they should contact in the event of a cyber incident (Interviews, 2015-6). The NRC maintains a hotline[8] for "anyone witnessing an oil spill, chemical relesase or maritime security incident," but there have not yet been thresholds guiding which types of incidents should be reported to the NRC (versus more locally, perhaps at an AMSC Cyber Subcommittee meeting). In fact, there are currently no regulations on reporting cyber incidents unless it reaches a Transportation Security Incident (TSI) level incident for the USCG, where TSI is defined as "any incident that results in a significant loss of life, environmental damage, transportation system disruption, or economic disruptions to a particular area."[9] No industry cyber incidents have ever reached the TSI level. We understand that the USCG Office of Port & Facility Compliance (CG-FAC) is updating its breach of security requirements soon to include thresholds for reporting (Interviews, 2015-6). [**R** 6.2.2, 6.2.8]

5.2.4. Enhancing AMSC Cyber Information Sharing

Currently, the AMSCs enable public and private partners in a geographic port area to meet periodically (often quarterly), discuss current concerns in the area, and build relationships of trust necessary for information sharing[10]. To maintain these relationships and extend them into cyberspace, each AMSC could follow the example of the Port of Pittsburgh AMSC, the Port of Northern California AMSC, the Port of New York and New Jersey AMSC and others and create a cyber security subcommittee (Interviews, 2015-6; Torres, 2015). As noted previously, about one-third of the AMSCs already have chartered a cyber security subcommittee. As the NY/NJ AMSC and others have done, all AMSCs could consider sharing cyber risk management information through the USCG HOMEPORT Portal (Interviews, 2015-6). [**R** 6.2.5, 6.2.6]

In many of our interviews, we were told that a large number of entities of the MTS do not have the resources to hire employees with sufficient background to understand anything beyond the most rudimentary aspects of good cyber hygiene, and certainly not information about evolving cyber attacks, cyber vulnerabilities and cyber defense. Some of these entities are represented on various AMSCs. More work is needed to understand organizational structures for information sharing that will develop ways to communicate cyber issues to the large number of MTS entities without technical expertise. [**R** 6.2.7]

---

[7] http://www.dhs.gov/topic/cybersecurity-information-sharing

[8] The hotline phone number can be found on the NRC homepage: http://www.nrc.uscg.mil/ Accessed 3/23/2016.

[9] http://www.uscg.mil/d8/msuBatonRouge/mtsa.asp

[10] For discussion of the importance of trust for information sharing, see: European Network and Information Security Agency (ENISA), 2010. *Incentives and Challenges for Information Sharing in the Context of Network and Information Security*.

5.2.5. Multi-National Maritime Organizations: CJOS, AAPA, IMO

Complex nation-specific laws on cyber related issues along with concerns of sharing information about national security with other nations makes multi-national information sharing very challenging. "Maritime operations to counter illegal activity at sea are difficult to coordinate between nations, governing bodies, security organizations, and armed forces. Responsibilities, jurisdiction, co-ordination, information and intelligence exchange, as well as the command and control of units conducting or supporting law enforcement operations are a maze of classifications, information systems, hierarchies and varied forces. … None of the groups alone can provide all the necessary capabilities and coordination needed to succeed against threats"[11]. To help facilitate this information sharing and other security issues, the North Atlantic Treaty Organization (NATO) developed a NATO Memorandum of Understanding to create the Combined Joint Operations from the Sea (CJOS) Center of Excellence. CJOS was established on June 28, 2006, and includes 13 nations: Canada, France, Germany, Greece, Italy, the Netherlands, Norway, Portugal, Romania, Spain, Turkey, the United Kingdom, and the United States. CJOS is located in Norfolk, Virginia and is the only NATO accredited COE in the U.S. The purpose of CJOS is to "support the transformation of joint maritime expeditionary operations in assistance to NATO"[12].

The CJOS Memorandum of Understanding states that external security is the responsibility of the host nation (US) and internal security is the responsibility of the CJOS Director, following NATO and US security regulations. Relating to information sharing, the nations involved in CJOS are responsible to safeguard the security of any classified information provided in the course of the CJOS mission. Confidentiality is expected to remain intact even if the MOU is terminated or withdrawn.

CJOS held Maritime Security Conferences (MSC) from 2008-2012 which built on the idea of information sharing. In 2012 they found that "a bottom-up approach is more likely to be supported than an international governance model. … The outcome of MSC 2012 identified widespread agreement that there is a need for information sharing and, for this sharing to occur, there needs to be a shift from the current 'need to know' mentality to a culture of 'need to share'"[13]. [**R** 6.2.9]

Another international maritime organization, the American Association of Port Authorities (AAPA), is a trade association representing more than 130 deep draft public ports in the United States, Canada, Latin America and the Caribbean. The AAPA provides education, services and advocacy for its members, which also include more than 300 associate and sustaining members such as inland river ports and firms doing business with corporate member ports. Some of the education opportunities available in 2015 included an intensive Marine Terminal Management Program, a Port Security Seminar and Exposition, a Cybersecurity Seminar, and a workshop on Shifting International Trade Routes. Along with the newsletters and surveys the AAPA publishes, they maintain a list of Port Industry Best Practices[14], which includes categories of resources such as Emergency Preparation Response and Recovery, that could potentially be a forum for sharing port cyber risk management guidelines. Just as BIMCO recently issued detailed Guidelines for Cyber Security Onboard Ships (BIMCO, 2016), some of our interviewees said that it might be appropriate for the AAPA to develop similarly-focused guidelines for port facility cyber risk management (Interviews, 2015-6). [**R** 6.2.10]

[11] http://www.act.nato.int/article-2013-2-14
[12] http://www.state.gov/documents/organization/75818.pdf
[13] http://www.cjoscoe.org
[14] http://www.aapa-ports.org/Issues/content.cfm?ItemNumber=1262&navItemNumber=543

The International Maritime Organization (IMO), an agency within the United Nations, has 171 member states and 3 associate members responsible for regulating shipping. The main role of the IMO "is to create a regulatory framework for the shipping industry that is fair and effective, universally adopted and universally implemented. In other words, its role is to create a level playing-field so that ship operators cannot address their financial issues by simply cutting corners and compromising on safety, security and environmental performance"[15].

In the IMO's 2014 year in review, The Maritime Safety Committee and the Facilitation Committee agreed to include on their agendas the topic of cyber security for the following year (2015)[16]. This came about after Canada presented a paper on the topic to the 39th session of the IMO facilitation committee in September of 2014. "The Canadian presentation called for voluntary guidelines on cyber-security practices to protect and enhance the resilience of electronic systems of ports, ships, marine facilities and other parts of the maritime transport system. It is understood to have suggested that cyber issues are brought into the coverage of the International Ship and Port Facility Security Code (ISPS)"[17]. The committee agreed, "recognising it as a relevant and urgent issue for the Organization, in order to guarantee the protection of the maritime transport network from cyber threats".

In a January 2016 IMO letter, describing trends affecting the organization in order to help develop their strategic framework for 2018-2023, cyber risk was at the top of the list. The following excerpt was taken from this letter: "The increasing trend in the use of cyber systems benefit the maritime industry, but their use also introduces great risk. From a security perspective cyber systems may be exposed to deliberate, malicious acts from individuals who may attempt to control, disable, or exploit cyber systems. From a safety perspective, non-targeted malware, innocent misuse of systems, and simple technical errors may impact vital systems related to ship and propulsion control, navigation-related technologies, industrial ship control technologies including propulsion, steering, ballast water management, electrical systems, heating, ventilation, air conditioning systems, cargo pumps, cargo tracking and control, ship stability control systems, fire detection and protection, gate access control and communication and monitoring systems, alarm systems and various hazardous gas alarm systems, pollution and other safety and environmental monitoring"[18]. However, the IMO does not yet publicly state what measures they will be taking.[**R** 6.2.11]

5.3.Motivation and Barriers for Information Sharing

The question of how to incentivize sharing among players in the MTS is a central one. As with any sharing scheme, information sharing for cyber risk management faces the "problem of the commons." Several industries appear to be further along in developing solutions, and their models provide guides. In complexity, MTS is closest to international finance, and the economic and security concerns of many kinds of organizations, and of competing nations, are involved. Positive incentives (motivations for information sharing) could include technical support and timely sharing of information or insurance

[15] http://www.imo.org/en/About/Pages/Default.aspx
[16] http://www.imo.org/en/MediaCentre/HotTopics/yearreview/Pages/2014-Security-and-facilitation.aspx
[17] http://www.allaboutshipping.co.uk/2014/10/25/imo-is-being-warned-of-scary-potential-of-maritime-cyber-attacks/
[18] http://www.imo.org/en/About/strategy/Documents/Member%20States%20-%20tdc/United%20States%20-%20Input%20to%20TDCs.pdf#search=cyber%20risk%20management

industry pressure (through rate reductions) to encourage participation. They also could include believable guarantees of protection from (1) action by competitors (2) legal action and (3) FOIA pressures by competitors, NGOs, and activist groups. Negative incentives (overcoming barriers to sharing) might include regulations and penalties for non-reporting. It may be possible to test some models in USCG exercises.

Providing incentives for sharing could be particularly important as the industry begins to take the small, initial steps that will lead to enhanced maritime cyber risk management. For example, we are recommending that the U.S. Government require "landlord" port operators[19] to incorporate maritime cyber risk management standards into the leases they issue to terminal operators for the right to use the ports. Landlord ports are highly autonomous and can easily implement requirements of this nature into their leases without waiting for a legislative or regulatory process, but terminal operators may then decide to "port shop" for easier restrictions, thereby hurting the ports working to improve cyber risk management. For this reason, regulation requiring these standards at all ports is needed to ensure a "level playing field" in cyber risk management, preventing terminal operators from being able to avoid cyber standards by relocating to a more "lax" port operator (Interviews, 2015-6). [**R** 6.3.1]

Realization of this kind of legislation or regulation will likely take some time, however, and in the interval, there are opportunities to motivate early adoption of enhanced cyber risk management practices. As port operators negotiate leases with tenants, they could, for example, offer discounted rates to tenants that agree to comply with cyber risk management standards (Interviews, 2015-6). Futhermore, the terms of port leases could be opportunities for requiring tenants' participation in a reinstantiated M-ISAC. [**R** 6.3.1, 6.3.2, 6.3.3]

Players in this industry bring greatly different resources to the problem (Interviews, 2015-6). The arrangements made at the E-ISAC (Electrical Industry) and the FS-ISAC (Financial) may yield useful models for development of incentives (Interviews, 2015-6; FS-ISAC, 2015). We heard in interviews, for example, that the FS-ISAC maintains a Gmail Listserv for communicating threat information to its members, and the fact that U.S. Law Enforcement is not allowed to join the list encourages foreign-based partners to participate (Interviews, 2015-6). Other models are the FBI, which shares at industry conferences, and the Oil and Gas industries (ONG-ISAC) (Interviews, 2015-6; FS-ISAC, 2015). It seems clear that incentives will have to be tailored to be effective for the various classes of players. [**R** 6.3.4, 6.3.5, 6.3.6]

Since information sharing benefits all, but costs the contributors, distillers and disseminators, there is a risk of "free-riding" (Gal-Or & Ghose, 2005). However, the MTS is an interdependent system of systems, and a major cyber event somewhere in the system will likely disrupt the business of all parties and potentially affect the reputation of the whole industry (Interviews, 2015-6). [**R** 6.3.5]

Some useful incentive models may be found in other domains, such as the WHO's provision of subsidized vaccine targeted to countries reporting outbreaks of bacterial meningitis (Laxminarayan, et al., 2014). It is possible that compliance in sharing will be motivated by the insurance industry, although it has not yet taken any positions on this issue (Interviews, 2015-6). [**R** 6.3.6]

[19] See the American Association of Port Authorities (AAPA) Glossary of Maritime Terms for definitions of "landlord" vs. "operating" ports. http://www.aapa-ports.org/Industry/content.cfm?ItemNumber=1077 Accessed 3/23/2016.

The European Network and Information Security Agency (ENISA) found, in a research effort regarding information sharing for network and information security, that stakeholders felt "Economic incentives stemming from cost savings" were of the highest importance for information sharing, whereas "Economic incentives from the provision of subsidies" or "Economic incentives stemming from the use of cyber insurance" were of low importance (ENISA, 2010). That is, the participants identified the most important incentive for participating in an Information Exchange (IE) such as an ISAC to be the cost savings they would realize from more efficiently allocating the information security resources of the group. The challenge remains, however, to prove that participation in an IE does bring these savings and efficiencies (ENISA, 2010). [**R** 6.3.6]

A different kind of incentive for information sharing, ranked third in importance out of ten incentives for information sharing by the participants in the ENISA research Delphi exercise, is the "presence of trust amongst IE participants". Although trust is perhaps more difficult to quantify than cost savings, many interviewees highlighted operating and sharing information within a community of trusted partners (such as the current AMSCs) to be a critical component of the current security arrangements (Interviews, 2015-6). Furthermore, a 2001 study of organizations accustomed to sharing information, conducted by by the U.S. General Accounting Office (GAO), found, "All of the organizations identified trust as the essential underlying element to successful relationships and said that trust could be built only over time and, primarily, through personal relationships" (U.S. GAO, 2001). [**R** 6.3.6]

5.4.What Information to Share, and What to Share Rapidly vs. Slowly

What information should be shared? The Cybersecurity Information Sharing Act of 2015 (Burr, 2015) proposes requirements for communication of "cyber threat indicators," defining these as the "information necessary to describe or identify." The Act identifies eight categories of cyber threats, and could be the framework of a strategy describing what to share regarding threats. More broadly, the FS-ISAC structures its sharing according to incidents, threats, vulnerabilities, and resolutions/solutions (FS-ISAC, 2015). We learned that information shared with the MS-ISAC may include: advisory notices, tactical information, and known malicious IPs (Interviews, 2015-6). Information to share will include: vulnerabilities, TAXii[20] information, botnet information, malicious IP addresses, near misses, incidents, threats, resolutions/solutions, and the seven key Netflow fields (Interviews, 2015-6). Once again the economic layer is in play here as only a select set of private sector companies and law enforcement agencies have the resources to dedicate groups of highly skilled people to analyze this information. [**R** 6.4.1]

A Red|Yellow|Green Traffic light protocol to code sensitivity of information could be useful (Interviews, 2015-6; FS-ISAC, 2015; BIMCO, 2016). [**R** 6.4.2] The Port of NY and NJ has developed what many regard as a "best practice" for sharing sensitive but unclassified information with private sector partners (Interviews, 2015-6). The process involves individual invitations to a closed door meeting where participants' identification are checked at the door. Participants are typically long-standing AMSC members, and the meeting is chaired by the COTP. If further dissemination of information beyond the meeting is deemed necessary, the USCG vets the information to remove the sensitive material. This process may include a USCG legal advisor if necessary. Once fully vetted, the information is posted to the HOMEPORT portal.

[20] **https://securityintelligence.com/how-stix-taxii-and-cybox-can-help**-with-standardizing-threat-information/

Targeted small briefings, including classified briefings, are vital, but these typically lag events by weeks. Faster sharing is needed. "Slow" sharing can also be done at industry conferences or with AMSCs (Interviews, 2015-6). Research may be needed to automate the filtering and classification of the large volume of information (Interviews, 2015-6). Additional research is needed into the cyber risk management industry issue of filtering the large volume of information available on cyber incidents. More information is not always better, and it can be difficult to filter through the noise to understand what is actually a malicious attack. Key players need to avoid information overload, which can cause actual events to be overlooked as noise. This is not just a maritime cyber issue, but a cyber risk management industry issue in general. [**R** 6.4.2, 6.4.4]

Because information about potentially catastrophic near misses may unduly influence cyber risk management investment decisions (Dillon & Tinsley, 2015), one can ask whether these events should be examined to determine whether resilience was key to the "miss." This could help others to learn from the disseminated information. [**R** 6.4.3]

5.5.Technologies to Support Information Sharing

Technology presents several challenges: Each player must have adequate resources to share and receive information, to protect sensitive information, and to respond promptly enough. The players have to agree on protocols for reporting problems, attacks, and countermeasures. The responsible coordinating bodies must also have technologies for receiving and filtering streams of information, prioritizing them, and classifying them for controlled dissemination to the players.

Rapid sharing requires standardized reporting, etc. The FS-ISAC employs the STIX and TAXii systems that are being developed by a community led by DHS. STIX and TAXii may be relevant for standardized reporting, but they are not software tools. Full implementation should not require vendor specific software (FS-ISAC, 2015-6; Interviews, 2015-6). Several existing protocols/systems could be evaluated to see whether they are appropriate for MTS use (Interviews, 2015-6). For example, the FS-ISAC uses technical systems developed by Soltra, a DTCC and FS-ISAC company. The systems include a threat intel server, SoltraEdge, to aggregate and distribute information about threats (peer-to-peer and firm-to-firm) and the SoltraNetwork that connects these servers in a hub and spoke manner. [**R** 6.5.1. 6.5.3]

Utilizing STIX and TAXii is the new DHS Automated Indicator Sharing (AIS)[21] program. As previously mentioned, this is now used by the NCCIC. AIS is a two-way sharing program, which does not need a human in the loop to share information; the information is shared from machine-to-machine, either from the NCCIC to partners or from partners/industry to the NCCIC.

The National Cybersecurity Protection System (NCPS) is a system of systems providing capabilities to defend the federal government's information technology infrastructure. NCPS broad cyber security capabilities include detection, analytics, information sharing, and prevention. For example, its analytics capabilities include Secure Information and Event Management (SIEM), Packet Capture (PCAP), Enhanced Analytical Database (EADB) and flow visualization, and Advanced Malware Analysis. These or related technologies may prove useful in developing information to share within certain segments of the MTS.

[21] https://www.us-cert.gov/ais

The ability to anonymously submit reports of cyber risk incidents or near misses could allow firms to share information without fears of harming their reputations or incurring regulatory penalties. An example of this kind of anonymized incident reporting is found in the collaboration of the American Bureau of Shipping (ABS) and Lamar University to develop and maintain an online Mariner Personal Safety (MPS) database[22] for tracking maritime injury and close call reports (Interviews, 2015-6). Another example of data anonymization is the Vocabulary for Event Reporting and Incident Sharing (VERIS) framework[23] used by Verizon to gather information for its annual Data Breach Investigation Report. Finally, the FS-ISAC has as one of its Cornerstones that information is able to be submitted anonymously through its technical systems (FS-ISAC, 2015). The M-ISAC or other consortium of MTS partners could increase participation in information sharing by identifying or developing an independent data anonymization platform for sharing cyber risk management incidents and false alarms (Interviews, 2015-6). [**R** 6.5.4]

Recent research in decentralized "trust systems" also may prove helpful (Minsky, 1991; Minsky and Leichter, 1995; Minsky and Ungureanu, 2000). [**R** 6.5.2]

6. Recommendations

6.1. The Role of the USCG and Extending Physical Security to Cyber Security – Cyber Risk Management

6.1.1. We strongly endorse the ongoing USCG effort to develop cyber risk management guidelines analogous to the physical security requirements found in 33CFR Subchapter H.

6.1.2. Since there many diverse players in the MTS, and they have competing interests, we recommend guidelines for the MTS be written at a "high" level – specifying the characteristics of a cyber risk management plan, not detailed technical prescriptions.

6.1.3. We recommend the NIST Framework (NIST, 2014) as a guide for the process of developing cyber risk management plans covering facilities, NIST (1990-2015) as a resource for federal government IT system security, and BIMCO (2016) as a resource for developing cyber risk management guidelines specific to vessels.

6.1.4. We recommend that physical security and cyber risk management be more strongly linked, reflecting the likelihood that a cyber attack may be manifest by physical damage or vice versa. This may be facilitated through the audit systems currently in place, such as found in 33CFR Subchapter H (Maritime Security, 2010), in addition to self-audits. These may also be integrated into current vessel and facility drills, exercises, and trainings. The BIMCO Guidelines may offer some insight of topics to include.

6.1.5. We recommend a research effort to develop cyber risk management performance-based standards and metrics to be used by the USCG in security audits, educational programs, and other

[22] http://ww2.eagle.org/en/rules-and-resources/safety-human-factors-in-design/mariner-personal-safety.html Accessed 3/24/2016
[23] http://veriscommunity.net/index.html Accessed 3/21/2016

applications. Again, these can be added as additional content into pre-existing vessel and facility drills, exercises, and training.

6.1.6. We recommend the USCG develop and roll out the capability to assess and communicate the cyber readiness of the MTS and its components.

6.1.7. We recommend that the USCG increase its effort to coordinate and lead regular cyber risk management exercises in collaboration with the AMSCs and in conjunction with phycial security exercises. Exercises should range in scope and complexity as appropriate from tabletops to full-scale simulated cyber attacks perhaps facilitated by access to a cyber range.

6.1.8. We recommend cyber risk management exercises as opportunities for evaluating proposed organizational structures, performance-based standards and technologies for information sharing within the USCG, and between the USCG, its commercial partners, and other government agencies.

6.1.9. We strongly endorse ongoing USCG efforts to provide guidelines for training to raise awareness of cyber risk management threats for members of the AMSCs. Considerations such as who pays for the training and who develops, delivers and receives the training need to be worked out.

6.1.10. We recommend cyber risk management training tailored to specific components of the maritime system be developed to coincide with, and enhance understanding of, new cyber guidance from the USCG.

6.1.11. We recommend that the USCG expand collaboration with other government agencies (such as NIST, ODNI, Cyber Command, NavSea, and DHS CERT) to develop technical standards for cyber risk management information sharing.

6.1.12. We recommend further research into the appropriate role of the USCG in pushing best practices for cyber risk management to the private sector.

6.1.13. We recommend further research into the appropriate role of the USCG in developing regulations for sharing information about cyber attacks, vulnerabilities, and defenses with the private sector.

6.2.Organizational Systems for Information Sharing

6.2.1. We recommend the USCG enhance its presence at the NCCIC into a 24x7 capability for coordinating with NCCIC partners and reporting cyber risk management alerts, trends and mitigation strategies to the USCG, commercial partners, and other appropriate government agencies.

6.2.2. We recommend that the USCG lead an organization (such as a branch of the NCCIC) for sharing cyber risk information with its MTS partners, which may include several tiers of information corresponding to the type of information to be shared (automated reports of probes vs. discussion of possible trends over time, etc.) with appropriate groups of partners such as ISACs, fusion centers, AMSCs, local FBI offices, and state and municipal law enforcement units. We note that not all MTS partners will be able to participate at all levels of sharing (limitations may be technical, economic, or based on national policy).

6.2.3 We recommend that private industry within the MTS develop and lead an industry-focused organization (such as a re-instantiated M-ISAC) for sharing cyber risk information, providing an arms-length relation to the USCG-led organization in Recommendation 6.2.1. Investigation of the business

and technical models employed by existing organizations such as the FS-ISAC, E-ISAC, ONG-ISAC, and A-ISAC, particularly as relates to supporting anonymous sharing of information, may provide a good starting point for this organization.

6.2.4. We recommend that the industry leaders of the M-ISAC establish membership levels that vary according to the member's size (ability to contribute financially) and industry sector (terminal operator, oil and gas import/export, international shipping, etc.).

6.2.5. We strongly endorse the requirement, proposed in the Strengthening Cybersecurity Information Sharing and Coordination in Our Ports Act of 2015 (Torres, 2015), that each AMSC create a cyber risk management working group or subcommittee, and we recommend the subcommittee meet at least quarterly.

6.2.6. We recommend a system-wide coordination effort to develop a compilation of mission, focus, and operation found at existing AMSC cyber security subcommittees, with results to be shared across AMSCs.

6.2.7. We recommend further research on the best organizational structures for sharing information with components of the MTS that do not have any information-technology-trained personnel.

6.2.8. We recommend that all MTS partners report cyber security incidents, including near misses, to the USCG National Response Center (NRC) until an alternative organization (perhaps the NCCIC) is identified and reporting requirements are specified in the cyber risk management guidelines referred to in Recommendation 6.1.1.

6.2.9. As found by CJOS, "a bottom-up approach is more likely to be supported than an international governance model". We recommend this approach be utilized, emphasizing buy-in from international industry partners as much as possible rather than regulations.

6.2.10. We recommend the American Association of Port Authorities (AAPA) develop cyber risk management guidelines for port facilities, similar to the BIMCO (2016) guidelines for ships.

6.2.11 We recommend that the USCG continue to work with the IMO and monitor their international efforts to establish cyber risk management guidelines.

6.3. Motivation and Barriers for Information Sharing

6.3.1. We recommend that the USCG advise Congress that legislation and/or regulation is needed that requires "landlord" port operators to incorporate maritime risk management standards in their leases to terminal operators and "operating" ports to adopt the standards themselves.

6.3.2. We recommend that "landlord" port operators offer discounts to terminal operators that agree to adopt cyber risk management standards before legislation requires it.

6.3.3. We recommend that "landlord" port operators require their tenants to be members of the M-ISAC once it is reinstantiated.

6.3.4. We recommend that the new M-ISAC communicate threat information among its membership in a way that does not involve the U.S. Government or Law Enforcement in order to encourage

participation by non-U.S. firms. We note that U.S. firms may be required to also (separately) report threat or incident information to an appropriate U.S. authority.

6.3.4. We recommend that industry partners working to establish new information sharing agreements evaluate the incentives used to avoid pitfalls such as free-riding and withholding critical information from competitors in the FS-ISAC, ONG-ISAC and E-ISAC.

6.3.5. We recommend research efforts focused on the following:

6.3.5.1: In-depth interviews with all participants in an AMSC to identify the specific barriers to investment in information sharing faced by these MTS partners. Incentive plans, such as identification of a third-party anonymization service for reporting incidents, can then be proposed to target these specific, MTS-centric barriers.

6.3.5.2: The legal challenges of global cyber risk management information sharing and incentives.

6.3.5.3: Methods to achieve rapid and useful information sharing in a way that both large and small players in the MTS can participate, and in particular on how one can entice larger content providers to take the lead on information sharing.

6.4.What Information to Share, and What to Share Rapidly vs. Slowly

6.4.1. We recommend that categories of information to be shared could be taken from existing sources that include: the TAXII, STIX and CybOX specifications[24], the FS-ISAC categories of information for submission (Incidents, Threats, Vulnerabilities, and Resolutions/Solutions), the threat types listed in CISA 2015, and data elements known to be shared by MTS entities with organizations such as the MS-ISAC.

6.4.2. We recommend development of standardized protocols for managing the sensitivity (as relates to confidentiality and to timing) of information to be shared. Examples of protocols in use that could serve as models are the USCG RGA (Red, Green, Amber) scheme, and the approach employed at the Port of NY/NJ.

6.4.3. We recommend that reports of "near misses" be shared together with an analysis of the apparent reason(s) the attack was unsuccessful.

6.4.4. We recommend additional research into the cyber risk management industry issue of filtering the large volume of information available on cyber incidents (noise vs. malicious). More information is not always better; instead, the research should focus on what is the most important critical information that key players need to avoid information overload, which can cause actual events to be overlooked as noise. Additionally, different MTS partner organizations, and different roles, positions, and levels within these organizations, will require different kinds of filters to ensure the right information reaches each party.

6.5.Technologies to Support Information Sharing

6.5.1. We recommend research to evaluate how existing technical protocols for information sharing (such as TAXii/STIX) are currently at use by MTS partners, such as the MS-ISAC, and how their use could

[24] https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity

be more widely adopted where needed. Rather than identify products from a single vendor, technical recommendations should identify industry protocols supported by multiple software products.

6.5.2. All of the models discussed so far have one or two central nodes, which present a single point of failure (SPOF). We recommend further research seeking distributed models that can deal with the complexities of the MTS without presenting a SPOF.

6.5.3. We recommend a research effort aimed at analyzing the many vehicles for sharing to see what role they may play in a comprehensive information sharing strategy for the MTS. Examples include: HOMEPORT, sharepoint, briefings (internal, other agencies, etc.), DHS Communities of Practice, forums, and automated network monitoring systems.

6.5.4. We recommend that the MTS industry research available anonymization platforms and technologies that could allow commercial partners to share cyber risk information such as incidents and false alarms without fear of negative publicity. Examples include: the online Mariner Personal Safety (MPS) database led by American Bureau of Shipping and Lamar University, the Vocabulary for Event Reporting and Incident Sharing (VERIS) framework[25] used by Verizon to gather information for its annual Data Breach Investigation Report, and the technical systems used by the FS-ISAC to allow anonymous submission of threat information by its members.

7. References Cited

BIMCO, 2016. The Guidelines on Cyber Security Onboard Ships. URL https://www.bimco.org/~/media/Products/Manuals-Pamphlets/Cyber_security_guidelines_for_ships/Guidelines_on_cyber_security_onboard_ships_version_1-1_Feb2016.ashx (accessed 1.12.16)

Burr, R., 2015. S.754 - 114th Congress (2015-2016): Cybersecurity Information Sharing Act of 2015 [WWW Document]. URL https://www.congress.gov/bill/114th-congress/senate-bill/754 (accessed 12.19.15).

C2M2, 2014. Cybersecurity Capability Maturity Model, Version 1.1. Department of Energy, February, 2014. URL http://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf (accessed 2.15.16)

CIS, 2015. CIS Critical Controls for Effective Cyber Defense Version 6.0. Center for Internet Security. URL http://www.cisecurity.org/critical-controls.cfm

Clark, B.G., and Roberts, F., Summary Report of Findings: Maritime Cyber Security Research Summit, July 2015.

[25] http://veriscommunity.net/index.html Accessed 3/21/2016

CSET Cybersecurity Evaluation Tool, 2015. YouTube Video Tutorial: 13 CSET 6.2 Questions Screen. URL https://www.youtube.com/watch?v=CfRDUqA5WnI

Davies, M., 2003. Obligations and Implications for Ships Encountering Persons in Need of Assistance at Sea. Pac Rim Pol J 12, 109.

Department of Homeland Security (DHS). Cyber Resilience Review. URL https://www.us-cert.gov/sites/default/files/c3vp/crr-fact-sheet.pdf

Dillon, R., Tinsley, C., Near-Misses and Decision Making Under Uncertainty in the Context of Cybersecurity. Ed. Book, Improving Homeland Security Decisions, forthcoming.

European Network and Information Security Agency (ENISA), 2010. Incentives and Challenges for Information Sharing in the Context of Network and Information Security.

Financial Services Information Sharing & Analysis Center (FS-ISAC), 2015. Operating Rules. URL https://www.fsisac.com/sites/default/files/FS-ISAC_OperatingRules_2015.pdf (accessed 1.12.16).

Gal-Or, E., Ghose, A., 2005. The Economic Incentives for Sharing Security Information. Information Systems Research 16(2), 186-208.

Interviews, 2015-6. Interviews with Industry and Other Experts, Conducted by CCICADA.

ISO/IEC, 2013. International Organization for Standardization, ISO/IEC 27001 – Information Security Management.

Konon, J., 2014. Control System Cybersecurity: Legacy systems are vulnerable to modern-day attacks. Proceedings of the Marine Satefy & Security Council, the Coast Guard Journal of Safety at Sea 71(4), 45-47.

Laxminarayan, R., Reif, J., Malani, A., 2014. Incentives for Reporting Disease Outbreaks. URL http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0090290. (accessed January 12, 2016).

Maritime Security, 33CFR Subchapter H pt. 101-107 (2010). URL https://www.gpo.gov/fdsys/granule/CFR-2010-title33-vol1/CFR-2010-title33-vol1-part101 (accessed 1.12.16).

Minsky, N.H., 1991. The imposition of protocols over open distributed systems. Softw. Eng. IEEE Trans. On 17, 183–195.

Minsky, N.H., Leichter, J., 1995. Law-governed Linda as a coordination model. Springer.

Minsky, N.H., Ungureanu, V., 2000. Law-governed interaction: a coordination and control mechanism for heterogeneous distributed systems. ACM Trans. Softw. Eng. Methodol. TOSEM 9, 273–305.

National Institute for Standards and Technology (NIST), 1990-2015. Special Publications SP-800 Computer Security. URL http://csrc.nist.gov/publications/PubsSPs.html#SP%20800

National Institute for Standards and Technology (NIST), 2014. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0. URL http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf (accessed 1.12.16)

National Institute for Standards and Technology, 2015. Overview of the Cybersecurity Framework. URL http://www.nist.gov/cyberframework/upload/cybersecurity_framework_coast_guard_maritime_public_meeting_2015-01-15.pdf

National Institute for Standards and Technology (NIST), 2016. Cybersecurity Framework Comments Reveal Views on a Framework Update, Increased Need to Share Best Practices and Expand Awareness. URL http://www.nist.gov/itl/acd/cybersecurity-framework-comments-reveal-views-on-a-framework-update.cfm

National Institute for Standards and Technology, 2016-2. Analysis of Cybersecurity Framework RFI Responses. URL http://www.nist.gov/cyberframework/upload/RFI3_Response_Analysis_final.pdf

Torres, N., 2015. H.R. 3878 – 114th Congress (2015-2016): Strengthening Cybersecurity Information Sharing and Coordination in Our Ports Act of 2015. URL https://www.congress.gov/bill/114th-congress/house-bill/3878/text (accessed 1.12.16).

United States General Accounting Office (U.S. GAO), 2001. Information Sharing. Practices that can benefit critical infrastructure protection. Washington, D.C.

(This page intentionally left blank.)

APPENDIX B. COVERING MARITIME CYBER SECURITY OBJECTIVE: HOW DO WE PROMOTE THE USE OF SOUND CYBER RISK MANAGEMENT PRINCIPLES?

American Military University
AMU
A member of the accredited American Public University System

WHITE PAPER STUDY IN CONJUNCTION WITH THE

COVERING MARITIME CYBER SECURITY OBJECTIVE:

"HOW DO WE PROMOTE THE USE OF SOUND CYBER RISK MANAGEMENT PRINCIPLES?"

April 2016

Unclassified 1

American Military University
AMU A member of the accredited American Public University System

EXECUTIVE SUMMARY

With the many types of Maritime Cyber Security Threats in existence, there comes the need to prepare and contain such risks in a responsible and intelligently aggressive manner. To assist in this endeavor, this White Paper is the culmination of extensive research conducted by an American Military University /American Public University (AMU/APU) Research Team which met from November 2015 to January 2016. The team consisted of members of several governmental and civilian entities associated with the Department of Homeland Security, Department of Defense and the National Security Agency, including seasoned military personnel from the Navy, Coast Guard, Air Force, Army, Marine Corps, and the National Guard. Researcher biographies follow the Conclusion. Tasked to answer the objective "How do we promote the use of sound cyber risk management principles?" their combined experience and insight greatly added to the direction and focus in providing the very best research and recommendations to the leadership of the United States Coast Guard (USCG). In this research, the AMU/APU team placed a great deal of emphasis on locating ways in which both an organization and the United States as a whole can be affected by Cyber Security Threats, which is ultimately the initial step that must be completed in any risk management strategy. The team then determined the most important elements of those risks and how to mitigate them. These techniques were then integrated into the mitigation process within a promotion and resiliency strategy to ensure that, in the event of a cyber attack, the USCG would be able to successfully and efficiently respond. Based on an extensive literature review, the team evaluated the risks, possible ways to mitigate them, and how to respond through promotion methods by organizing them into five areas designated as pillars: Awareness, Flexible and Adaptable Security, Domain Understanding, Enabling the Mission, and Risk Management. Each of these pillars stands for a very important aspect that must be understood and implemented unanimously, for if one is not constructed as an equal with the others, the entire structure falls apart. Through this design and understanding, promotion of sound cyber risk principles is obtained.

Unclassified 2

American Military University
AMU A member of the accredited American Public University System

INTRODUCTION

For many Americans, the advent of technology and its advantages are taken for granted. Their own personal safety and security tends to be something they rarely ever consider until something goes wrong and it is far too late to respond. It is the responsibility of those who have the ability to protect the American public and, ultimately, the world, from the growing threat that a cyber system poses not only to our National Security, but our own individual security.

For a majority of consumers, the worldwide web, ancillary networks and anything coupled to it should be simple, efficient and as convenient as possible. This means the consumers desire what many industry leaders have begun to provide such as a single username and password across all possible combination of devices and systems that can accomplish nearly everything they might achieve on a daily basis. This concept of simplicity seems like a great idea; however, the more things become connected to a single or non-complex pathway activity, the higher the risk involved. Why does centralizing and simplifying things within the cyber realm create greater security risk? Simply, attackers ultimately need to figure out less ways to access all necessary information to plan and carry out not only a cyber intrusion, but also a physical attack on a target of their choice. In this day and age, that also means attacks on the even easier target of individual personnel. In the intelligence realm, we all know that the easiest way to solve a problem is to break it into several pieces like a puzzle. Then, you begin to put it together, one piece at a time rather than trying to create an entire picture in a single event. When cyber security becomes involved, it no longer takes an entire team to acquire this information efficiently. Theoretically, a single individual who has even the smallest amount of background in computers and a $500-dollar laptop can do the same task in a matter of hours. That individual could hack into targeted agencies' or companies' records, which are now all stored digitally, such as the Office of Personnel Management which was hacked in the summer of 2015 (Weintraub Schifferle, 2015). Those hackers potentially can gain access to nearly every starting point they may need, for an attack on every individual's personal information who has ever applied to work with the government.

Unclassified 3

For individual agencies such as the United States Coast Guard (USCG), which this study was specifically prepared for, this means preparing for added responsibilities outside maintaining protection for the homeland as their mission states. They must also protect their personnel, personnel's information, and their own agency from both the threat of external attack, as well as that of an insider. In addition, it compels the USCG to inform companies of potential Maritime Cyber Security Threats. If any one area fails to maintain security, the entire system can collapse. Therefore, all agencies, individuals and government need to heighten their focus on risk management and security from not only physical threats, but also cyber attacks. These issues also affect the Maritime Transportation System in their daily management of international shipping. Yet, despite technological advances, the critical infrastructure concerns are threatened, to some degree, by these same mediums. Cyber communication is now the most pertinent medium of communication of any type, in any situation. Electronic communication involves the spread of information, and information is power. It is for this reason that all security professionals also recognize that we not only have to be pro-active to manage all these risks, but also figure out ways to be resilient in the event an attack is successful. "Resilience" is the ability to rebound after something difficult. So in the event of a cyber attack, for example, shuts down all critical infrastructures, how does an agency proceed? Will the agency fall apart or will it return even stronger and bounce back quickly. To best accomplish the goal of an enhanced and strengthened recovery, this team proposes weaving a layered security network, recognizing the cyber environment as its own vulnerability and using everyone to safeguard against threats. To do this, we must focus on promoting three primary things: Teamwork, Resilience and Risk Mitigation by utilizing and incorporating, different departments and agencies, with the common goal of cyber security and safety in mind.

RESOURCES AND METHODOLOGY

The AMU Team utilized scholarly resources that can be verified such as government publications, peer reviewed articles and other such verifiably accurate documents.

In a two-month timeframe, the team's initial research commenced with a comprehensive list that was presented to the team by AMU instructors and then new information developed by different members of the team selected to a specific area.

Furthermore, the research presented a peculiar challenge for the team, as the intended recipient may be from a completely unclassified environment, and many of the potential pieces of research are at minimum restriction or above and could not be used. Yet, members of the team know some of the data of such reports.

The qualitative approach was selected to best accommodate the available resources, time constraints of the project, and the intended end user environment, while at the same time allowing for the most complete analysis available from the team.

Pattern Matching

-Cyber Security is a problem in other realms; therefore, cyber is a problem in the maritime environment, as the same concerns exist as in other environments. This realization requires educated assumptions as to how they correlate in order to best deal with the threats.

Content Analysis

-Key concept grouping

-Indexing, categorized by grouping key words and themes

Cases Studies / Secondary Analysis

-Use already published records and data

-Use current and valid data: the cyber world is fast moving and evolving in nature

By addressing our methodology in this manner, we have also organized our analysis and recommendations in a logical way, which answer many of the questions an intelligently aggressive leader is looking for on a topic such as risk management.

American Military University
AMU A member of the accredited American Public University System

Status of the Research, Gaps, and Areas of research that need further exploration:

New and emerging field and focus

-Additional research is needed, especially in maritime area

-Landscape of threat changing constantly

-Many of the answers have not yet been found and the questions are in constant evolution

Evolving and growing field

-Many gaps in research due to fast evolving variables-The technology is advancing faster than the response to it

-Qualitative/Creative thought is needed to attempt to predict the future of the cyber world and possible threat from it

Trends of attack types

-Criminal, terrorism and espionage remain as constantly expanding vital concerns. Additional research and information sharing remain, to determine whether or not there is any relationship between them or if they are distinctly separate

Promoting Cyber Security

-Focusing on training all personnel on the importance of Cyber Security principles (first step in any risk management is awareness)

-Limiting or not allowing personal use of networks at work

-Encouraging teamwork not only among members of the same entity, but also between other entities

Unclassified 6

American Military University
A member of the accredited American Public University System

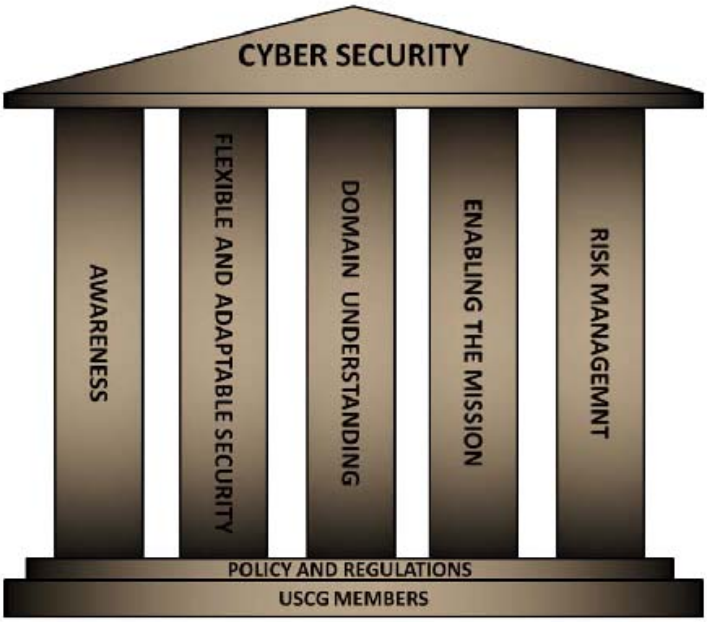
The Cyber environment

-Extremely porous with multiple vulnerabilities

-A wide variety of players and customers with diverse levels of structure and security needs

-Will require a multi-phase approach to engage and minimize the threat environment.

The task - facing the cyber domain will require dealing with the 5 primary pillars built upon a base of policy and regulations and enacted by the Maritime Transportation System.



1. **Awareness:** All players must realize there is a threat. Research indicated that the threats posed and the level of sophistication of adversaries is much greater than personnel realize. These threats are rapidly evolving and there must be continual education, awareness and training.

Unclassified 7

2. **Flexible and Adaptive Security:** with a wide range of players at multiple levels, the security will need the ability to spread across a varied cyber-scape and be scalable in order to be usable to all levels of players.
3. **Domain Understanding:** there must be an understanding of the terrain of the cyber-scape and the range of threats in that terrain. The Maritime domain is extremely varied and vast in its scope, as such it presents a broad range of potential threat domains. In order to effectively deal with each domain, the awareness of the challenges to each must be understood by those in it.
4. **Enabling the Mission:** it is critical that all parties are enabled, possibly at different levels, to deal with the threats in the cyber environment. From sensitive and secure to completely un-vetted, players must have information available to them at varying levels of security that enables the cross sharing of information.
5. **Risk Management:** not all threats can be stopped, or immediately dealt with. There must be a planned risk management structure to deal with the range of threats and manage them at an acceptable level.

Promotion Method Solutions: Building upon the pillars of understanding cyber security, we move toward promotion methods. We will examine some of the areas, which the research indicates needs to be addressed and further explored.

The concept of understanding cyber security naturally leads to the principles of risk management in the above referenced category, and if followed helps make others aware of how important it is.

There are only a few ways of promoting anything -Essentially filling some need (monetary, country, self image, fear of job loss, devotion to duty or a cause).

How do we promote? The act of motivation deals with a goal or purpose, or encouragement toward an outcome.

American Military University
AMU A member of the accredited American Public University System

Types of Motivation: Positive and Negative

Positive Motivation

Recognition or awards: National, local (i.e., best new cyber safety practice, etc.) in the industry through newsletters, magazines or industry awards.

Creation of a New Field: Prestige needs to be added to the security offices within the shipping companies and ancillary companies that support them. This recognition will alert the shipping companies and their customers of which entities are pursuing best practices in countering the threats through education directed action and training in real-time scenarios. Prestige needs to be added to the IT/Cyber/Intel sector, as this is a fast evolving field with major ramifications.

Education:

-Establish a Cyber Department and stronger IT support

-Attract qualified graduates via signing bonuses and special pay programs

-Use combination of online learning modules, specific courses, and conferences to develop and maintain cyber proficiency

-Send personnel to cyber specific schools, such as Defense Cyber Investigations Training Academy (DCITA)

Creation of an Innovation Hotline or email address:

-This would be from inside a company, identifying real vulnerabilities and hopefully giving actionable solutions toward fixing them (give a quarterly award for best idea, best vulnerability identified best solution, etc.), obviously praise and reward these people

-Rewards: for turning in malicious emails (monetary, passes, free computer/electronics, etc.)

Unclassified 9

American Military University
AMU A member of the accredited American Public University System

Raising Awareness:

Weekly Cyber Newsletters or email:

-This is what we are seeing

-This is what happened

-This was the repercussion or punishment of this incident

Technology: Networks

-Quarantine Zone (or firewall) of sorts that establishes a set boundary between inside and outside a network

-The ability to scan outside data/incoming messages before they are allowed access – should be primarily automated and less human initiated

-The use of WIFI and Bluetooth technology makes these steps difficult, but they need to happen

Technology: Bio-scan vs. Password Access

-Using fingerprint scanning or facial recognition for system access instead of passwords

-We need to remember too many passwords that are getting longer and more complex

-You must change them too frequently and not able to reuse past ones

-This forces them to be written somewhere or forgotten (causing vulnerability and access delays)

-This gives approved personnel easier secure access, prevents aggravation

-Less chance of creating workarounds (such as writing down of passwords) = less insider threats

Unclassified 10

American Military University
A member of the accredited American Public University System

Negative Motivation

Held Accountable:

Widely based on punishment or fear (jail, civil lawsuit, job loss, discharge)

Repercussions for failure to follow procedure:

-Forced to take a class or present a class to co-workers on an incident/best practices (raising awareness which is the most important)

Overall Environment Including Port Security:

-Mandate regular patch updates from all vendors and those who have access

-Mandate sharing of data on cyber attacks with partners who track and combat such efforts

-Offer preferred status to companies/partners with high standards of Cyber Security, for example one's with dedicated Cyber Security and Data Breach reporting officers. This enhances port security operations

-Enact data monitoring and possible disabling of access of employees deemed high risk or disgruntled, and those who show signs of meeting that criteria

AMU/APUS RESEARCH: THE RIGHT CHOICE AND RESEARCH STUDY FORCE MULTIPLIER

Inclusion of AMU/APUS is an important addition to any military (or civilian) research project. AMU/APUS brings a unique perspective based on an expansive background. Students at AMU/APUS are comprised of military and other government agency members from a broad array of technical areas. This broad experience base serves as a significant force multiplier – as even a small number of individuals involved in a study such as this one, provides a broad reach with a tremendous depth of expertise. Facilitating this study we have a combination of active duty and prior service members representing Navy, Army, Air Force, Marine Corps, Coast Guard, National Security Agency, Custom and Border Patrol and other civilian agencies giving us a wide range of

Unclassified 11

standard operating procedures and tactics used throughout the US Government and Cyber Security environment unmatched by other options! AMU/APUS involvement is a valuable partner in any future research or study, especially those relating to Department of Homeland Security and Department of Defense procedures and policy implementation.

What Remains in the Near Future

Cyber security professionals are in great need, not just in the maritime industry, but also in all aspects of government and businesses, in general. There are not enough security professionals to keep pace with the ever-advancing technology. According to Lee and Rotoloni, "…there is a significant lack of trained security experts, which will result in a shortfall of as many as 1.5 million workers by 2020" (Lee and Rotoloni. 2015, 4). Trying to overcome these shortfalls is no easy task because it takes years for students to obtain a degree in cyber security and another year of on-the-job training to become proficient in defending networks, "When Intel hires a new computer science or engineering graduate for a security position, it takes about one year to train…them for their work…" (Lee and Rotolini. 2015, 5). Training these professionals is a long-term solution that will eventually provide much needed cyber security. Furthermore, the USCG should work towards increasing their cyber security staff to include hiring more contractors to fill in personnel gaps.

One way to enhance cyber security, is simply to educate employees about the safety practices that should be taken while working online, "Companies need to focus on educating their employees about security issues – teaching them about the dangers and consequences of phishing, unencrypted data and lax reactions (Lee and Rotolini. 2015, 6). Most employees may not be aware that what they do at work could be a potential risk to the network; therefore, unintentionally compromise the work place. Simply connecting while in the Maritime environment could open the door to dangerous attacks as many network connections are already infected with a variety of attacks waiting to strike.

One cyber expert reported that after he visited a ship, he would routinely destroy his own laptop. He said that was a reasonable action to take, considering the level of contamination by viruses in the systems he saw afloat. Routinely, pirated software can be found in navigational systems. Also a hazard is external devices brought aboard by the crew, which are also heavily contaminated. (Grey, Michael. 2016).

By incorporating cyber awareness training, employees will be less prone to accidentally compromising the network. Furthermore, this is a simple way to enable employees to be security assets rather than a hindrance to network security. If need be, "Companies should, if appropriate, clamp down on personal use of employer-issued devices to minimize threats or monitor the use of consumer devices in the workplace (Lee and Rotolini. 2015,6). Removing these devices would maintain security in the workplace. Employers could utilize a safe space for devices to be used and lockboxes to safely and securely store their devices before re-entering their place of work.

Additionally, the national government needs to realize vulnerabilities within their port infrastructures and provide the necessary training and manpower to successfully improve their cyber security (Jensen. 2015, 38). Cyber-attacks on ports can have damaging effects on the economy because such attacks can cause crippling delays in the importing and exporting of goods to different countries. Various delays due to natural disasters highlight the economic importance of the shipping industry, "Northeast ports lost an estimated $50 billion -- $1 billion in cargo delays alone – because of Hurricane Sandy in 2012." (Walters. 2015, 1) Furthermore, "In 2002, the key ports on the western coast of the United States were shut down for ten days due to a labour dispute…it was estimated that this had a cost to the United States economy of $1-2 billion USD per day due to disrupted supply chains. (Jensen. 2015, 35) Complex cyber-attacks by technically advanced adversaries can produce these same results or worse if the industry cannot adapt to new threats.

This realization cannot occur too soon as the threat level is increasing at a dramatic rate. "The number of incidents reported by federal agencies to the federal information security incident center has increased by nearly 680 percent" (Wilshusen. 2012).

Further, not only are the number of attacks increasing, but the sophistication and caliber of the attackers is also ramping up to unseen levels of participation:

- Iran: "…with a massive attack on U.S. bank websites in 2012."
- North Korea with its "hacking of Sony Pictures last year."
- "Russia is a near peer to the United States… The country's use of cyber offensive operations has been documented both in Georgia in 2008 and more recently with Russia's invasion of Crimea in 2014." (Su, E. 2015. P. 4)

The effect of the increased sophistication and capability can be felt in industries once considered ultra-secure such as national and state power grids in the U.S. and abroad, as well as closely protected information used in multinational corporate negotiations:

1. In Florida, a hacker caused a large power outage as he strayed while attempting to map the infrastructure.
2. Overseas breaches of utility computer systems have occurred, with some resulting in power outages and attempted extortion, as ransoms were demanded. The attacks were validated by the CIA. Access is believed to have occurred through the Internet.
3. There is "…a huge increase in focused attacks on our national infrastructure networks" The source(s) of the attacks is/are believed to be foreign.
4. As executives travelled through China, spyware was uploaded into their networks. "cyber counterintelligence" threat (Harris. 2008).

The data is clear, the cyber world is no longer secure, and the elements making it less secure are increasing exponentially with expanding sophistication.

Governments need to take charge of their cyber security programs and to seriously address cyber security issues. This should include working closely with departments and to develop interagency cooperation in terms of finding solutions to cyber security problems, "Domestically, agencies should address continuity and simplicity in identifying cyber threats, such as the definition and severity of threats, attacks, and solutions, while avoiding the creation of catch-all regulation that hinders business" (Walters. 2015, 3).

While a catchall regulation could potentially hinder business, the body of research indicates a broader solution approach such as a common regulation standard would be a good start to dealing with the threat, but such a step would be very complicated, involve multiple jurisdictions and governments, and need to cover a wide range of systems. As a result, a single common environment is viewed as unlikely in the near term. "Cyberspace is currently seen as "ungovernable, unknowable, makes us vulnerable, is inevitably threatening and is inhabited by a range of threatening and hostile actors" (Barnard-Wills and Ashenden. 2012).

The situation in the United States alone is extremely challenging and complicated as even with a single government body, and examining only the requirements for the

Maritime areas, protecting the nation will require a collective effort that involves cooperation between all agencies and departments in the United States to come together to create comprehensive security measures to protect America's ports.

Further, the creation of comprehensive measures will require a change in thinking and assessment in order to reach such measures, which may add to the challenge. "The authors describe the problem not being the lack of cyber security promotion but the inability of policy makers to fully understand the risk of cybersecurity as being the problem. (Kelic, A., Collier, Z. A., Brown, C., Beyeler, W. E., Outkin, A. V., Vargas, V. N., . . . Linkov, I. 2013).

In a sense, the cyber security world is evolving into a realm that will need to be looked at as new, and in new ways even though much of it is currently in existence, in order to grasp what will be needed in the future.

Going on, in order to truly secure America's ports, there also has to be coordination internationally, "Increasing cyber information includes working with international partners because cyber attackers may enter U.S. port networks by any available means" (Walters. 2015, 3). Working with other countries and international organizations can truly make the maritime industry's cyber security reforms successful. Attempts are underway in Europe to address the challenge in broad reach. "The European Union has been tinkering with, but has not yet implemented, a single Europe wide Data Protection Directive that would equalise regulation across all EU States" (Lackie, Lara. 2016).

If those involved in the Maritime industries can agree and execute a streamlined cyber security strategy, then it would be much easier to monitor threats and share vital information pertaining to cyber-attacks. Doing this would involve the International Maritime Organization and although it would take a few years to come to an agreement on a streamlined cyber security strategy, it would be a step in the right direction (Jensen. 2015, 38).

Sound maritime cyber security is a complex task that will require the help of all those involved in this industry, but not to do so could prove catastrophic. "Imagine shutting down a port. Imagine running a ship aground. These are the kinds of implications we're worried about."- Todd Humphreys, a GPS expert at the University of Texas. (Roberts, John. 2013)

Such scenarios may seem extreme, but when looking for a baseline view of where overall industry standards currently stand outside the maritime environment, even among such sensitive areas as government personnel records, a recent audit found the mandatory regulations were not being adhered to.

A recent comment indicated "…only 75 percent of OPM's critical systems had valid authorizations in accordance with FISMA [Federal Information Security Management Act] regulations, and in January, an inspector general audit of OPM that deemed the agency's cyber security sufficient relied on unverified data simulation…" (Kanowitz, S. 2015).

When it comes to the maritime environment, and ships, a recent study indicates the scenario is even worse. A Copenhagen-based firm believes even larger vulnerabilities exist from unpatched Microsoft servers that could allow attackers to exploit and take control of the servers. Microsoft had released patches in April but spot checks revealed 37% of the servers haven't been patched (Network World. 2015).

Which leads to a conclusion that not enough is being done to deal with the potential threat, especially in non-mandated areas of concern. In short, there may be entire systems that are already potentially severely infected in the Maritime Industry environment.

CONCLUSION

The UCSG should work towards getting those involved in the maritime industry to formulate a comprehensive cyber security strategy that will streamline maritime defenses. Doing so will allow for adequate information sharing which will make it easier to identify weaknesses and potential cyber-attacks that could have crippling effects.

The impact of the attacks are already impactful, "2015 saw some of the biggest data hacks to date costing the global economy some US$400bn, highlighting the inability of companies to properly guard valuable entrusted data (Lackie, Lara. 2016)."

Furthermore, information technology professionals and security experts need to stay informed when it comes to new ways terrorists and criminals implement new viruses and ways to hack network systems. Learning these new advancements can help provide them with the necessary knowledge to develop tools to combat cyber terrorism and cyber-criminal activity. If the Maritime environment follows suit with traditional non-

maritime corporate environments, there will likely be a new broad acceptance of the position of Cyber Security Officer finding its way into business leadership. This move will likely come as a result of the high cost, and potential liability, according to Lackie's research, which theorizes the new reporting officers will become a part of organizational fabric across the globe as enforcement steps up in response to the expense. The enhanced enforcement already exists in the Unites States and is expected soon in Europe.

Developed work/supporting materials available

(1) PowerPoint Brief
(2) Open Source Literature Review

American Military University
A member of the accredited American Public University System

AMU/APUS RESEARCH TEAM

Jessica L. Adkisson, Petty Officer Second Class, U.S. Navy. Currently stationed at Naval Air Station Fallon, Nevada working as an intelligence specialist. Bachelors of the Arts Degree in Global Legal Studies from Arcadia University also studied abroad at both the National University of Ireland in Galway, Ireland as well as the University of the Western Cape in Bellville, South Africa. Active duty for the USN for four years, previously deploying on the USS Harry S Truman.

Jacob A. Babb, Master Sergeant, U.S. Air Force, Emergency Manager currently stationed at Kirtland Air Force Base as an instructor for the Defense Threat Reduction Agency. Bachelor of Arts in Disaster and Emergency Management from American Military University. Served active duty Air Force for 16 years as a Satellite, Wide-band and Telemetry Communications technician and as an Installation Emergency Manger.

Eric S. Casida, Lieutenant, U.S. Coast Guard, HC-130H Aircraft Commander, currently stationed at Air Station Barbers Point, Hawaii, Seven years active duty. Bachelor of Science in Aviation Technology from Metropolitan State University. Previously Duty Stations: Sector New Orleans Response-Enforcement, and Air Station Sacramento.

Frank S. Hooton, Lieutenant, Texas Military Department, attached to Texas Department of Public Safety/Texas Rangers Division, Commanding Officer Rio Grande Valley Joint Operations Intelligence Center. Holds a Bachelor of Arts in Journalism from San Diego State University. Serving Active duty, deployed to Operation Border Star. Began service graduating from USMC OCS at Quantico.

Gabriel Nunez, Specialist, U.S. Army, Currently stationed at Camp Zama, Japan serving as an intelligence specialist. Bachelor of Arts in Political Science and International Studies from Loyola University Chicago. Served in the Army since 2012 and deployed to Afghanistan in 2013 in support of Operation Enduring Freedom.

Jeremy Quittschreiber, Sergeant, North Dakota Army National Guard, Attended University of North Dakota, Bachelor of Science in Criminal Justice. Served in the North Dakota Army National Guard for five years as an Avenger Team Chief, is currently an E-5/SGT and has mobilized in support of Operation Noble Eagle. Currently employed as an EMT-B with Essentia Health EMS and license eligible to be a Police Officer in the State of Minnesota. Currently working toward continuing service with the North Dakota Air National Guard.

Joshua 'Jay' S. Weisbecker, Captain, U.S. Army, Military Intelligence Officer, currently stationed at Joint Base San Antonio, Lackland Air Force Base in San Antonio, Texas. Bachelor of Arts (Cum Laude) from Chaminade University of Honolulu, double major in Political and Historical Studies. Served in the U.S. Army since 2003, as a Section Sergeant, Platoon Sergeant, Platoon Leader and Executive Officer. Two combat deployments in support of Operation Enduring Freedom and Operation Iraqi Freedom.

Unclassified 18

American Military University
A member of the accredited American Public University System

AMU/APUS ACADEMIC MEMBERS

Dr. Nicole Drumhiller joined American Public University System in 2012 and is currently the Program Director for the Intelligence Studies program. Since 2006 she has taught courses on international politics, comparative politics, security studies, political psychology, and civil liberties. She is currently working on a number of collaborative projects, including her work assessing physicians that have become political dictators; she is also carrying out a collaborative project looking at the perceptions of terror among targets of the radical environmental and animal rights movement; and she is also working on a co-edited book specific to maritime cyber security.

Dr. Eduardo V. Martinez holds a Juris Doctorate and has been active in intelligence and emergency management at the federal level including the U.S. State Department and US Navy. In 2010, following a tour as a Navy Emergency Preparedness Liaison Officer, in which he was involved in efforts related to Hurricanes Gustav, Wilma and Rita and Katrina, and the Deepwater Horizon Oil Spill, he was named as the Executive Director, National Transportation Security Center of Excellence. Dr. Martinez has been an educator of Security Management at APUS since 2014.

Unclassified 19

American Military University
A member of the accredited American Public University System

REFERENCES

Barnard-Wills, D., & Ashenden, D. (2012). "Securing virtual space: Cyber war, cyber terror, and risk". *Space and Culture, 15(2), 110-123.*

Grey, Michael. (2016). "Cyber Attacks - Coping with New Threats to the Maritime World." *Seatrade Maritime News.*

Harris, S. (2008). China's cyber-militia. *National Journal, 40*(22), 16.

Jensen, Lars. 2015. "Challenges in Maritime Cyber-Resilience," *Technology Innovation Management Review*, (April): 35-39.

Kanowitz, S. (2015). "Old technology, poor governance to blame in OPM breach, report finds." *FierceGovernmentIT.com*. .retrieved from http://www.fiercegovernmentit.com/story/old-technology-poor-governance-blame-opm-breach-report-finds/2015-07-20?utm_medium=nl&utm_source=internal&mkt_tok=3RkMMJWWfF9wsRons6jJdO%252FhmjTEU5z14uQrW6CylMI%252F0ER3fOvrPUfGjI4DSsVrM6%252BTFAwTG5toziV8R7LMKM1ty9MQWxTk

Kelic, A., Collier, Z. A., Brown, C., Beyeler, W. E., Outkin, A. V., Vargas, V. N., . . . Linkov, I. (2013). "Decision framework for evaluating the macroeconomic risks and policy impacts of cyber attacks". *Environment Systems & Decisions, 33(4), 544-560.*

Lackie, Lara. (2016). "2016 – the rise of the cyber security and data breach reporting officer." *Itsecurityguru.org*. Retrieved from http://www.itsecurityguru.org/2016/01/07/2016-the-rise-of-the-cyber-security-and-data-breach-reporting-officer. Retrieved from http://www.itsecurityguru.org/2016/01/07/2016-the-rise-of-the-cyber-security-and-data-breach-reporting-officer/

Lee, Wenke and Rotolini, Bo. 2015. "Emerging Cyber Threats Report 2016," *Georgia Institute of Technology*, (October): 1-17.

Network World. (2015). Maritime Cybersecurity Firm: 37% of Microsoft Servers on Ships Vulnerable to Hacking." *Network World*, May 4, 2015.

Roberts, John. (2013). "EXCLUSIVE: GPS Flaw Could Let Terrorists Hijack Ships, Planes." *Technology Fox News*. Retrieved from http://www.foxnews.com/tech/2013/07/26/exclusive-gps-flaw-could-let-terrorists-hijack-ships-planes.html.

Su, E. (2015). "China Reveals Its Cyberwar Secrets". *Reuters.*

Walters, Riley. 2015. "The U.S. Needs to Secure Maritime Ports by Securing Network Ports," *The Heritage Foundation*, No. 4353 (February): 1-3.

Weintraub Schifferle, Lisa. 2015. "OPM data breach – what should you do?" *Consumer Information* (blog). *Federal Trade Commission*, June 4. Retrieved from http://www.consumer.ftc.gov/blog/opm-data-breach-what-should-you-do.

Wilshusen, G. (2012). "Cybersecurity, Threats Impacting the Nation." *GAO-12-666T Cyber Threats*.

(This page intentionally left blank.)

APPENDIX C. ECONOMIC CONSEQUENCE ANALYSIS OF MARITIME CYBER THREATS

National Center for Risk and Economic Analysis of Terrorism Events

University of Southern California

Economic Consequence Analysis of Maritime Cyber Threats

by

Adam Rose

with

The Maritime Cyber Economic Consequence Analysis Working Group

April 18,, 2016

Economic Consequence Analysis of Maritime Cyber Threats

by

Adam Rose[1]

I. Introduction

The development and implementation of cyber technology is accelerating at a rapid pace in all facets of society. This is especially the case in areas of national defense in general and in the maritime domain in particular, where the U.S. Coast Guard is charged with the safety and security of vessels and ports. While cyber systems enhance defense and business operations, they also make them more vulnerable to disruptions because of the increased network dependency.

One major example pertains to cyber threats affecting ports. The impacts are wide ranging and not just confined to individual ships, cargo damage, or port operations. They cause a disruption in downstream supply chains for U.S. businesses depending on imports in their production process. They also cause a short fall in the supply to satisfy consumer demands. Analogously, they disrupt upstream supply-chains relating to U.S. exports whose production is halted because goods cannot be transported overseas. Actual events and simulation studies have indicated losses of tens of billions of dollars from various broader impacts of port disruptions (see, e.g., Cohen, 2002; Park, 2008; Rose and Wei, 2013; Werling, 2014). Cyber disruptions could have similar outcomes.

However, those affected do not stand by passively. They undertake various types of post-disaster resilience by using remaining resources more efficiently and recovering more quickly. These responses take place with regard to cyber capability and also other aspects of port operations such as the use of excess capacity and ship re-routing. Other resilience tactics are implemented up and down the supply chain, such as use of inventories, conservation, input substitution, and lining up new suppliers).

The purpose of this white paper is to set forth a comprehensive framework for the estimation of total economic consequences of maritime cyber threats. This includes a categorization of threats and how they directly affect port operations. It includes a characterization of the major types of indirect, or ripple, effects this may cause. It also includes the specification of cyber resilience tactics that can reduce business interruption losses.

We will utilize this framework to develop a rapid estimation capability for the economic consequences of maritime cyber threats. The principal investigator has recently led a research team that developed a user-friendly software system capable of providing such rapid estimates for a dozen diverse threats to the U.S. economy (Rose et al., 2015). This decision support system is known as the Economic Consequence Analysis Tool, or E-CAT. The next step is to incorporate several types of cyber threats into this platform.

---

[1] The author is Research Professor, Price School of Public Policy, University of Southern California (USC), and Faculty Affiliate, Center for Risk and Economic Analysis of Terrorism Events (CREATE), USC. This research is funded by U.S. Department of Homeland Security under Grant Award Number 2010-ST-061-RE0001-05. The author acknowledges the collaboration of Dan Wei on previous port studies, the collaboration on the development of the Economic Consequence Analysis Tool (E-CAT) of Fynn Prager, Zhenhua Chen and Sam Chatterjee, and the research assistance of Joshua Banks and Noah Miller. This summary also received valuable input from members of the Maritime Cyber Economic Consequence Analysis Working Group (see Appendix A). The author is, of course, responsible for any errors or omissions.

The enhanced software system is intended to help high-level decision-makers in the maritime cyber domain assess the severity of various threats in real time. This is a key aspect of a benefit-cost analysis or risk-benefit analysis, as the benefits of reducing threats are essentially the averted negative consequences. This holds both for pre-event mitigation efforts and post-event resilience.

Note this research does not address all maritime cyber related issues. It does not assess the value of compromised military operations due to cyber threats. It does not assess the full extent of property damage. And it does not address pre-event mitigation.[2] Consequences are measured in gross terms in the absence of resilience and in net terms in its presence. The metrics used are standard macroeconomic indicators of business interruption, such as gross domestic product (GDP), personal income, and employment.

II. The Role of Economic Consequence Analysis in the USCG Cyber Strategy

The design of this project takes direction from the *United States Coast Guard Cyber Strategy* (USCG, 2015), which presents the Coast Guard's vision for operating in the cyber domain.

To begin, Economic Consequence Analysis (ECA) is at the heart of the document's definition of a Cyber Incident — "An occurrence that actually or potentially results in adverse consequences to an information system or the information that the system processes, stores, or transmits and that may require response action to mitigate the consequences" (USCG, 2015 p. 41, based on DHS, 2014).

Our focus will be on Cyber-Dependent Critical Infrastructure -- "Critical Infrastructure where a cyber security incident can result in catastrophic regional or national effects on public health or safety, economic security, or national security" (USCG, 2015 p. 41, based on Executive Order 13636, 2013). The *Cyber Strategy* document notes that the Coast Guard is responsible for protecting the Maritime Transportation System (MTS), which consists of 360 sea and river ports that service $1.3 trillion in annual cargo. Other US government agencies have also stressed the importance of this system. For example a Government Accountability Office report (GAO, 2014) emphasized the critical role of port cybersecurity to the continued full operation of these ports.

A decision-support system that estimates the economic consequences of maritime cyber threats fits into several of the Coast Guard's strategic priorities. For example, in relation to the priority of Protecting Infrastructure, one of the objectives is to "identify existing cyber security risk assessment tools, and where appropriate, tap them for Coast Guard use and share them with the maritime industry" (USCG, 2015, p. 32). A related objective is to "Modify Maritime Security Risk Assessment Model (MSRM) to incorporate cyber risks, or identify a similar tool that performs the same function (USCG, 2015, p. 32). In terms of the cross-cutting goal of Ensuring Long-Turn Success, there is a stated need for communicating in real time (USCG, 2015, p. 36).

Although most of the *Cyber Strategy* document focuses on pre-event mitigation, significant portions do address post-event activities, which we discuss further below under the heading of *resilience*. Although this term is not defined in isolation, network resilience is defined as -- the ability of a network to: (1) provide continuous operation, (i.e., highly resistant to disruption and able to operate in a degraded mode if damaged; (2) recover effectively if failure does occur; and (3) scale to meet rapid or unpredictable demands (USCG, 2015, p. 43; based on DHS, 2014). The terms *response* and *recovery* are closely connected to resilience in both *Cyber Strategy* and in the E-CAT Tool. For example, Cyber Strategy defines recovery as -- "The activities after the incident to restore essential

[2] The reader interested in pre-event mitigation of cyber threats is referred to Farrow (2015) and Sinha et al. (2015).

services and operations in the short and medium term and fully restore all capabilities in the longer term (USCG, 2015, p. 43, based on DHS, 2014).

III. A General Framework for Maritime Cyber Consequence Analysis

And overarching framework of analysis combining maritime physical, cyber, and economic systems would contain the following key elements:

1. Categorization of Major Systems dependent on cyber networks

- Coast Guard
  - command centers
  - bases
  - intelligence units
  - individual vessels
  - surface support equipment
- Ports
  - operations centers
  - loading facilities
  - emergency response centers and equipment
- Ships (by origin, destination, and type)
- Cargo (by origin, destination, and type)
- Supply-Chain (upstream and downstream for each type of cargo)
- Regional Economy (by size and economic structure)

2. Cyber Landscape, covering the role of cyber in each of the major systems. For starters, this could be a logistical analysis.

3. Cargo Movement, covering docking needs, handling equipment, and cargo characteristics perishability, fertility, strategic importance. Again a logistical analysis would be in order.

4. Type of Threat (including various subcategories)

- Natural
- Human Intentional
- Human Accidental
- Technological Failure

These various components could then be organized into a *Threat-Consequence Matrix*, which displays the degree to which various types of cyber threats/incidents have potential impacts on the various systems. It would be useful to distinguish direct and indirect threat affects. Indicators of impacts would include degree of function and capacity. For starters, one could use qualitative designations ranging from low to high impacts (see also the discussion of an Economic Consequence Enumeration Table below.

IV. The CREATE Economic Consequence Analysis Framework

CREATE's expanded framework for estimating economic consequences of terrorist attacks and natural disasters is shown in Figure 1-1. It has been formulated to account for several standard and new considerations that affect bottom line impacts (Rose 2009a; Rose, 2015a).

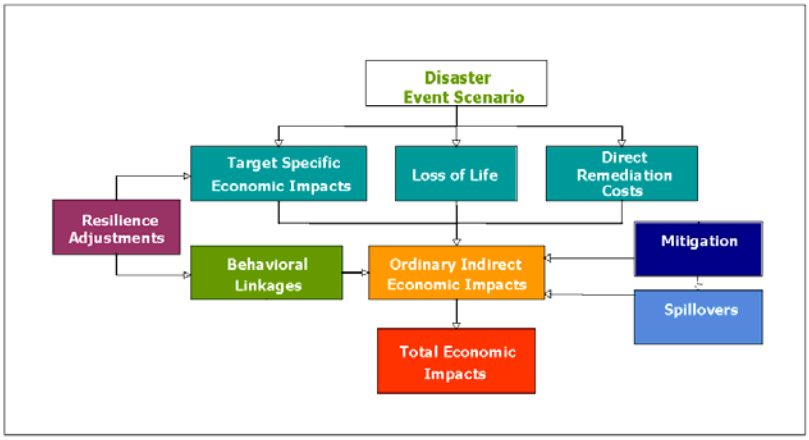


Figure 1. Economic Assessment Framework Overview

For many years, the estimation of losses from disasters focused almost entirely on standard target-specific (Direct) Economic Impacts and Loss of Life, and, to some extent, Ordinary Indirect Effects in terms of multiplier (quantity supply-chain), general equilibrium (multi-market quantity and price interactions) or macroeconomic (aggregate behavioral) effects.

The first major refinement to these standard economic consequences is the inclusion of *Resilience*, which refer to actions that mute business interruption and that hasten recovery. Rose (2004, 2009) has proposed as an operational metric of resilience: the avoided losses resulting from implementing a given resilient tactic as a proportion of the maximum potential losses for a given event in the absence of that tactic. Rose et al. (2009) measured the resilience of the New York Metropolitan Area economy to the 9/11 World Trade Center attacks at 72 percent as a result of business relocation as a resilient response. This stemmed from the fact that 95 percent of the businesses, comprising 98 percent of the employment, in the World Trade Center area did not shut down but rather relocated their operations, mainly within the New York Metro Area (the losses are simply due to the time lags in the relocation).[3]

In the past decade, the major extension of economic consequence analysis has been to include *Behavioral linkages*. A prime example is the "fear factor," which refers to changes in risk perception that translate into changes in economic behavior and may amplify damages instead of reducing them. Rose et al. (2009) measured the effect of the nearly 2-year downturn in air travel and related tourism in the U.S. following 9/11 at $85 billion, which accounted for over 80 percent of the estimated business interruption losses stemming from the event. A recent study by Giesecke et al. (2012) of a potential RDD ("dirty bomb") attack on the financial district of Los

[3] Others have used this metric as well to measure resilience (see, e.g., Kajitani and Tatano, 2009). For a broader view of cyber resilience, see Linkov et al. (2013).

Angeles would lead to social amplification of risk and stigma effects that could exceed the conventional "resource loss" effects by fourteen-fold.

The framework includes three other aspects necessary for a comprehensive analysis, the implications of which are often misinterpreted. The first is *Remediation*, which is typically not part of traditional economic impact analysis and has a conventional role in hazard loss estimation as simply repair and reconstruction. In the case of a terrorist attack, this can take on a much larger role, especially if the attack is caused by an insidious chemical, biological, radiologic or nuclear (CBRN) agent. For example, Baker (2008) found that the cost of remediation for a radionuclide attack on a reservoir of a small city of 100,000 was equal to the sum of the property and business interruption losses because of the extensive spread of the contamination and the high standards of remediation set by U.S. EPA.

Second, *Mitigation*, public and private actions prior to the event that reduce impacts, also enters the picture of a comprehensive economic consequence framework in its move toward a full-blown counterpart to benefit-cost analysis (BCA). The interesting consideration here is the interpretation by many that remediation and mitigation have benefits stemming from their direct expenditures alone (aside from the standard benefits of avoided losses). This perspective is often criticized because it appears to ignore the basic principle that resources are expended in the course of implementing remediation or mitigation, and that these resources typically must be diverted from productive use elsewhere. Of course, if the economy is not at full employment (the typical situation), or, at the regional level, where in-migration of new workers is likely, then indirect effects can be included, as admitted by most authorities on BCA (see, e.g., Boardman et al. 2001). BCA does not make an a priori judgment on this question and simply explores whether the employment adds, detracts, or is neutral with respect to the bottom-line, e.g., its impact on GDP. The answer has a great deal to do with whether the economy is initially at full employment, but is also influenced by whether higher-order effects of resource diversion are larger or smaller than those associated with mitigation or remediation.

Third, the mitigation effort can generate various types of "non-market" *Spillover* effects in the form of congestion, delays, inconveniences, changes in property values, changes in the business environment, and changes in the natural environment. These are difficult to measure, but have been found to be significant in both negative and positive directions, e.g., closed-circuit television surveillance is minimally intrusive, and its improvement in the business environment due to the public feeling safer from both terrorism and ordinary street crime can outweigh the intrusion on privacy (Rose et al. 2014).

The presence of *Resilience* and *Behavioral Responses* imparts significant variability to the economic consequences of terrorism in relation to attack mechanisms and targets. Simple rules of thumb cannot be used as in the relatively mundane areas of general economic impact analysis. Computable general equilibrium modeling is relatively superior to other model forms because of its ability to incorporate resilient actions (see, e.g., Rose and Liao 2005) and the behavioral consequences of changes in risk perceptions (see, e.g., Geisecke et al., 2012).

V. Illustration of Application of the ECA Framework to Port and Supply Chain Disruptions

We now provide an illustration of the application of the CREATE ECA Framework to the estimation of the economic consequences of 2 simulated port disruptions. The first pertains to a 90-day closure of Port Arthur/Port Beaumont complex due to a shipping accident (see Rose and Wei, 2011; 2013) and a 2-day closure of the Ports of Plus

Angeles and Long Beach due to a tsunami (Rose et al., 2016). Overall, the examples relate to a more comprehensive and enlightened view the value of America's ports.

The standard approach to estimating the economic impacts of a port is to determine the direct impacts of the port's operation (lost operating revenue) and then apply some form of multiplier. More recently, it has been popular to use both supply-side and demand-side impact multipliers, but just applied just to port operations alone. Accordingly, the calculations would proceed as follows:

- PA/PB: $220 million X 5.9 = $1.3 billion
- LA/LB: $1465 million X 5.9 = $8.6 billion

However, the standard approach misses the value of the cargo and contribution to the rest of the economy. Thus, the prior analysis would grossly understate the economic consequences of these port shutdowns. At the same time, many analyses that include supply-chain aspects fail to take into account resilience, or the ability to mute the negative consequences by using remaining resources more efficiently or recovering more quickly, which have the effects of offsetting some of these negative impacts.

A more comprehensive view of the economic consequence domain is presented in Figure 2, which displays the major linkages in tracing port disruptions from closure and damages beginning with direct economic impacts through short-run and longer-run impacts across five analytical stages of a disaster scenario (see also Rose et al., 2016).

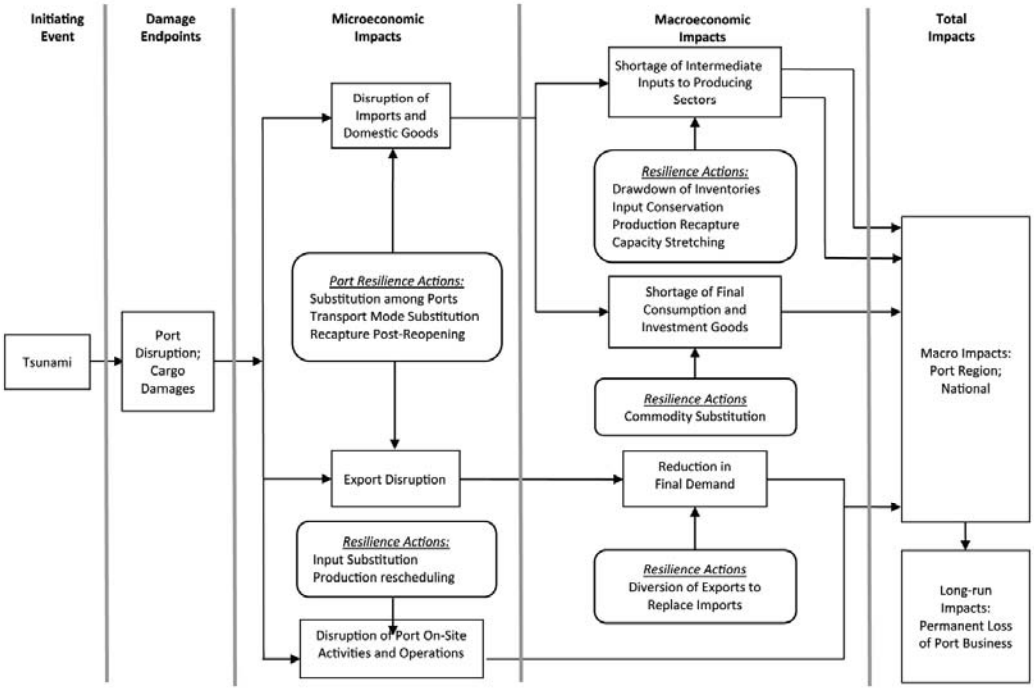


Figure 2. Estimating Total Economic Impacts of a Port Disruption, Cargo Damages & Terminal Downtime

The analysis begins with the tsunami event, which first translates into a risk of a port shutdown, cargo damage, and isolated terminal downtime for extended periods of time. At the port level, this leads to disruption of imports, exports, and port onsite activities and operations. Various resilience measures can be implemented to mute impacts at the outset, including rerouting the traffic to other ports, diversion of exports for use as import substitutes, use of inventories by port customers, relocating activities within the ports, and rescheduling of activities once the port reopens by working overtime or extra shifts.

At the level of the macroeconomy, impacts stem from increased scarcity of intermediate and final commodities, and reduction in final demand associated with a decline in exports. Both supply-side and demand-side impacts must be taken into account when evaluating total economic impact. Supply-side impacts affect customers of imported goods down the supply chain, while demand-side impacts affect these customers' suppliers up the supply chain. Intermediate goods imports are subject to both supply and demand impacts. Firms using imports as intermediate inputs to production, as well as successive rounds of downstream customers are subject to supply shortfalls. In addition, curtailment of production by import-using businesses also reduces the demand for intermediate commodities produced by successive rounds of upstream suppliers within the region, or nation. Curtailments of "final" (finished) imported goods supplies only impact end-users (consumers, government, and purchasers of capital equipment) without generating forward or backward linkage effects, and are simply added to the total macroeconomic impacts.

The shutdown of port operations limiting export shipments is characterized as an impact on suppliers, since downstream customers are outside the region and thus do not affect California's GDP. Conversely, disruption of export commodities reduces the demand for inputs to the production of these goods. First-round suppliers in turn reduce their demand, triggering a cascading decline in upstream production activities, analogous to that experienced by imports. The sum of all of these impacts is a multiple of the original initiating shock; hence, the term "multiplier" effect (both price and quantity) characterizes that manner in which these reactions yield macroeconomic impacts.

The estimation of the numerous macroeconomic linkages and resilience offsets can also be illustrated by the results of the simulated 90-day disruption at Port Arthur/Port Beaumont (see Rose and Wei, 2013). Again the standard estimate of economic impact on the US economy presented at the outset of this section was $1.3 billion. Taking all of the linkages into account raises this estimate to $14.8 billion in the absence of resilience. However, there are many resilience tactics that are applicable as shown below, isted in terms of their percentage ability to reduce gross macroeconomic consequences, such as GDP.. These range from very small gain from accessing the Strategic Petroleum Reserve or conservation efforts by the petrochemical industry dominating the surrounding economic region to rather high levels of resilience from imports ship rerouting in production rescheduling (making up lost production at a later date when input supplies are restored). Note that the total amount of resilience in terms of the reduction business interruption losses is 67% of the base estimates (the individual tactics are not fully additive, but contain some overlaps and offsets of their own). Thus, the bottom-line estimate of the economic consequences of the Port Arthur/Port Beaumont shutdown is $4.8 billion, or 3.7 times the initial estimate.

Strategic Petroleum Reserve	2.4%
Ordinary Inventories of All Goods	17.0
Conservation by Customers	3.0
Import Ship Rerouting	23.1
Export Diversion (to Replace Imports)	7.0
Production Rescheduling (Recapture)	25.4
Total Resilience (not additive)	67.0%

VI. E-CAT

A. Reduced Form Analysis

The state-of-the-art modeling approach for economic consequence analysis is computable general equilibrium (CGE) analysis. This approach models the economy in terms of the multi-market responses of individual producers and consumers in response to price changes, government policies, and external shocks, subject to constraints on labor, capital, natural resources. It essentially models the economy as a set of interconnected supply chains (see, e.g., Dixon and Rimmer, 2002). CGE models have been used extensively for the analysis of economic consequences of terrorism and natural disasters (see, e.g., Rose et al., 2007; Rose et al., 2009; Dixon et al., 2011; Geisecke et al., 2012; and Sue Wing et al. (2015). CGE models are especially complex, involving thousands of equations representing production, consumption and trade activities. These models are typically be on the utilization of those without extensive backgrounds in economics in general and CGE modeling itself.

A "reduced-form" capability refers to a simplified version of a more complex model that can readily be operated by users with a limited amount of knowledge of economics and with a rapid turnaround. Examples of these models have been developed by Dixon and Rimmer (2013) for computable general equilibrium (CGE) models and by Rose et al. (2011) for macroeconometric models.

Essentially, for a given scenario, the CGE model is run hundreds of times for variations in key variables. This provides the "synthetic" data for statistical regression equations that are the reduced form. The dependent variable is a major consequence type (e.g., GDP losses or employment losses), while the independent variables explain these losses to the extent possible.

Three factors should be considered in performing this analysis. First is the soundness of the theoretical underpinnings. This is guaranteed to a great extent by the fact that the synthetic data are generated by CGE models, which have been vetted on both a theoretical and empirical plane. CGE models reflect the behavioral responses of businesses and households within an economy to changes in prices, as well as taxes, regulation and other external shocks, within the constraints of labor, capital, and natural resource assets. CGE models are based on economic theory relating to producer and consumer choice and the workings of markets. They are able to estimate not only the direct responses but also indirect ones leading to total economic impacts, or consequences, referred to as "general equilibrium". In this modeling approach these impacts relate to price and quantity interactions in upstream and downstream markets. CGE models are constructed on the basis of a comprehensive set of economic accounts for production, household and institutional sectors, as well as some parameters, such as price and substitution elasticities, from the literature.

The soundness of the CGE model helps to ensure that results are likely to be reasonably accurate. However, we should note that accuracy depends on more than just sound theoretical underpinnings and internal consistency of the model, but also is affected by the key variables that are included or omitted. For each threat we consider 16 categories of direct impacts that might be relevant and quantify those that are likely to have significant effects on the results. This "Enumeration" approach is discussed in the following chapter. The third consideration is ease-of-use. While the complexity of the underlying CGE model is a plus, the opposite requirement is needed here. The reduced form regression equations include a limited number of variables that are transparent and for which numerical values can readily be obtained. The user thus need only plug these variables into the estimating equation, and a simple multiplication by parameter values yields the value of the dependent variable. The reduced form equations have been constituted in a user-friendly spreadsheet format to facilitate this application.

B. E-CAT Model Construction

E-CAT is constructed in 7 steps, as outlined in Figure 3. In Step 1, "Enumeration Tables" for as many as 16 categories of impacts for each threat are filled out according to upper and lower bounds identified from searches of relevant historical data of prior threat incidents, related literature, and/or expert judgment. In Step 2, lower and upper bound Direct Impact numerical values are estimated for each of the Enumeration Table categories that are determined to be above the "Low Influence" threshold.

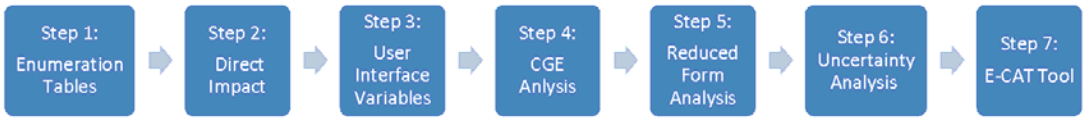


Figure 3. Seven-step E-CAT Research Framework

In Step 3, unique sets of User Interface Variables are identified for each threat and grouped under the following categories: Magnitude, Time of Day, Duration, Economic Structure, Location, Other, Behavioral Avoidance, Behavioral Aversion, Resilience Recapture, and Resilience Relocation. Randomized draws of 100 User Interface Variable combinations generate uniformly distributed values between range boundaries for the Magnitude variable and different options for the other variables relevant to each threat. These 100 random draws are then converted to CGE inputs via a series of linkages.

In Step 4, CGE model simulations are run for each of the 100 random draw scenarios. The identified relevant Direct Impact values are then input into the CREATE CGE model of the US economy (USCGE), which captures the combined and interactive effects of these impacts through price changes and substitution effects across multiple economic institutions – 58 sectors, 9 household groups, government institutions, and international traders. GDP and employment impacts for up to the first year of consequences are generated for each of these 100 scenarios, and where relevant the Economic Structure of the impacted region is also factored in by scaling the national average results across three different example regional economy structures to render 400 unique GDP and employment results.

In Step 5, multivariate regression analysis is conducted to estimate the influence of each of the User Interface Variables on the dependent variables of GDP and employment impacts, respectively. This analysis produces a reduced-form equation on the basis of Ordinary Least-Squares and Quantile regression analysis, allowing for estimates of mean, 5th percentile, 25th percentile, 50th percentile, 75th percentile, and 95th percentile results.

In Step 6, these reduced-form equations are combined to model the mean response and uncertainty surrounding the GDP and employment results for any given combination of User Input Variables. Uncertainty distributions are determined by user inputs of the parameters of a triangle distribution (i.e. a low-bound, a mid-point, and an upper-bound) for the Magnitude variable, alongside user inputs of the other variables for that particular threat. Validation criteria and methods applicable to CGE modeling are also implemented.

In Step 7, the coefficients from the reduced-form equations are input into the E-CAT Tool. The Tool is designed to be a user-friendly interface with which to explore the deterministic and probabilistic results of the reduced-form

analysis of the CGE modeling for each threat. Users first select a threat and the level of detail for the results they would like. The resulting E-CAT Tool User Interface provides an Input Area, whereby the user selects values for each of the relevant User Input Variables, and an Output Area, and where economic impact results for GDP and employment are presented in both tabular and graphical formats and with respect to both point estimates and distributions.

C. E-CAT Software

Following Rose et al. (2015), this section introduces the design of the E-CAT user interface tool. The tool is based on Excel and Visual Basic for Application (VBA). Three different economic consequence options are developed for each type of threat, including a point estimate (option 1), interval estimate (option 2) and uncertainty distribution (option 3). Step-by-step instructions are presented in the User's Guide in Rose et al. (2015).

The conceptual framework of the E-CAT user interface tool is illustrated in Figure 4. The analytical function of E-CAT is structured in four layers. The master user interface is designed in layer 1, which functions as the gate for various options. The different user options are designed in layer 2, which functions as the major platform for both data input and output visualization. User input information is translated from contextual format into numerical format and is then calculated based on the corresponding reduced-form coefficients stored in layer 4. User option 3 differs from option 1 and 2 in that an additional step for Latin-hypercube sampling (LHS) procedure is added in layer 3 to present the output uncertainty in various forms of probability distribution.

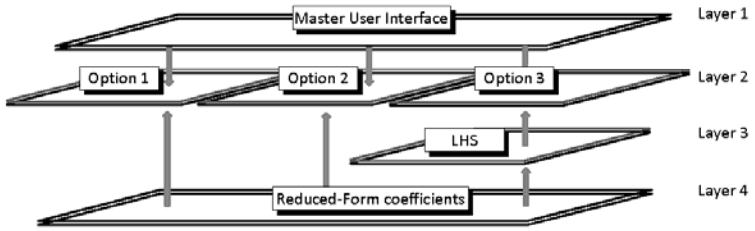


Figure 4. E-CAT User Interface Tool Structure Design

The designs of the various functional pages of E-CAT are introduced as follows. The master user interface page, as illustrated in Figure 5, is designed for the user to specify the types of threat and option of output estimation. The current version of E-CAT is able to conduct economic consequence analysis for the following categories of threats: human pandemic, nuclear attack, animal disease, earthquake, flood, tornado and aviation system disruption. Three output estimation options are provided for each threat. When a user specifies the type of threat as "human pandemic" and the output option type as "point estimate", a point estimate page as illustrated in Figure 6 is presented automatically. After the consequence analysis, the user can return to the main menu to select another threat or output option type by clicking the "Main Menu" button on the top right of each option page. The result can also be printed automatically when clicking the "Print Results" button. In addition, a "Reset Default" button is added in case the user wants to reset all the settings.

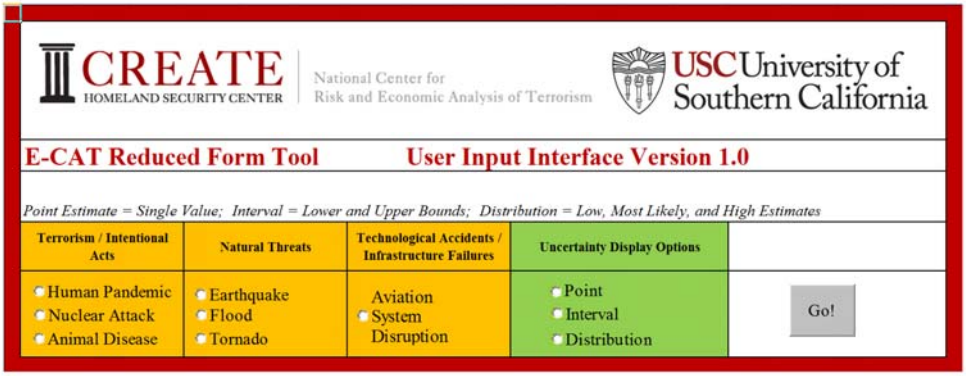


Figure 5. E-CAT User Interface for Threat Type and Option Selection

The point estimate (Figure 6) allows the user to calculate the economic consequence of a selected threat type in terms of GDP and employment losses based on a single magnitude input variable as well as other user input variables, such as "time of day", "duration", "resilience", "location", etc. the area for user input is highlighted in yellow color boxes, whereas grey boxes are not applicable for the specified threat type. For instance, in the case of Option 1 for the human pandemic scenario, user is provided with five selection options in terms of magnitude, duration, behavioral-avoidance, behavioral-aversion and resilience-recapture. The magnitude variable requires an input of numerical values within the given range as suggested, whereas other variables provide various options of categorical selection from a drop-down list. For instance, the "time of day" variable allows the user to choose either a daytime or a nighttime. The "duration" variable allows user to choose either a 6-month period or a 9-month period. The "resilience" variable provides user with three options: no resilience, lower-bound resilience and upper-bound resilience, whereas the two variables denoting behavioral effects only provide a "Yes or No" option for the users. Any change of an input variable would lead to an immediate update of results presented in the white color area. Outputs are presented in both numerical terms and cumulative distribution graphs. The numerical outputs of the mean estimates and estimates at various quantile levels are presented in both level change and percent change, respectively.

As shown in Figure 6, without considering behavioral effects and resilience, in a human pandemic case where 60 million people are infected during a 6-month period, the mean GDP loss is $66.08 billion dollars, which is around 0.405 percent decline of U.S. national GDP, and the mean employment loss is 1,071 thousand jobs, which is equivalent to a 0.834 percent reduction in jobs nationally. Behavioral effects in terms of avoidance and aversion, and resilience in terms of production recapture could have substantially alter the bottom-line. For instance, the mean estimate of GDP loss is amplified significantly to $79.88 billions of dollars if the behavioral-avoidance option is switched on in this case. However, if lower-bound resilience-recapture is selected, the mean estimate of GDP loss then reduces to $55.33 billion dollars. If an upper-bound resilience-recapture is selected, the mean estimate of GDP loss then reduces to $35.76 billion dollars.

Option 2 of the E-CAT user interface (not shown) provides interval estimate, which allows user to calculate economic consequence of a selected threat in terms of GDP and employment losses based on the given range of magnitude, together with other user input variables.

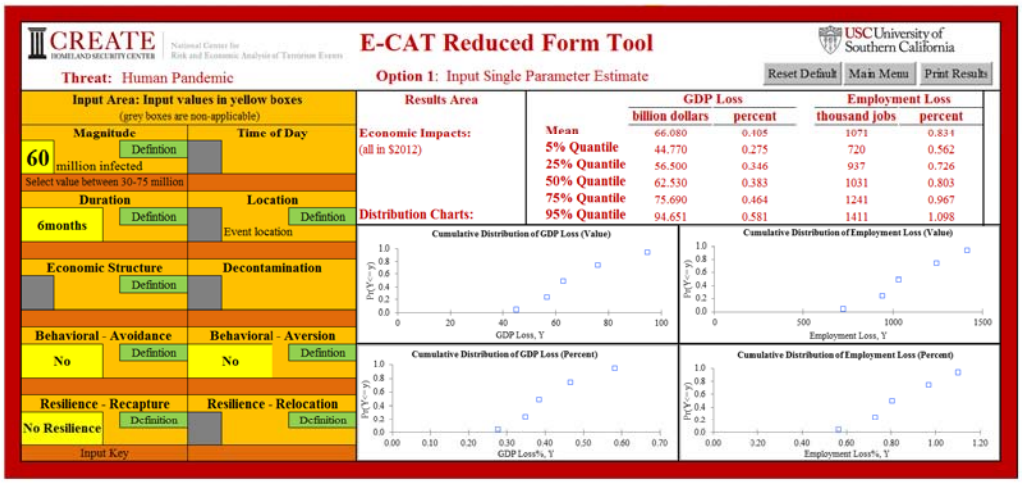


Figure 6. E-CAT User Interface Option 1 (Human Pandemic)

The uncertainty distribution estimate as illustrated in Figure 7 provides the user with an option to calculate GDP and employment losses based on a triangular distribution of the magnitude inputs, with interactions to other user input variables. In this option, the user is able to specify the magnitude values in terms of lower, middle and upper bounds. In addition, the user could also specify attributes, such as duration, behavioral-avoidance, behavioral-aversion and resilience-recapture. Numerical estimates of GDP and employment losses are displayed automatically in the output area. In addition, the cumulative frequency distribution charts and the relative frequency distribution charts of the mean estimates of GDP and employment losses are updated automatically.

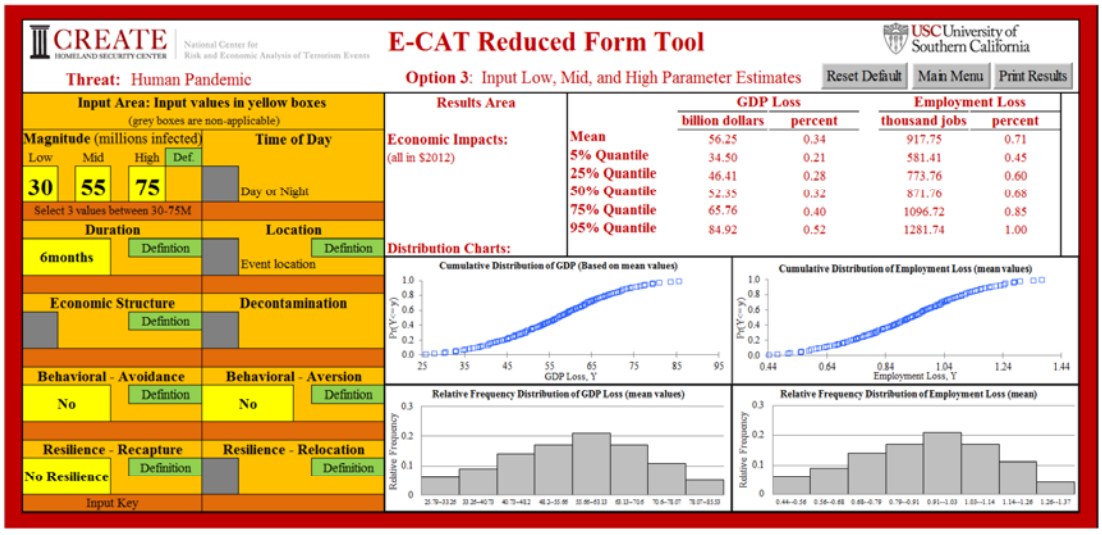


Figure 7. E-CAT User Interface Option 3 (Human Pandemic)

VII. Measurement of Cyber Resilience

This section summarizes the measurement of cyber resilience. This is done for several aspects of the cyber domain: 1) various types of cyber communications systems, 2) the electricity network, 3) manufacturing of communications equipment, and 4) provision of various cyber support services. The analysis is performed both on the supplier-side and customer-side. It includes not only the direct impacts but those rippling through the supply chain both upstream and downstream. The analysis is based on the Resilience framework developed by Rose (2009), and applied to several disaster scenarios in general and to electricity and supply-chain analyses in particular (see, Rose et al., 2007;; Rose and Wei, 2013; Rose et al., 2016).

To date, there is no comprehensive study of cyber resilience. There are several in-depth studies on protecting cyber systems from various types of attacks, including criminal, malicious, and terrorist threats. However, nearly all of these represent pre-event mitigation to reduce the chance of an attack or minimize the direct effect of an attack. Resilience, in our study, refers to actions taken in response to disruption from a disaster, i.e., post-disaster recovery (Rose, 2007; 2009). Of course, resilience is a process, and its capacity can be enhanced prior to disaster, but nearly all of these enhancements are not implemented until after the disaster strikes. Examples are the stockpiling of critical inputs or back-up generators, even though they will not be utilized until a disaster strikes. We also note that resilience differs with respect to suppliers of cyber equipment/services and their customers. In general, resilience on the supplier-side often involves expensive redundancies of equipment and systems, while many of the resilience options on the customer-side are relatively inexpensive, and in fact can pay for themselves (e.g., prioritization of access to limited bandwidth, substitution of satellite-based phones).

Table 1 summarizes studies on the microeconomic resilience options, or tactics, for businesses on the supplier and customer-sides. By microeconomic level, we are referring to the operation of the individual business, in contrast to meso-level resilience, which pertains to the operation of the entire industry or market, and macro-level resilience, which pertains to the entire regional or national economies. Following Rose (2004; 2007), the residence options can be either "inherent" or "adaptive." The former represents resilience capacities that already exist or are planned in the economic system and would simply be accessed to increase the functioning of business activities (to the extent possible) in response to disruptions. The latter refers to any expansion of resilience from improvisation or regulatory and administrative changes. The categories of resilience emanate from economic production theory, which is the conceptual basis for analyzing how business transforms various inputs into the goods or services it produces (Rose, 2015). The column headed "Possible Action" refers to specific resilience tactics that represent the build-up of resilience capacity prior to disaster or the response after the disaster strikes. The column "Cost of Resilience" provides a rough approximation of the cost of actually implementing resilience. The "Effect of Resilience" provides a general indication of the extent to which it can reduce business interruption losses. The cost and benefits of resilience tactics could only be quantified where some evidence could be found.

A major source of customer-side cyber resilience is the existence of multiple communications systems that support input substitution. Fiber-optic, or hard-wired, systems are the most vulnerable to earthquakes in terms of physical damage and repair, followed by cellular data systems dependent on cell towers. Satellite providers are the most reliable in the face of an earthquake threat, but are not as widely used and have vulnerabilities of their own with respect to technological accidents and solar weather. Of course, substitution potential must be tempered by possible delays in re-routing and limits to system capacity, which have frequently caused systems to crash in the aftermath of disasters (cf., Altman 2012; Vantage Point, 2013).

At the outset, we note that the literature and interviews by other researchers on the HayWired study (e.g., Wein, 2015) emphasize that critical facilities are far better prepared in terms of resilience than ordinary business

enterprises. For example, NASA has extensive redundant and back-up systems.[4] Of course, recent experience indicates that no system is fail-safe. Another overriding issue is that technological advances have simultaneously made us more vulnerable and more able to respond to cyber disruptions.

The first cyber resilience tactic presented in Table 1 is Conservation. Examples include reducing nonessential usage, restricting nonessential access, and recycling cyber equipment. For example, removing non-essential access increases the ability and speed of responding to a cyber breach or general disruption by reducing the number of access points (CyberSheath, 2014). Note that Conservation is an especially attractive resilience tactic, since it often pays for, or even more than pays for, itself. However, it is limited in scope in terms of being able to reduce business interruption from disasters in other or related contexts (see, e.g., Rose and Lim, 2002; Rose et al., 2007) and there is every indication that this applies to the cyber realm as well.

Input Substitution has extensive possibilities in the case of cyber. It ranges from increased flexibility of systems to various substitutes and back-up capabilities (see, e.g., Chongvilaivan, 2012; Sheffi, 2005). Flexibility refers to both supply procurement and to the conversion of inputs into final goods and services. The former entails investment into business-relationships between corporate management and suppliers, which leads to combined efforts towards quickly overcoming supply-chain disruptions.[5] "Multi-sourcing" is a classic example. Conversion flexibility relates to machinery and processes, which facilitates adjustment in resources and employees as necessary (Zoli and Healy, 2012). There are many examples of back-ups, including portable electricity generators. More dramatic examples include the use of "Cells on Wheels" following Hurricane Sandy, in which Verizon deployed several mobile cell-towers throughout New York City in response to a number of conventional cell towers going down (Richtel, 2009).

Import Substitution refers to bringing in goods and services in short supply from outside the region. It pertains primarily to the manufacturing of cyber equipment and various supply-chain effects. Setting up alternatives in advance, or at the minimum, researching options, can ensure smoother substitution of inputs following a disaster. Of course, it can be constrained by damage to transportation infrastructure, as often results from natural disasters

Inventories refer to stockpiling critical inputs for the production of cyber equipment, other supply-chain inputs, and cyber systems. Sheffi (2005) notes the classic example of Nokia being much better prepared for a disruption of semi-conductor supply inputs than its major competitor, Ericsson, and thus was able to significantly increase its market share in the aftermath of the disruption. Note that the cost of inventories is not the actual value of the goods themselves, but simply the carrying costs. The goods themselves are simply replacement for the cost that would have been incurred had the ordinary supplies been forthcoming. That said, it should be further noted that carrying costs of electronic goods are typically much higher than other goods, as they depreciate quite quickly (and carrying cost is more than interest and storage costs, but also the cost of the obsolete inventory itself). Some companies, such as Dell, circumvent these carrying costs with a "Made-to-Order" business model, in which they typically hold only four days' worth of inventory, ordering more as they receive orders. At first glance this would seem a less-resilient business model, more prone to supply chain disruption, but during the semi-conductor shortage in 1999 their "Made-to-Order" direct consumer marketing model allowed Dell to steer its customers

[4] We distinguish these two terms as follows: "Redundant" refers to an entire system, and is usually applied to the supplier-side. "Back-up" refers to select components, and is usually applied to the customer-side.

[5] Supply-chain modification is an example of a meso-level resilience tactic, as is the tactic of market-oriented non-interruptible service contracts to be discussed below. Import substitution is an example of a macro-level resilience tactic.

TABLE 1. MICROECONOMIC RESILIENCE OPTIONS FOR BUSINESSES`

Category	Action/Investment	Cost of Resilience	Effect of Resilience	Source
Conservation				
• reduce non-essential use	data consolidation	more than pays for itself	significant	
• remove non-essential access	remove non-essential administrator access	more than pays for itself (453hours * (IT-wage+Mngr-wage) * 3days + 260hours * (IT-wage+Mngr-wage) * 7days)	significant (increases ability and speed of responding to a breach by reducing access points)	CyberSheath (2014)
Input Substitution				
• paper records, traditional couriers	re-contract	low to moderate cost	significant at small scale	
• enhance flexibility of input combinations	supply procurement flexibility	low (investment in aligning corporate-supplier relationship)	significant (quickly overcome disruptions through greater cooperation between businesses)	Chongvilaivan (2012)
	process conversion flexibility	low (investment in standardized processes, identical machinery)	significant (ease of relocation)	Chongvilaivan (2012)
• wireless-to-wired, and wired-to wireless internet and phone access	use text messaging or social media	low to moderate cost	significant	
	Cells on Wheels (COWs)	moderate (price of device + long term storage; transportation)	moderate to large	Richtel (2009)
	satellite phones	low to moderate ($189-$300 monthly rental charges; $6-$9 per minute)	moderate to large (most reliable method of communication)	Verizon (2015)
	femtocells (small mobile cellular base station)	low (small scale: <$100)	moderate to large (restores cell coverage; improved battery life for devices)	Ricknas (2010)
	cellular signal boosters	low (small scale: ~$850; large business: ~$3,500; industrial scale: ~$4,000)	moderate to large (restores cell coverage; improved battery life for devices)	SureCall (2015)
	voice over IP telephone lines	low to moderate ($2,500 - $15,000 for initial installation + $40-65 per line/month)	moderate (requires an internet connection)	Chacos (2012) Kremlace (2012)
Import Substitution				
• mutual aid agreements	cooperative agreement	low	low to moderate	
• re-routing of goods/services	data-center failover	low (slowdown in internet services)	moderate	

Category	Action/Investment	Cost of Resilience	Effect of Resilience	Source
• supply-chain management	multi-sourcing strategy	loss of quantity discount; higher admin costs; reduces strength of established partnerships; competition leads to lower costs	moderate	Linthorst (2006)
Inventories (Stockpiles)				
• pool resources	cooperative agreements	very low	significant	
• stockpile products and other essentials	"safety" stock	low (carrying cost only; but higher than normal as cyber equipment depreciates quickly)	significant (safety net for disruption of supply; lower costs when purchased in bulk)	Sheffi (2005)
• stockpile product inputs	build-to-order (stockpile inputs & parts instead of finished products)	low (revise how business operates; some loss of economies of scale)	significant (allows business to more efficiently use stockpile to meet customer demand while input supply chains are reestablished)	Papadakis (2006) Chongvilaivan (2012) Sheffi (2005)
	direct consumer marketing (in conjunction with built-to-order model)	low (cost of training/updating marketers & customer service staff)	significant (allows promotion of products that were unaffected by supply chain disruption)	Sheffi (2005)
• batteries	install battery storage	low ($250/kwh capacity; base 100kwh, expandable up to 10mwh)	moderate (allows for 100kwh - 10mwh worth of electricity to be stored)	Kassner (2015)
Excess Capacity				
• maintain in good order	maintain in good order	low	significant	
• system redundancy	Redundant Array of Independent Disks (RAID); on- or off-site	low ($200 - $15,000+ for RAID setup; for off-site add cost of storage)	significant	Khasymski (2015)
	e-mail and work mirroring software; off-site	low ($150 + $0.50 per user/month to $1,000 per server + $0.50 per user/month	moderate (requires a working internet connection)	Gros (2003)
	cloud-based backup servers; off-site	low (cloud server: $0.024 - $0.061 per GB/month & $0.0036 per 100,000 transactions)	moderate (allows for easy connection to data if relocation is necessary)	Microsoft (2015) Dell Servers (2015)
	tape backups; off-site	low ($1,500 - $25,000 per month)	moderate (much cheaper than RAID storage)	Gros (2003)
	distributed data centers with data center "failover" capabilities	low	moderate	Wein (2015)
• maintain capacity	multiple internet service provider (ISP) contracts	low (cost of additional ISP contracts + $275-$4000 for routing equipment)	moderate (maintains internet connections in the case of an ISP losing connectivity)	Barracuda (2015) Amazon (2015)

Category	Action/Investment	Cost of Resilience	Effect of Resilience	Source
• maintain service	uninterruptible internet service premiums	low (usually 5% or less)	low to moderate (ISP will prioritize returning service to the business over other customers)	
Input Isolation				
• decrease dependence	permanent and temporary			
• segment production	identify less essential cyber needs			
Relocation				
• physical move	arrange for facilities in advance	low to moderate	large	Rose et al. (2009)
• telecommuting		low	moderate	
Production Recapture				
• overtime/extra shifts		low (overtime pay)	high (production and sales are not lost)	Park et al. (2011)
• restarting procedures	uninterruptible power supply (UPS) with generators	low ($4,000 - $15,000; plus cost of fuel and generators for as long as power is down)	moderate	Datacenter UPS (2015) Bruschi et. al. (2011) Liebert Corporation (2004)
Technological Change	increase flexibility			
• change processes				
• alter product characteristics				
Management Effectiveness				
• succession/continuity	train; increase versatility	low	low to moderate	
• increased awareness/information sharing	cybersecurity framework	low (<175 full time employee hours to implement, otherwise resources are free)	low to moderate	Casey et al. (2015) NIST (2014)
	Homeland Security Information Network	low (average cost of $43.80 per month per user)	low (provides a platform to share sensitive information, collaboration tools, virtual meeting space, documents & alerts)	IT Dashboard (2015) DHS (2015)
• emergency procedures	ensure emergency lines of communication with local government	low (minimal training; lines of communication)	low	Samuelson (2013) Chen (2013)

towards products that it had on hand and products that were less affected by the shortage. Alternatively, this could be termed a marketing strategy to promote resilience.

Excess Capacity overlaps to a great extent with system redundancy, which is primarily a supply-side resilience tactic. Typically, it is viewed as a rather expensive option, as, for example, in the case of back-up transformers for electric power systems. However, cloud-based backups are a relatively inexpensive option. Another possibility related to this resilience tactic is the development of uninterruptible internet service contracts, which could give firms the option to pay a small fee for being priority customers in the event of shortages in internet access. Furthermore, multiple overlapping contracts with different internet service providers (ISPs) could provide higher day-to-day speeds and larger bandwidth, while providing redundancy towards maintaining service should one or more ISPs experience service loss following a disaster (Barracuda, 2015; Amazon, 2015). Finally, we recognize the inherent redundancy in the internet – data network system here. E.g. Facebook data centers can failover, data can be rerouted.

Input Isolation is referred to in the technical earthquake literature by its complement -- "Importance" (see ATC, 1991). It pertains to the ability to separate aspects of the production process from dependence on lifeline utilities, including cyber systems. The Cybersecurity Framework, a federally developed set of guidelines for cyber standards and practices, provides resources to identify which aspects are essential and nonessential (NIST, 2014). Input Isolation obviously applies to many aspects of agriculture with respect to electricity and communications, but it is increasingly less of an option as our economy advances in terms of technological sophistication. While it is typically inherent in the system or production process, it can also be applied in the aftermath of the disaster through improvisation.

Relocation is a tactic that increases resilience by physically moving the business' operations to a location away from the affected area. This requires not only the arrangement for alternate facilities with sufficient capacity, but is also facilitated by the standardization of processes and operations to allow for movement. Relocation would also include tele-commuting if the nature of the business allows for it.

Production Recapture refers to the ability to make up lost production by working extra shifts or over time after communication services and other capabilities are restored. It might involve replacement of expensive equipment that has been damaged, but otherwise the cost is only that of overtime pay for workers (Park et al., 2010). It is further facilitated by hastening the restarting of services such as electricity and internet access. This in turn can be promoted by other resilience tactics, such as uninterruptible Power Supplies (UPS), a form of input substitution, which provide an emergency power source until back-up generators can be started or central power service is restored.

Technological change is a tactic that can increase resilience capacity by imparting additional flexibility into production systems both before and after the earthquake hits (Zolli and Healy, 2011). It can also refer to important improvisations in the way goods and services are produced in the aftermath of a disaster.

Management-effectiveness refers to any improvements in decision-making and expertise that improve functionality, primarily by using existing scarce resources more efficiently. Much of it refers to improvisation, but some relates to established emergency-management plans and information services. The Cybersecurity Framework is one such service that provides a platform for information to be shared between businesses on current threats and the tools available to counter and rebound from these threats. Typically, it is a relatively inexpensive option with costs limited solely to the implementation of the framework.

VIII. Systems Analysis of Economic Consequences of Maritime Cyber Threats

Figure 8 presents the many components of a system and their interconnections to estimate the economic consequences of maritime cyber threats. It begins with the specification of major characteristics of these threats and then includes the data set inputs and modules that use these inputs to perform a sequence of calculations leading to the estimation of Total Economic Consequences (TECs). Rectangles represent input data, diamonds represent the calculation modules, and ovals represent model outputs.

The initial input into the System is the specification of the Threat by type and key characteristics, the major categories of which are listed in the right-hand margin of the figure. Broader features of the Maritime Context, data from CART on ports and shipping and a history of cyber incidents, and information on the Cyber Role in this context are fed into an Incident Determination Module that calculates the major Incident Features, the major categories of which are listed in the right-hand margin again. The arrows connecting these 3 sets of input data are solid ones indicating that they are always included in the estimation. Another set of data that feeds into this Module, but on an optional basis, is information on Interdiction/Mitigation that can dampen the frequency and severity of each incident.

Incident Features along with 2 other sets of data are fed into the Direct Economic Consequences (DECs) Module. The first is an Enumeration Table, which lists the various categories of direct impacts that are applicable to a given Threat/Context combination. Because of the importance of Cyber-related considerations, information on the Cyber Role is again included. The Direct Economic Consequences Module then yields a set of estimates of DECs. Here, there are 2 optional enhancements of the analysis through the inclusion of Behavioral Response (e.g., fear arising from CBRN threats) and Microeconomic Resilience (e.g., ship-rerouting, use of inventories to cushion the economic shock of a disruption of critical input materials, production rescheduling). The first of these input data sets typically exacerbates the DECs, while the latter typically mutes them. These two aspects along with the Mitigation and Interdiction represent the major policy levers the Coast Guard has to reduce economic consequences.

The Direct Economic Consequences are then fed into the E-CAT Module along with data on Supply Chains and a Logistical Model to estimate Total Economic Consequences. Here again, there are options, including first Meso/Macro Resilience (e.g., price changes that spur resource reallocation or reliance on imported supplies from other regions through other transport modes). The system also can incorporate the effects of Repair and Reconstruction, relating to longer-term recovery of the economy. Both of these optional features reduce the level of TECs.

Note that the optional features of the System are intended to enable the user to analyze TECs in the absence of any external influences, such as private and public policy responses, behavioral reactions, resilience and recovery activities. This enables the user to examine the influence of each of these factors that significantly affect TEC one at a time to gauge their relative effectiveness. Including the costs of these various influences, so as to be able to gauge their relative cost-effectiveness, is a key to developing an overall Risk Management Strategy.

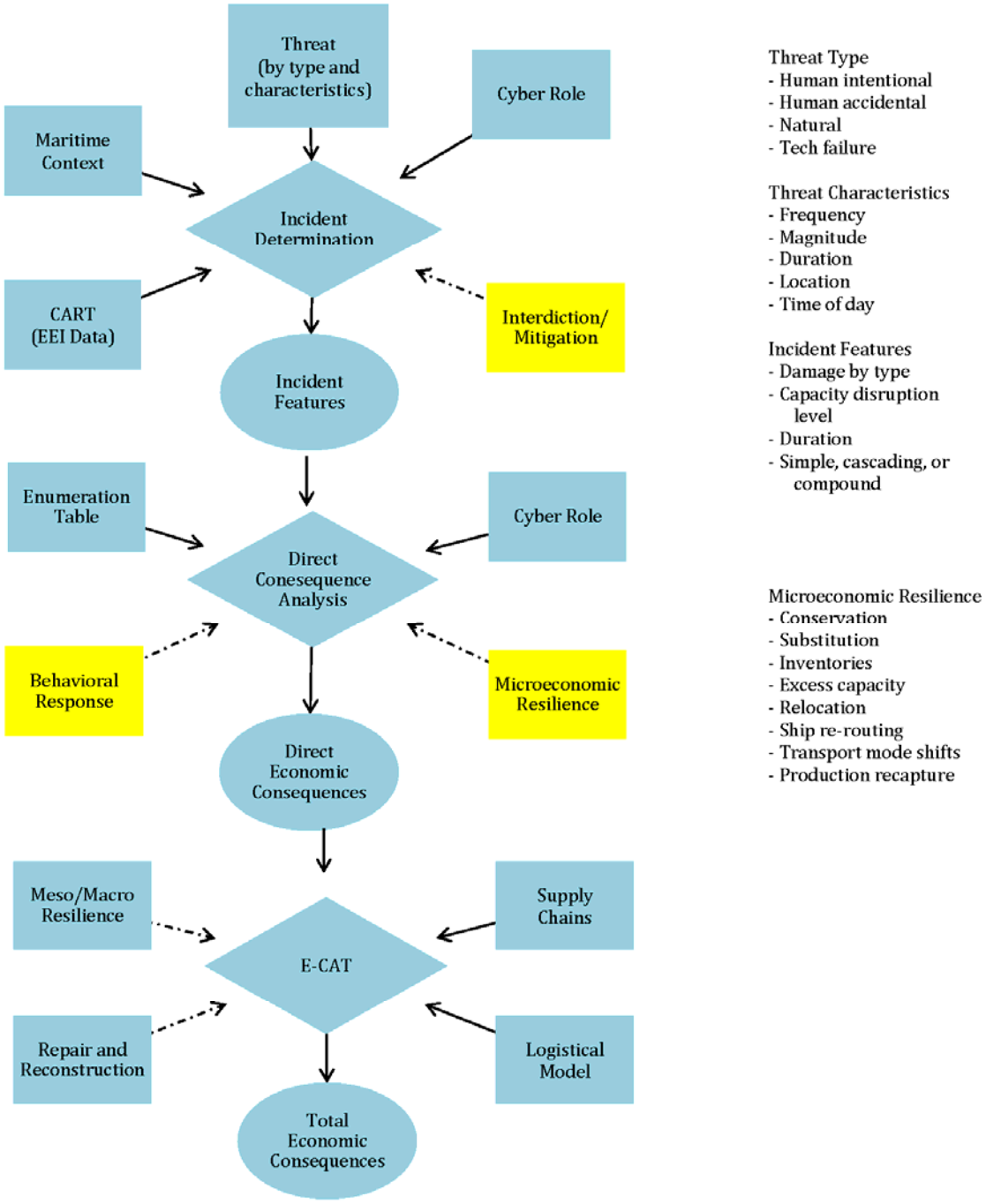


Figure 8. System for Estimating Economic Consequences of Maritime Cyber Threats

20

IX. Conclusion

This white paper has summarized the current state of the author's research on economic consequence analysis (ECA) of maritime cyber threats. It has identified the role of ECA in the overall U.S. Coast Guard's cyber strategy, and has outlined a framework for integrating the two. It has summarized the well-established CREATE ECA Framework and illustrated its application to prior studies of port disruptions. These studies have demonstrated the need for a comprehensive framework that includes proper attention, not only to standard features of traditional economic impact analysis, but also to aspects of resilience, behavioral linkages, and remediation of damages.

The white paper also presented a summary of the recently developed Economic Consequence Analysis Tool (E-CAT), which is intended to provide rapid estimates of economic losses from more than 30 types of threats, including those related to the cyber domain and transportation system disruptions. Finally, we presented a summary of research on numerous resilience tactics applicable to the recovery from cyber threats.

The goal of this on-going research is to incorporate into E-CAT the capability to rapidly estimate economic consequences of various maritime cyber threats. These will be chosen and their characteristics determine in collaboration with the USCG. The E-CAT methodology will be adapted to the special needs of this objective. The product to be transitioned to the USCG will essentially be a decision-support capability that will enable high-level decision-makers to better allocate resources across numerous threats.

Appendix. Members of the Maritime Cyber Economic Consequence Analysis Working Group

Name	Affiliation
Captain Bruce Clark	Cal Maritime Academy
Paul Kantor	CCICADA
Joseph Couch	USCG Atlantic Area
Evi Dube	LLNL
David Moskoff	USMMA
LTC Ernest Wong	Army Cyber Institute United States Military Academy
Randy Sandone	Critical Infrastructure Resilience Institute (CIRI)
Craig Moss	Oak Ridge National Lab
Adam Rose	CREATE, USC
Dan Wei	CREATE, USC
Zhenhua Chen	CREATE, USC

Selected Text References

Cohen, S. 2002. "Economic Impacts of A West Coast Dock Shutdown," *University of California at Berkeley*, Berkeley, CA.

Dixon, P.B., B. Lee, T. Muehlenbeck, M.T. Rimmer, A. Rose, and G. Verikios. 2010. "Effects on the U.S. of an H1N1 Epidemic: Analysis with a Quarterly CGE Model," *Journal of Homeland Security and Emergency Management* 7(1): Article 7.

Executive Order 13636. 2013. "Improving Critical Infrastructure Cyber Security," Office of the President, Washington, DC.

Farrow, S. 2015. "Integrating Cyber Losses into the Standard Microeconomics of the Consumer and Firm: Defining Losses in the Gordon and Loeb Model," Universityy of Maryland, Baltimore

Geisecke, J., W. Burns, A. Barrett, E. Bayrak, A. Rose, P. Slovic and M. Suher. 2012. "Assessment of the Regional Economic Impacts of Catastrophic Events: A CGE Analysis of Resource Loss and Behavioral Effects of a Radiological Dispersion Device Attack Scenario," *Risk Analysis* 32: 583-600.

Kajitani, Y., and H. Tatano. 2009. "Estimation of Lifeline Resilience Factors based on Empirical Surveys of Japanese Industries," *Earthquake Spectra* 25(4): 755-76.

Kajitani, Y., Chang, S., and Tatano, H. (2013). "Economic impacts of the 2011 Tohoku-Oki Earthquake and Tsunami." *Earthquake Spectra*, 29(SI): S457–S78.

Linkov, I., D. Eisenberg, K. Plourde, T. Seager, and J. Allen. 2013. "Resilience Metrics for Cyber Systems," *Environment Systems and Decisions* 33(4): 471-76.

Lauland, A. 2016. "Prepare for Cyber Katrina," *U.S. News and Wrold Report*, March 30. http://www.usnews.com/opinion/blogs/world-report/articles/2016-03-30/emergency-response-procedures-must-be-established-for-cyberattacks

Park, J.Y. 2008. "The Economic Impacts of Dirty Bomb Attacks on the Los Angeles and Long Beach Ports: Applying the Supply-Driven NIEMO (National Interstate Economic Model)," *Journal of Homeland Security and Emergency Management* 5(1), Article 21.

Rose, A. 2004. "Defining and Measuring Economic Resilience to Disasters," *Disaster Prevention and Management*, 13(4): 307-14.

Rose, A. 2009. *Economic Resilience to Disasters*, Community and Regional Resilience Institute Report No. 8, Oak Ridge National Laboratory, Oak Ridge, TN.

Rose, A. 2015a. "Macroeconomic Consequences of Terrorist Attacks: Estimation for the Analysis of Policies and Rules," in C. Mansfield and V.K. Smith (eds.), *Benefit Transfer for the Analysis of DHS Policies and Rules*, Cheltenham, UK: Edward Elgar.

Rose, A. 2015b. "A Methodology for Incorporating Cyber Resilience into Computable General Equilibrium Models," CREATE, USC.

Rose, A. and D. Wei. 2013. "Estimating the Economic Consequences of a Port Shutdown: The Special Role of Resilience," *Economic Systems Research* 25(2): 212-32.

Rose, A., G. Oladosu, and S. Liao. 2007. "Business Interruption Impacts of a Terrorist Attack on the Electric Power System of Los Angeles: Customer Resilience to a Total Blackout," *Risk Analysis* 27:13-31.

Rose, A., F. Prager, Z. Chen, and S. Chatterjee. 2015. *Economic Consequence Analysis Tool* (*E-CAT*), Final Report to DHS Policy Office, CREATE, USC, Los Angeles, CA.

Rose, A., G. Oladosu, B. Lee and G. Beeler Asay. 2009. "The Economic Impacts of the 2001 Terrorist Attacks on the World Trade Center: A Computable General Equilibrium Analysis," *Peace Economics, Peace Science, and Public Policy* 15: Article 6.

Rose, I. Sue Wing, D. Wei and A. Wein. 2016. "Economic Impacts of a California Tsunami," *Natural Hazards Review*, forthcoming.

Sheffi, Y. 2005. *The Resilient Enterprise*. Cambridge, MA: MIT Press.

Sinha, A. T. Nguyen, D. Kar, M.Brown, M. Tambe, and A. Jiang. 2015. "From Physical Security to Cybersecurity." *Journal of Cybersecurity* 1(1): 19-35.

Sue Wing, I., A. Rose, D. Wei, and A. Wein. 2016. "Impacts of the USGS ARkStorm Scenario on the California *Economy," Natural Hazards Review*, forthcoming.

U.S. Coast Guard. 2015. *United States Coast Guard Cyber Strategy*. Washington, DC.

U.S. Department of Homeland Security. 2015. *National Cybersecurity Assessments and Technical Services: Capability Brief.*

Werling, J. 2014. "The National Impact of a West Coast Port Stoppage," *National Association of Manufacturers*, Washington, DC.

Zolli, A. and A. M. Healy. 2012. *Resilience: Why Things Bounce Back*. New York: Free Press.

Cyber Resilience References

Altman. L. 2012.
http://www.continuityinsights.com/articles/2012/03/satellite-communications-myths-costs-capabilities

Amazon. 2015. Peplink Balance 20 Dual-Wan Router (pricing). Retrieved from: http://www.amazon.com/Peplink-Balance-20-Dual-WAN-Router/dp/B0042210U6/ref=sr_1_12?s=pc&ie=UTF8&qid=1373925222&sr=1-12&tag=viglink20237-20

Barracuda. 2015. Link Balancer, Advanced Internet Link Load Balancing. Retrieved from:
https://www.barracuda.com/products/linkbalancer/models#SUB

Bruschi, J., P. Rumsey, R. Anliker, L. Chu, and S. Gregson. 2011. "Best Practice Guide for Energy-Efficient Data Center Design," Department of Energy, Washington DC.
http://energy.gov/sites/prod/files/2013/10/f3/eedatacenterbestpractices.pdf

Casey, T., Fiftal, K., Landfield, K., Miller, J., Morgan, D., and Willis, B. 2015. "The Cybersecurity Framework in Action: An Intel Use Case," Intel Corporation, Santa Clara, CA.
http://www.intel.com/content/www/us/en/government/cybersecurity-framework-in-action-use-case-brief.html

Chacos, B. 2012. "VoIP buying guide for small business," *PC World Magazine*, April 14. Retrieved from: http://www.pcworld.com/article/260859/voip_buying_guide_for_small_business.html?page=2

Chen, B. 2013. "F.C.C. Seeks Ways to Keep Phones Alive in a Storm," *New York Times*, February 5. Retrieved from: http://bits.blogs.nytimes.com/2013/02/05/f-c-c-revisits-communications-failures-after-hurricane-sandy/

Chongvilaivan, A. 2012. "Thailand's 2011 flooding: Its impact on direct exports and global supply chains," *ARTNeT Working Paper Series*, No. 113. https://www.econstor.eu/dspace/bitstream/10419/64271/1/715937650.pdf

CyberSheath Services International. 2014. "The Role of Privileged Accounts in High Profile Breaches," May. http://lp.cyberark.com/rs/cyberarksoftware/images/wp-cybersheath-role-of-privileged-accounts-6-2-14-en.pdf

Dell. 2015. "Dell PowerEdge Servers," http://www.dell.com/us/business/p/servers?~ck=bt

Dell. 2015. "Datacenter UPS," http://accessories.us.dell.com/sna/category.aspx?c=us&l=en&s=bsd&cs=04&category_id=7071

Department of Homeland Security (DHS). 2013. National Initiative for Cybersecurity Careers and Studies (website). https://www.dhs.gov/news/2013/02/21/dhs-launches-national-initiative-cybersecurity-careers-and-studies#

Department of Homeland Security (DHS). 2015. "Homeland Security Information Network - Critical Infrastructure," May. https://www.dhs.gov/critical-infrastructure-0

FEMA. 2015. http://m.fema.gov/get-tech-ready-additional-tips

Goldman, D. 2012. http://money.cnn.com/2012/10/29/technology/mobile/cell-phone-sandy/

Green N., T. Bentley And D. Tappin 2014. A Multi-Level Analysis of Telework Adoption and Outcomes within Organisations Following a Natural Disaster. Ergonomics, Work & Health Ltd, New Zealand. Retrieved from: http://www.ergonomics.org.nz/LinkClick.aspx?fileticket=S_FdRN6qWpc%3D&tabid=39

Gros, M. 2003. "Taking Care of Business – Small, midsize and large companies have different disaster-recovery needs and budgets. The CRN Test Center details a wide range of solutions to help your customers weather the storm," *Computer Reseller News*. Retrieved from: http://go.galegroup.com/ps/i.do?id=GALE%7CA108267908&v=2.1&u=usocal_main&it=r&p=AONE&sw=w&asid=e4066cd2123764c27c43f5afc6f2ba82

IT Dashboard. 2015. "DHS - Homeland Security Information Network (HSIN)." https://itdashboard.gov/investment?buscid=134

Kassner, M. P. 2015. "Tesla's Powerpack proposes battery powered data centers." Datacenter Dynamics, London. Retrieved from: http://www.datacenterdynamics.com/critical-environment/teslas-powerpack-proposes-battery-power-for-data-centers/93974.fullarticle

Khasymski, A., and M. Rafique. 2015. "Realizing Accelerated Cost-Effective Distributed RAID," in A. Khasymski and M. Rafique (eds.), *Handbook on Data Centers*, New Paltz, NY: Springer, pp. 729 - 752. http://link.springer.com/chapter/10.1007/978-1-4939-2092-1_25

Kremlacek, R. 2012. "How Much Does a Business VoIP Installation Actually Cost?" *TeleDynamic*, May 22. Retrieved from: http://www.teledynamic.com/blog/bid/139621/How-Much-Does-a-Business-VOIP-Installation-Actually-Cost

Liebert Corporation. 2004. "Choosing the Right UPS for Small and Midsize Data Centers: A Cost and Reliability Comparison," Liebert Corporation, Columbus, OH. http://www.upsystems-inc.com/sites/default/files/resources/cost-and-reliability.pdf

Linthorst, M., and J. Telgen. 2006. "Public Purchasing Future: Buying from Multiple Suppliers," in K. Thai and G. Piga (eds.), *Advancing Public Procurement: Practices, Innovation and Knowledge-Sharing*, Boca Raton: PrAcademics Press, pp. 471-482. http://www.utwente.nl/bms/iebis/staff/linthorst/67_linthorst_telgen_edited_acc.pdf

Microsoft. 2015. "Backup Pricing." http://azure.microsoft.com/en-us/pricing/details/backup/

National Institute of Standards and Technology (NIST). 2014. "Framework for Improving Critical Infrastructure Cybersecurity." http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

Papadakis, I. 2006. "Financial Performance of Supply Chains after Disruptions: An Event Study," *Suuply Chain Management*, 11(1): pp. 25-33. http://libproxy.usc.edu/login?url=http://search.proquest.com.libproxy1.usc.edu/docview/216866096?accountid=14749

Richtel, M. 2009. "Inauguration Crowd Will Test Cellphone Networks," *New York Times*, January 18. Retrieved from: http://www.nytimes.com/2009/01/19/technology/19cell.html

Ricknas, M. 2010. "Femtocell Prices Have Dropped Below $100, Says Vendor," *PCWorld*, March 30. Retrieved from: http://www.pcworld.com/article/192855/article.html

Samuelson, T. 2013. "After Sandy, Questions Linger Over Cellphone Reliability," *NPR*, April 29. Retrieved from: http://www.npr.org/sections/alltechconsidered/2013/04/29/179243218/after-sandy-questions-linger-over-cellphone-reliability

SureCall. 2015. "Cellular Signal Boosters for Commercial." Retrieved from: http://www.surecall.com/product/cellphonebooster/15/0/0/CommercialBoosters

Vantage Point. 2013. http://apps.fcc.gov/ecfs/document/view?id=7520956711

Verizon. 2015. "Satellite Phone FAQs." http://www.vzwsatellite.com/faqs

APPENDIX D. CYBER PROJECT AT USC

Cyber Project at USC

Milind Tambe

University of Southern California

April 2016

PROJECT 1: Detecting and Acting Against Data Exfiltration attempts

Protecting against data exfiltration, the unauthorized transfer of sensitive or critical information, is of vital concern. Losses can range from competitive advantage or trade secrets to the leaking of confidential documents, and endangerment of national security. As it stands, detecting and protecting against such an attack is extremely difficult. Exfiltration attacks are often lost in the high volume of network traffic and can closely resemble normal network activity, and as such it is difficult to distinguish legitimate user activity from malicious attacks. Additionally, with these attacks it is possible to discretely transfer small amounts of data over long periods of time, meaning that any suspicious queries will not be immediately obvious. While there exists some detectors which can protect against these kinds of attacks, they are not water tight and often miss attacks. These detectors also have high false positive rates, misdassifying legitimate traffic as suspicious. All of these factors make data exfiltration a very difficult problem to solve.

Current state of research: To address this problem we wrap each of these imperfect exfiltration detectors (and possibly other detectors such as malware detector) in a decision making framework known as a Partially Observable Markov Decision Process (POMDP) in order to allow it to leverage additional network information and better reason about the true state of the network and whether exfiltration is occurring. POMDPs are rich modeling frameworks that allow us to not only take into account costs of different defender actions, but the probability of different events. By modeling the network this way we will be able to improve not only on the detection rates but also be able to determine best response actions to take in face of any suspicious activity. For example, if a machine is known to have sensitive data, it may make us more suspicious of data being exfiltrated from this machine. Actions can range from increasing surveillance by deploying more detectors or increasing the threshold on currently existing detectors to defensive actions like blocking a network protocol or port. However, these actions may also result in loss in the form of a performance hit or disruption of normal functioning of the network. POMDPs allow us to balance cost against potential benefit.

We are also taking advantage of structure in the problem in designing our model. Data exfiltration typically occurs in three stages; the intrusion stage, where an attacker attempts to breach the network,

the discovery stage, where an attacker may install malware or otherwise subvert the network system, and finally the exfiltration stage, where the attacker attempts to exfiltrate data. This typical attack flow allows us to use information from other detectors in the network in a strategic way. Not only do alerts from our intrusion detection systems and malware detectors allow us to heighten our suspicion about the exfiltration of data, but the specific timing of these events will allow us to more easily distinguish a signal of attack from the noise of the network. We have built an initial POMDP model, and with the help of researchers from HP Labs and researchers from Information Sciences Institute, USC, are about to start using a network and data exfiltration attack simulation on the DETERlab testbed to test this model. HP Labs researchers have promised further real world data.

DETER Simulation

DETER supplies a virtualized set of machines as well as a network connecting them. Specifically, we simulate a set of servers connected to outside nodes via an access point. The servers run different detectors, including both detectors specific to DNS exfiltration and more general IDS and/or malware detectors. Because DETER provides an isolated environment, we can test our POMDP with real malware supplied by HP Labs. To camouflage the traffic generated by this malware, we have created a group of agents who simulate the actions of normal users by periodically making DNS queries for sites that these users might try and visit. The test for the POMDP will be to use reports from the detectors to pick out signs of data exfiltration from the background traffic.

PROJECT 2: Detecting and Acting Against Cyber attacks: Adding up Cyber-physical Clues

In this project, the second part of our decision aid, we wish to detect attacks that are generated from outside an organization and that are trying to infiltrate a network; we wish to assist network administrators defend their networks. This project is motivated by the observation that an attack in progress often produces a series of suspicious events but not a single smoking gun. Examples include access to sensitive files, phishing emails, or improperly logged shipping containers. Importantly, such alerts could also be false positives produced by normal activity. The defender must decide whether they add up to a serious threat, and what an appropriate response is. For instance, the defender could take steps to acquire more information by launching more cyber or physical monitoring operations (but at some extra cost such as delays in network traffic), heighten physical security, or shut down parts of the network or port altogether. Each of these steps has an associated cost which must be balanced against the likelihood that an attack is underway. We are producing this attack-detection part of our decision aid for the defender; this will infer the current threat level and recommend the optimal response based on a cost-benefit analysis. For example, shutting down an entire network may not be the right response on the first instance of a suspicious packet.

Current state of research: Here we will also use a POMDP model as it will allow us to balance costs and benefits under uncertainty to help build a decision aid and assist network administrators. Furthermore, in order to evaluate this research, we are constructing a simulation of a cyber-physical system inhabited by agents who engage in both normal and malicious behaviors. The simulation is built in the DETER testbed operated by the USC Information Sciences Institute. Using the DETER testbed, this simulation will emulate an actual computer network, against which agents launch common attacks (SQL injection,

DDoS, etc.). Our decision aid will then be trained to recognize potential attacks and deploy defenses against them. The DETER testbed also allows simulating agents that interact with the computer network. This ability can be harnessed to simulate the physical part of the system (such of physical sensors) and also simulate physical attacks.

(This page intentionally left blank.)