Proceedings of the 2017 Maritime Risk Symposium: The Global Maritime Cybersecurity Challenge Tiffin University

November 13-14, 2017

Edited by:
Scott Blough, Executive Director
Center for Cyber Defense & Forensics at Tiffin University &
Alexandra Quinn, Graduate Assistant
Center for Cyber Defense & Forensics at Tiffin University

Suggested citation content:
Proceedings of the 2017 Maritime Risk Symposium: The Global Maritime Cybersecurity Challenge, 13-14 November 2017, Eds. Scott Blough and Alexandra Quinn. Tiffin, Ohio: Tiffin University, 2019.

Table of Contents:

8th Annual Maritime Risk Symposium
Introduction
Scott Blough

The maritime industry, like every other segment of the US economy, is dependent upon technology for every aspect of its operation. However, the maritime environments present some unique challenges to keeping data safe and reliable. Cyber threats continue to be present in today's political and technological landscape, increasing the need for improved security measures. With a focus on the articulation of current and future maritime cyber challenges and threats, MRS 2017: Cyber Security in the Maritime Transportation System brought together local and federal experts alongside academics and industry professionals to outline the implementation and operationalization of a sound maritime cyber strategy. The symposium assessed threats, vulnerabilities and recent advancements in both attack vectors and maritime cyber security research to inspire ideas for innovative research to define the next generation of maritime cyber security.

The symposium was held at Tiffin University on November 13-14, 2017 and attracted 225 attendees. The attendees included 31 students from eight universities and 14 attendees from five countries (United Kingdom, Mexico, Canada, Romania, and Singapore). The attendees represented 29 different educational institutions, all branches of the United States Military, various Federal Law Enforcement and Homeland Security agencies, and multiple private sector organizations. The 2017 Maritime Risk Symposium is the 8th annual Maritime Risk Symposium.

The major research questions developed during the MRS 2017 were:

1. How should the maritime transportation system handle the widespread proliferation of legacy systems and the vulnerabilities they present?
2. What metrics can be used for resilience in the maritime cyber systems and can resilience be quantified?
3. What metrics can be used for trust in cyber-physical systems and can trust be quantified?
4. How can the maritime transportation system protect against combined physical and cyber attacks?
5. What are the key challenges in training/retraining different players in the maritime transportation system in good cyber behavior and how can people be trained to change their behavior?

Summary of Keynote Address by
Rear Admiral Joanna M. Nunan, U. S. Coast Guard

On November 14, 2017, I had the great honor and pleasure to be a keynote speaker at the 2017 Maritime Risk Symposium, at Tiffin University. Surrounded as I was by college students who have grown up wired to the net, as well as experts of national and international stature, I was by far the least cyber-savvy person in the room. I could, however, provide context to the discussions in two significant ways:

- Describing the real world challenges the Coast Guard faces every day - which cyber attacks would only worsen
- Telling the experts what the Coast Guard needs from them - workable cyber solutions that become effective standards and enforceable regulations

My approach was to describe maritime risk in four broad categories: infrastructure, environment, security, and cybersecurity. First, however, I had to establish my central premise that taking on challenges is a process of defining specific problems coming up with answers, and turning the best possible solution into regulations that are clear to officials and mariners alike. The example that I used was the surprisingly high number of fatalities every year among recreational boaters, specifically people paddling around in canoes or kayaks. The Coast Guard long ago arrived at a solution and through the years has gone to great lengths to convince the public to wear life jackets, but in many cases the message does not make it through. That's how it goes in the business of risk: sometimes the best laid plans are not in place when they are needed most.

The sheer scale of the Great Lakes and the economic activity they support was a key part of my discussion on infrastructure. This is a massive portion of the American continent, holding one- fifth of the entire world's fresh surface water, and on which more than 160 million metric tons of cargo are moved every year. Forty provincial and interstate highways are linked to 15 major ports and 50 smaller regional ports. Thirty-five billion dollars in business revenues and $14 billion in wages and salaries are generated within this system. Keeping maritime traffic moving safely is the job of the Coast Guard, and this is not without its challenges. I spoke of the narrow, twisting St. Mary's River, which runs between Lakes Superior and Huron and is barely large enough to accommodate the enormous 1,000-foot freighters that pass in each direction.

There is no room for error, but seemingly plenty of opportunity. In August 2017, when a freighter ran aground, traffic up and down the river was forced to stop. The crisis that concerned Washington in this case was the huge amount of material that had stopped moving through the economy. The immediate crisis, the grounding itself, luckily was solved in short order. However,

it very clearly pointed out the precarious state of affairs in this restricted yet vital waterway. Compounding this is a man-made problem: of the four locks at Sault Ste. Marie, only one of them is large enough to handle the 1,000 foot ships carrying iron ore. This is the Poe lock, the Achilles Heel of the North American economy. Should anything go wrong with its ancient infrastructure, the consequences would cascade into a severe recession in both the United States and Canada. The solution's easy. We just have to dig another lock - but we have to convince leaders in both countries that this is a priority.

My discussion of meeting risks to the environment was intended to provide a bit of a happier ending, an example of teamwork in which the U.S. and Canadian coast guards, along with other agencies, worked together to define the scope of a problem, consider possible solutions, and then enact policies that have major impact. I wanted to establish a precedent, a working model by which many of these same leaders should approach cyber security.

I focused mainly on ballast water, which is carried in tanks inside a ship to control stability. The problem comes when a ship arrives in the Great Lakes from another part of the world. If they decide to pump out ballast water they've been holding for a long time, they've just dumped a bunch of plants and animals, especially on a microscopic level, that have never been in the Great Lakes before. Scientists say that about 180 invasive species have been introduced to the region, all of which play havoc with the food web and ecosystem.

In 2006, the Great Lakes Ballast Water Working Group was formed by the U. S. Coast Guard and agencies from Canada. Over the years, they have created solutions and established standards. The private sector, reacting to this and how the International Maritime Organization is facing this problem all over the world, has been developing workable, reliable, and affordable systems that can filter and decontaminate ballast water. U.S. law now says that any newly built ships have to come with ballast water management systems. U.S. law also says that existing ships have to have them installed.

Security along our 1500-mile maritime border is at once a vast challenge and the setting for a particularly clever form of teamwork. By no means have we tackled every form of danger that confronts us, but the U.S. and Canada have created a superb template for combining their efforts. I first described the very serious threats to security we face. Ahmed Ressam was an Al Qaeda member trained in Afghanistan who crossed from Canada into the U.S. in an attempt to bomb the Los Angeles airport on New Year's Eve 1999. We have information that members of ISIS, Al Qaeda, Hezbollah, and Hamas are present in the region, as are people willing to support their efforts. Smuggling continues, as does human trafficking.

The U. S. Coast Guard and the Royal Canadian Mounted Police have launched a program called Shiprider, in which SWAT-like boarding teams from each service work together to conduct law enforcement operations. This is a very carefully orchestrated legal arrangement

which includes comprehensive training for everyone involved. The procedures that the boarding teams use have been carefully reviewed to be legally airtight in either a Canadian or American courtroom. Criminals can no longer run for the border. There is no border. When I finally made it to cyber security, I told the experts - and the experts in training - that what we would need from them is the same kind of success stories we've seen in law enforcement and environmental technology. They would have to define the challenge - and I was well aware it's always changing - and they'd have to meet it. Then they'd have to pass along solutions that work for everyone. Ultimately, my two main points were:

- Cyber security has to become a lot less mysterious. We as normal people have to understand what the bad guys are up to and what the good guys are doing to stop them.
- Cyber security is going to have to follow the same narrative that the issue of ballast water did. This is the process: problem, solutions, standards, regulation, enforcement.

This is actually happening, I've been informed. The Coast Guard has gotten to the point where a working group has proposed standards which could eventually become regulations. Just as with the ballast water, where we are requiring ships to have systems on board, we're going to require that ships have cyber security software installed. That means that when Coast Guard inspectors go on board to examine an engine room or firefighting equipment, they'll also have a laptop to plug into the ship's system to make sure a protection program is up and running.

That last part may be a ways away - and that's where they come in, I told the young people in attendance. The battle's far from over. I hope they were inspired enough by the experts on hand to join the fight.

Biographical Statement:
Rear Admiral Joanna M. Nunan, U. S. Coast Guard

As the Ninth Coast Guard District Commander, Rear Admiral Joanna Nunan overseas U.S. Coast Guard operations in the Great Lakes and Saint Lawrence Seaway, an area that encompasses eight states, 1,500 mile international border, and workforce of 6,000 active duty, reserve, civilian and auxiliary men and women.

Panel on Cyber Threats to the Maritime Domain
Andrew E. Tucci

Abstract

The speakers provided a summary of cyber threats and vulnerabilities in the maritime industry. Threats were categorized by tiers, from low level "nuisance" tiers exploiting pre-existing, known vulnerabilities to nation states and advanced persistent threats. Attack classes were similarly categorized, and associated with broad protection and/or resilience strategies. The presentation identified cyber-dependent systems employed in the marine industry and supporting critical infrastructure, asserting that each has some degree of vulnerability. The presentation illustrated these vulnerabilities by describing two recent cyber attacks, one related to port terminals, and another to GPS systems. Finally, the presentation provided an overview of emerging cyber risk management frameworks and best practices.

Cyber Threat Capabilities

A wide range of threat actors can and do impact an equally large range of vulnerabilities in the maritime industry. While threat actors are ubiquitous, they vary in their degree of sophistication, techniques, and motivations. The following descriptions can be helpful in understanding the varying threat levels:

- Tiers I and II attackers primarily exploit known vulnerabilities.
- Tiers III and IV attackers are better funded and have a level of expertise and sophistication sufficient to discover and exploit new vulnerabilities.
- Tiers V and VI attackers can invest large amounts of time and money to create vulnerabilities, even in well protected systems.

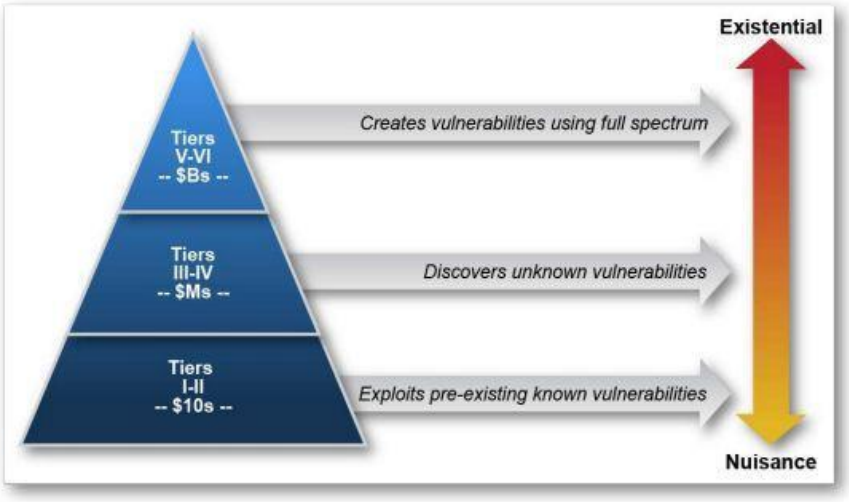


Figure ES.1 Cyber Threat Taxonomy

Another way to categorize cyber security events is by the nature of the attack, and what can be done to prevent or prepare for them. From an attacker's perspective, Tier I and Tier II attacks are "low hanging fruit," easy to exploit. Widely available anti-virus systems, used in combination with sound cyber hygiene practices, regular system updates, and employee training can make these far less likely. Like most cyber attacks, these low hanging fruit events are financially motivated, and come in the form of ransomware, theft of intellectual property, or Point of Sale targeted exploits. Large and small organizations are subject to these attacks if they don't take precautions.

Unfortunately, even larger, well-resourced organizations don't always take effective measures. In some cases they become the victims of "big and nosy" breaches, such as last year's attack on Equifax. In such cases the harm is passed on to the target organization's many customers or users, which sometimes number in the millions. Insurance and a good public relations program may be needed, especially if the organization is cutting corners in the technical, policy, and training measures appropriate to the level of risk.

Advanced Persistent Threats (APT) represent a different level of attack class. These organizations, which may or may not be state sponsored, will take a "slow and stealthy" approach to find (or create) a vulnerability, establish a presence on a targeted system, and exfiltrate data or take other action over time, preferably without the victim ever being aware. Attackers with this level of sophistication will not be stopped by routine protective measures, but may be revealed by anomaly detection or other compromise indicators. Having a good understanding of your baseline cyber activity, especially in critical systems, is key to detecting this type of attack.

Nation state actors represent the most sophisticated of APTs. While few, if any organizations have the resources and technical ability to offer credible countermeasures to such threats, they should certainly take what measures they can in order to avoid falling victim to lesser threats. Also, it is important to understand that APTs are often reluctant to use their most sophisticated capabilities, simply because doing so costs them resources, creates the potential for attribution, and risks exposing those capabilities in ways that might allow rival organizations to eventually develop countermeasures. Finally, even when organizations are incapable of mounting an effective defense, they can and should conduct response and recovery planning for that inevitable day when they discover they have been hacked.

Maritime Cyber Systems at Risk

The maritime industry was slow to recognize cyber as a legitimate risk. In many cases companies assumed that the relatively low state of technology in the maritime industry kept them immune, or that their cyber enabled systems were air gapped, generally unknown to hackers, protected by human in the loop policies, or otherwise at low risk.

In fact, like the rest of society, the marine industry is heavily dependent on cyber technology. In some ways, the maritime industry is particularly vulnerable:

- It is mobile, necessitating wireless connections
- It is global, bringing in international players and transactions

- It is high volume, meaning that even where profit margins are small, financial transactions are large
- It is heavily dependent on contractors and other third parties, all of whom need some level of cyber access to given segments of an organization. Configuration management and access control policies may suffer as equipment is swapped out, contractors swarm over ships and terminals, and new, cyber dependent operational systems are added or upgraded under the radar of IT staffs primarily focused on financial systems.
- It uses both Operational Technology (OT) for industrial control activity, and information technology (IT) for business and operational support activities. In some cases, such as terminal operating systems, OT and IT systems are integrated.

Common cyber technologies in the industry include:

- Navigation, including GPS, electronic charts, AIS, autopilot
- Voyage Data Records (which integrate many electronic systems)
- Propulsion and engine management systems
- Cargo control and tracking
- Hazardous conditions/gas detection, fire detection
- Ballast water and stability systems
- Lighting, access control, gate control
- Terminal Operating Systems
- Business and financial systems
- Emergency communications and alarms
- Crew communication and entertainment systems, passenger services

As the marine industry continues to adopt cyber technology to reduce costs and improve service, cyber risks will grow. The rapidly emerging Internet of Things further increases the attack surface area (and therefore vulnerabilities) of the marine industry.

Maersk Cyber Incident

In 2017, the NotPetya incident impacted global shipping giant Maersk. At first glance, NotPetya was a typical ransomware event, where the attacker gains control of the victim's system and demands a ransom (typically paid in bitcoin) to release the files. Ransomware attacks are generally done by low to moderate skilled hackers, and while they may or may not release the ransomed files, their motivation is clearly financial. In this case, the attack was quite sophisticated, and apparently intended merely for disruption rather than financial gain, as the "back end' payment system was quickly and easily shut down, almost no ransom paid, and the files never recovered.

Regardless of the motivation of the hackers, or the technical details of the attack, the impact was clear: Maersk and its port operator, APM Terminals were shut down for many days and perhaps $300 million in costs. Terminals around the world were impacted, with effects cascading across the supply chain.

Maersk was able to recover through a huge effort by its employees, customers, and partners, and via an equally huge expenditure of funds to reformat or replace much of its computer system. Smaller organizations without these resources might not have recovered at all. It is also worth noting that investigators do not believe that Maersk was actually targeted by this attack, which was likely focused on the Ukrainian power infrastructure. Clearly a targeted attack against vital components of the marine industry could have even greater consequences.

GPS spoofing in the Black Sea

The marine industry is heavily dependent on GPS for navigation, cargo tracking, and other operations. Given its low power and open architecture, GPS systems are inherently vulnerable to jamming and spoofing. Jamming is the introduction of RF "noise" that eliminates the ability of a GPS receiver to operate. Spoofing involves the deliberate introduction of false signals such that the GPS receiver will calculate the wrong position for the vessel. While prudent mariners can detect both of these issues by employing visual and other non-GPS methods to determine their position, both attack vectors can create substantial risk, particularly for navigation at night, in bad weather, in close quarters, or other circumstances where conditions are challenging.

In June 2017, a vessel transiting the northeast portion of the Black Sea reported multiple instances of GPS interference. Approximately 20 other vessels in the same area appeared to experience similar interference. The GPS display not only showed the wrong position, it indicated the position was "safe" within a 100 meter accuracy. To add to the confusion, AIS also showed numerous "ghost" vessels that did not appear on radar. The master wisely used radar, paper charts, and other methods to confirm his actual position.

The master reported the incident to the U.S. Coast Guard Navigation Center, which enabled the Coast Guard to evaluate and confirm the incident, and issue an advisory to others. Mariners can make similar reports at: https://www.navcen.uscg.gov/?pageName=gpsUserInput. While there were no groundings, collisions, or other damage resulting from this incident, it clearly shows the vulnerability of a technology fundamental to the maritime industry.

At about the same time, two tragedies involving U.S. Navy vessels raised questions in the industry's mind about the potential for GPS spoofing or disruptions to cause disasters at sea. Subsequent investigation into the collisions involving the USS FITZGERALD and the USS JOHN McCAIN found no evidence of GPS manipulation, and in fact confirmed a series of human errors. Nonetheless, in close quarters situations, even a momentary uncertainty about one's position can have disastrous results.

Managing the Cyber Threat

The cyber and maritime industries are taking action to address these cyber threats. Cyber systems in the maritime industry are no different from those in other industries (indeed, this is precisely why the industry is at risk), and good cyber practices apply to all. Following the outline of the NIST Framework, maritime organizations can begin by ensuring they have an accurate inventory of their systems, and are following sound network architecture practices. This is part of the "identify" stage of the NIST Framework, which also includes identifying users, software, hardware, and the persons responsible for overall cyber risk management and governance.

Various government and non-government organizations are establishing maritime specific cyber risk management standards, including the U.S. Coast Guard, the International Maritime Organization, and various industry groups. Information sharing is vital to any effective cyber risk management system, and Information Sharing and Analysis Centers and Organizations (ISACs/ISAOs) can help perform this function.

Despite the admittedly technical nature of cybersecurity, the most important element remains the human one. To address cyber threats, organizations need to grow a cyber-savvy workforce, train personnel to follow good cyber hygiene and detect problems, and foster a culture of cyber safety and security.

Biographical Statement:
Andrew Tucci

Andrew Tucci is a U.S. Coast Guard officer with 28 years of service. He has spent much of his career working with commercial vessels and ports. He helped author the Coast Guard's Cyber Strategy, and has had a leading role in developing maritime cyber risk management policies.

Panel: Afloat Cyber Vulnerabilities – Synthesising Views and Projecting Forwards

Kimberly Tam and Kevin Jones

Abstract

As one of the most important transportation systems in the modern world, securing the maritime infrastructure is essential for protecting people, goods, and the global economy. This demands both broad and deep understanding of the various components and environments involved and their cyber-risks and vulnerabilities, especially those unique to the maritime arena. The four panelists at the annual Maritime Risk Symposium (MRS) in 2017 each gave their thoughts and opinions on the subject of Afloat Cyber Vulnerabilities. Discussions on these issues primarily centered on the maritime-cyber concerns of ships, as their technology and functionality are significantly different from traditional computing systems. This article presents a synthesis of the presented views and combined efforts for securing the future.

Introduction and Background

This article is primarily based on the presentations of four panelists at MRS 2017 symposium on the topic of maritime cyber-security at sea, or "Afloat Cyber Vulnerabilities". In order of presentation the speakers were Prof. Kevin Jones, Dr. Tom Longstaff, Mr. Chris DeWitt, and Mr. Jason Kent with Captain David Moskoff as the panel chair. All panelists primarily had security-related backgrounds and have migrated toward maritime-cyber so their combined talks provided a robust and thorough look at ship vulnerabilities facing the world today.

Individual panelists were able to set the stage by discussing the evolution of cyber-security, separate from maritime initially, as traditional cyber-related issues (such as the financial industry and energy grids) have a longer history to draw from [1]. More specifically they examined traditional threats that can be transferred to the maritime environment with no, or minimal, adaptations. This included generic human vulnerabilities such as phishing emails and the use of personal devices. A review of literature for cybersecurity frameworks for critical infrastructure was also provided in order to show various examples of implemented cyber-security policies, best practices, and standard frameworks for both information and operational technology (IT/OT) systems. This establishes similar vulnerabilities between traditional systems and those afloat, which then leads to the more pressing issue of risks and vulnerabilities unique to the maritime sector and how to addresses them going forward.

Early in the discussion the first panelist illustrated that, not only were maritime vessels unique in the world of cyber-security, but the range of ship types, attacker types, system age, outcomes, and functionality meant that the scope of risks and vulnerabilities is also exceptionally wide (Figure 1). Other panelists voiced similar observations in that, because of the lifespan and age of the average ship (20 years is roughly the average age [2]), ships are unusual in that they connect a network of new, old, secure, and insecure systems. Furthermore, while many industries are international, components of the infrastructure do not normally physically move across borders as frequently as the global fleet. While similar to airplanes, voyage duration, amount of goods moved, and port-ship interactions separate maritime cyber-security from otherwise similar issues. Furthermore, as discussed, understanding today's maritime-cyber vulnerabilities requires a consideration of the functionality and operations of each maritime system and the unique resulting outcomes an attack on those systems can have.

Lessons Learned

Given the background story supplied by the panelists, it is clear the current maritime-cyber security landscape and the majority of related vulnerabilities are not well understood. However, the range of real-world vulnerabilities discussed during this panel (e.g. bridge-based information theft, GPS misdirection, cyber-physical cargo attacks, and denial of service on networks) demonstrate that the maritime-cyber threat is real and must be addressed.

It was discussed that, in order to move forward, it is important to be able to rank risks to properly focus resources in order to reduce the amount and severity of existing maritime-cyber risks and vulnerabilities. Essentially, it is important to fully understand the current threats in order to address and prevent them effectively. Another learning outcome of the panel is ensuring that the definition of maritime-cyber risks fully considers the unique functionalities and operations of ships. This includes systems such as rudders and cargo maintenance, and the networks that connect them [3]. The maritime cyber-security problem is also further complicated by the increase in sophisticated software throughout the ship, intended to improved automation and autonomy, as they it introduces more vulnerabilities.

The maritime-cyber vulnerability landscape established by the panelists also included a look at the current state of vulnerability mitigation, primarily implemented by policies, checklists and cyber hygiene. However, these attempts have been largely ineffectual in lowering the risks associated with maritime-cyber vulnerabilities. At this point, the issue of trust was introduced, which defines the basic premise of security. Which systems can be trusted? What security protocols, checklists, supply-chains, and policies can be trusted?

In turn, this expands the issue of maritime-cyber security beyond specific physical locations such as a ship, port, et cetera, as the ship is a part of a larger infrastructure and it is important to understand whether the chain of supply, chain of command management, and chain of trust are secure and robust, i.e. trustworthy. While system redundancy is one possible threat mitigation option, it is important to also understand and rank vulnerabilities and guide technological solutions such as machine learning and big data analytics. For example, the panel and the chair discussed the risks and vulnerabilities related to GPS jamming and how relied-upon it is. Such an attack would be low effort, and so the risk would be high, and as the global fleet is reliant on this one technology that enables global positioning. Therefore, it is important that trust is not misplaced and the proper management and system changes are made.

Future Directions and Research Questions

As the technology on-board ships, and connected to ships, become more advanced it becomes increasingly important to understand and mitigate cyber-vulnerabilities. This may require the use of well-used, traditional methods like machine learning and big data analysis, as one panelist has mentioned. However, due to the differences between the technology, functionality, and environments between maritime systems and others, it is important to create or adapt frameworks and policies that are capable of ranking and mitigating risks and vulnerabilities for today's ships, and those of tomorrow [4]. Furthermore, this must include securing any supply chains and management teams connected to the ships in order to establish robust security. In essence, this boils down to a few core research questions to be addressed:

- How to we rank risks and vulnerabilities to focus research efforts?
- How can we secure isolated systems? What tools can reduce the attack surface?
- How can we monitor and secure networked systems?
- How do autonomous ships differ and how can they be secured?
- How far does the supply chain extend, and how do we secure the weak links?
- How do we increase cyber-knowledge and awareness from crew through to higher management?

Conclusions

It is important as the maritime community continues to advance its technology to ensure they are trustworthy and robust against maritime cyber-attacks. The panelists discussing afloat cyber vulnerabilities at MRS 2017 discussed the evolution of technology up to the today, current ship vulnerabilities and risks, and how frameworks, technological solutions, and policy must continue to evolve as threats also advance in order to provide global safety since ships are an essential comportment to not just to the shipping industry, but the flow of world goods, global economy, and national wellbeing.

Panel on Legal and Insurance Issues in Maritime Cyber
Andrew E. Tucci

Abstract

The insurance industry views cyber as a risk management challenge, since perfect cyber security is impossible. The marine industry has significant cyber vulnerabilities, and has been impacted by many cyber events, causing significant and growing losses. Emerging industry and government standards is an encouraging sign and allows insurance carriers to assess the degree to which clients are exercising due diligence to protect themselves from cyber attacks. While insurance companies are providing cyber insurance products, they are challenged by the lack of actuarial data on cyber incidents and losses. Available data suggests growing risk exposure. Due to a perceived lack of reporting, the actual number of incidents is unknown. Regulatory requirements for marine operators to meet certain cyber standards, and to report cyber incidents may lead to greater transparency and risk management practices, reducing risk. Additional questions remain, including the impact of cyber on war risk, the potential for moral hazard as companies rely on insurance, and the actual effectiveness of cyber standards in reducing the frequency and impact of cyber incidents in the marine industry.

Cyber Security as Risk Management

Insurers, who are by definition the last step in risk management activities, encourage maritime operators to recognize that 100% cyber security is impossible. For this reason, operators need to view cyber as a risk management challenge, and one that includes a substantial role for resilience and recovery. Questions about how well an organization can operate if/when subject to a successful cyber attack are at least as relevant as what measures the organization is taking to protect from such attacks. A very realistic approach is to recognize that there are two types of companies: those that have been hacked, and those that know it. The reality is that if you or your company have an email address or a smart phone, you have been hacked.

It is also important for operators to recognize that cyber has moved well beyond financial data and privacy issues to include operational technology, the Internet of Things, and the potential for significant financial losses and operational impacts. Fiat Chrysler's 2015 recall of 1.4 million vehicles to fix a software flaw that left cars vulnerable to hacks that could impact breaking, steering, and acceleration is one example of an incident with high costs and the potential for a kinetic impact on human safety.

Cyber Vulnerabilities in the Marine Industry

The maritime industry, including vessel and port facility operations, have many critical cyber based systems, including navigation, propulsion, communications, cargo control, and business activity. Vulnerabilities and poor cyber security practices are common, with the industry heavily connected, mobile, international, dependent on contractors, and often employing out of date software, unpatched systems, and free use of USB drives to move data from ship to

shore. Unsurprisingly, the maritime industry has been the victim of many cyber attacks over time, coming from sources as diverse as nation states, organized crime, insiders, and lower level actors.

In some cases, maritime companies are specifically targeted. For example, pirates using cyber tools to identify high value ships, cargos, and routes. The bunkering community, heavily reliant on e-mail to arrange for services and make payments, has been hit many times, sometimes by relatively simple scams, such as a criminal impersonating a known customer to receive free fuel,[1] or by impersonating a bunkering company and asking a customer to make payment to a new (false) account.

In the maritime industry and others however, most cyber attacks result from automated systems that simply scan open systems, generate phishing e-mails, or otherwise probe across the internet for vulnerabilities. Phishing e-mails continue to be a common tactic, with up to 80% of individuals who receive and click on a fake e-mail then go on to actually provide useful information to the hackers, essentially ensuring a successful breach. While such events can lead to significant losses, they may or may not be covered by any given insurance policy. Cyber insurance is not a mature field, and there are many gaps in the types of losses a policy may cover. Operators need to understand the extent of their coverage, what exclusions and caps may apply, and exercise due diligence to protect their own systems.

Cyber Security Standards and Guidance

Understanding the extent of cyber risk exposure and what measures a vessel operator should take has been a challenge for insurers and the maritime industry. The scarcity of data (in the form of documented incidents with known losses) presents a challenge to insurance carriers, who traditionally rely on actuarial tables built on decades of data to predict losses and establish premiums. Furthermore, although organizations such as NIST, SANS, and the Center for Internet Security have well established cyber standards, until very recently the lack of maritime specific cyber security standards left many maritime operators uncertain about what measures they should take on their own behalf.

Emerging standards applicable to the marine industry and improved, if imperfect data is leading to improvements in this field. In 2011, the European Union Agency for Network and Information Security (ENISA) published one of the first reports on maritime cyber security.[2] The Government Accountability Office (GAO) published a report on cybersecurity and maritime critical infrastructure in 2014,[3] with other reports and preliminary standards coming from industry, the U.S. Coast Guard, and the International Maritime Organization.

These emerging standards are providing marine operators and insurers with a basis for determining an appropriate level of "due diligence". Vessels must be sea-worthy and cyber-

[1] https://shipandbunker.com/news/am/171559-recent-cyber-attacks-highlight-bunker-industry-vulnerability Accessed 2 April 2018.
[2] https://www.enisa.europa.eu/news/enisa-news/first-eu-report-on-maritime-cyber-security, accessed 2 April 2018.
[3] https://www.gao.gov/products/GAO-14-459, accessed 2 April 2018.

worthy if they wish coverage from insurance providers. Even if covered by insurance, a vessel's liability due to, for example, a GPS spoofing or jamming incident may be dependent on the cyber measures the operator took to anticipate, prevent, and prepare for such an event. Furthermore, what measures apply to what companies remains uncertain, as does the way in which a client is expected to demonstrate their adherence to those practices to an insurance provider.

Cyber Insurance and Maritime Industry

Cyber insurance has grown from perhaps $150 million in 1999 to a $3 billion market by the end of 2017, with a limited number of very large writers with premiums in excess of $100 million, and additional carriers in lower ranges. As the market has grown, carriers have begun to acquire data to help evaluate risk. One study looked at approximately 8,000 cyber related incidents impacting various subsectors of the maritime industry over the last 20 years. Some observations from this data include:

- While the number of incidents per company has remained steady, the total number of incidents, and the total number of companies affected is going up
- Although a third of incidents have zero losses, average loss per incident is now at approximately $2 million and growing
- The peak loss for a single incident is growing, with some now in the $80-$100[4] million range
- Malicious data breaches and unauthorized disclosures are the most common type of incidents
- IT processing losses are rare but have the highest cost per incident
- Within the maritime industry, the ports, harbors, and infrastructure sub-sector are second only to marine financial services in terms of the number of incidents per company
- Unlike most industries, in the marine industry, there seems to be no correlation between the size of a company and the total financial loss associated with a cyber incident

While this limited study is informative, insurance carriers knows that it is limited by a lack of transparency and information sharing about cyber incidents from the marine industry. Improved data will help the insurance industry reduce uncovered losses and provide better coverage. While cyber security has clearly moved from the realm of the IT specialists to the board room,[5] the challenges maritime operators and the marine insurance industry face in assessing and evaluating cyber risks demonstrate that much work remains. This includes better technical solutions, improved data analysis, information sharing, policy, and oversight/auditing.

[4] Marine operator Maersk suffered a $300 million loss from the notPetya incident in 2017

[5] The Security and Exchange Commission began addressing cyber risks and disclosures in 2011, and provided updated interpretive guidance in February of 2018

Additional Questions and Future Research

- How does cyber technology impact war risk insurance? In marine insurance, acts of war are typically not covered by insurance policies, and special limitations apply to acts of terrorism. It is unclear if and how a nation-state based cyber attack on a vessel operator, especially one carrying a national security cargo, would be addressed. This same question may be considered from the perspective of a combined cyber and physical attack.
- Moral hazard is the phenomena whereby one party decreases responsible behavior after transferring risk to another, as in insurance. As cyber insurance for the maritime industry is relatively new, and mature regulatory standards are not yet in place, is it possible that insured (but unregulated) marine operators may actually reduce their compliance with cyber security best practices, resulting in increased incidents?
- Lack of information sharing and incident reporting is a widely recognized problem with cyber, particularly in industries that lack clear disclosure requirements. Anonymous surveys, or a comparison to industries that are subject to disclosure requirements (e.g. banking, credit, and electrical grid) could reveal the extent of impacts in the marine industry.
- Since insurance providers are requiring marine operators to demonstrate some level of compliance with cyber standards, a "before and after" study of the number and impact of cyber incidents would be very useful in revealing how effective these standards actually are. Another approach would be to compare the number and impact of incidents of an insured company with a comparable, but uninsured operator.

Appendix A – Cyber Security Insurance Coverage

1. Most Cyber Insurance policies are modular in nature, as they contain a number of different coverages blended under one policy form. Below is an overview of the coverage sections in a typical cyber insurance policy form.

first-party costs (direct loss and/or out of pocket expenses incurred)
third-party costs (claims and defense expenses, including damages and settlements)

Coverage	Description
Business Income/ Extra Expense	Reimbursement for loss of income and/or extra expense resulting from an interruption or suspension of computer systems due to a failure of technology. Includes coverage for dependent business interruption and forensic expenses.
Data Asset Protection	Recovery of costs and expenses you incur to restore, recreate, or recollect your data and other intangible assets (i.e., databases, software, applications) that are corrupted or destroyed by a computer attack.

Event Management	The following costs resulting from a privacy breach or cyber event: • Forensic services. • Breach notification services (including legal fees, call center, etc.). • Identity/fraud monitoring expenses. • Public relations.
Cyber Extortion	Costs of consultants and extortion monies for threats related to interrupting systems and releasing private information.
Privacy Liability	Defense and liability for failure to prevent unauthorized access, disclosure or collection of confidential information, or for failure of others to whom you have entrusted such information (e.g., pension actuary, data storage facility, credit card processor). Also includes liability for not properly notifying of a privacy breach. Coverage includes corporate information such as third-party trade secrets. Likely Claimants: customers, employees, trading partners.
Network Security Liability	Defense and liability for failure of system security to prevent or mitigate a computer attack including but not limited to spread of virus or a denial of service. Failure of system security includes failure of written policies and procedures addressing technology use. Likely Claimants: third-party loss, customers, employees.
Privacy Regulatory Defense Costs	Costs to defend an action or investigation by regulator due to a privacy breach, including indemnification for any fines or penalties assessed. Likely Claimants: Attorney General, FTC.
Media Liability	Defense and liability for online libel, slander, disparagement, misappropriation of name or likeness, plagiarism, copyright infringement, negligence in content to those that relied on content. Likely Claimants: authors, producers, publishers, competitors, license holders.

Biographical Statement:

Andrew Tucci

Andrew Tucci is a U.S. Coast Guard officer with 28 years of service. He has spent much of his career working with commercial vessels and ports. He helped author the Coast Guard's Cyber Strategy, and has had a leading role in developing maritime cyber risk management policies.

Panel on Advancing Maritime Cyber Education and Research
Christopher W. Doane

Abstract

This paper discusses the criticality of cyber security, and the intense need to improve cyber security education, and to increase funding in this area. This paper discusses the allocation of funding by the military, and the need to increase funding in the cyber security sector. Developing cyber security programs at a higher educational level is also stressed, and the necessity of these programs is outlined.

Defense of Maritime Security System (MTS) is critical to both the U.S. and global economy. As the MTS becomes increasingly reliant on technology and automation, cyber security becomes a more vital element of defending the MTS. As the vast majority of the U.S. MTS is privately owned and government regulated, both sectors must come to grips with this rapidly evolving vulnerability. This requires continuously educating both management and employees on cyber security and developing a clear career path for cyber security professionals.

Mr. Sean Plankey, Cyber Intelligence Advisor for BP, stated that for the federal workforce, specifically the U.S. Coast Guard, to move forward in developing cyber expertise they need to make investments in their people. Mr. Plankey noted that the militaries, including the Coast Guard, are willing to invest about $250K and two years to train a pilot as accepted cost. The U.S. has enjoyed air superiority since World War II, but is not dominant in cyberspace and yet, there is still a debate on investments in a cyber-career path and education plan.

Mr. Plankey offered several thoughts to close out his comments. Cyber is not about certifications, it is about capability; experience in Information Technology is not a qualification. Rather than changing processes for cyber security, seek to improve systems and security posture through the inclusion of cyber security. It is all about the long game; cyberspace is the most contested environment, more so than the physical domain. National security matters and cyber threats to critical infrastructure are threats to the nation; ports are critical infrastructure.

RADM Kevin Lunday, Commander, U.S. Coast Guard Cyber Command, has the mission to assist operational commanders. Admiral Lunday identified cyber space as a dynamic and rapidly changing operational domain that requires continuous learning. Within the cyber domain, people, not technology, are most important. Admiral Lunday recommended the National Initiative for Cybersecurity Education (NICE) Framework, with its 50 specific work roles in cyber space, as an excellent source for a common set of standards, education, training, and certification for government and the private sector. He also noted that the U.S. Coast Guard Academy is preparing to offer a Cyber Systems major. (Editor's note: It now does so. See

https://www.uscga.edu/cyber-systems/) He concluded by suggesting that formal cyber education programs must be grounded in the law, ethics, and human behavior.

Dr. Susanne Wetzel, Professor of Computer Science at Stevens Institute of Technology, built upon RADM Lunday's comments regarding cyber education. Dr. Wetzel described how cyber security at Stevens has migrated from a Master's program down to a Bachelor's program independent from a specified technical field. She agreed with RADM Lunday regarding the interdisciplinary requirements as cyber touches all domains. She also noted that universities are following the Department of Homeland Security and National Security Agency criteria, but an independent accreditation body is needed. She further noted that there are not enough students in the education pipeline to fill anticipated positions. She suggested that an underlying problem in drawing students into a cyber education program is understanding what a cyber career path looks like – What does working in cyber security look like? What room is there for professional growth? Finally, Dr. Wetzel noted that cyber education needs to start early in life.

Dr. Dave Mayhew, Director of Secure Architecture Initiative and the Secure Architecture and Infrastructure Laboratory at the University of Alabama, continued the cyber education and career path discussion identifying a natural tension between what is good for the student (understanding) and what is good for the employer (technical savvy to meet immediate short-term needs). In the years available to them, Dr. Mayhew argued that schools cannot teach students both principles and technical skills. Industry must plan on hiring employees who cannot produce for 12 to 18 months as they learn the technical aspects. Dr. Mayhew echoed the interdisciplinary nature of cyber noting that cyber is everything; it touches or is in everything. As such, it defies universities' traditional silos of education. He also supported the need for a cyber-accreditation body as cyber is hot and cyber degree programs are popping up everywhere. Dr. Mayhew concluded by declaring that employers must influence higher education to teach principles over technical knowledge and that those seeking an education in cyber should choose colleges that are contributing to the science and are involved with industry.

Major Alan Lin, Assistant Professor of Computer Science at the U.S. Air Force Institute of Technology, addressed educating the workforce in cyber security through games and gamification (using game elements implicitly or explicitly in something that is not a game). Major Lin noted that games offer a chance to practice what is learned. Research questions that Major Lin is focused on are: 1) General cyber training is hygiene focused, what about operations? 2) Cyber is not a solo effort, how can we do collaborative training? 3) Current training is not fun, how can we teach/learn concepts efficiently making it more fun and/or interesting? Major Lin discussed his focus on developing serious games to spur critical thinking

about risks, missions, and resources with a focus on decision-making and employing cyber effects.

The question and answer phase of the panel brought out five main themes: 1) Need to teach employees/users an understanding of the cyber threat and how it works, just telling them what not to do is ineffective; 2) Provide employees with a "hotwash" when an attack occurs – what happened, how did it happen, how to prevent it from happening again; 3) Cyber security requires a cultural change in how we view and incorporate cyber into our management hierarchy; 4) People are the weakest link and the greatest strength (if properly trained and/or educated); and 5) We must make our cyber systems resilient to people, they will do unexpected and irrational things.

In summary, the panel identified an urgent need for the U.S. Coast Guard and MTS operators to invest more effectively in cyber security, both in terms of importance to senior leadership and educational investment including a clear career path for cyber professionals. Universities must join in this educational investment creating an independently accredited, multi-disciplinary program that provides cyber graduates with a broad understanding of the legal and ethical issues related to cyber as well as favoring a broader theoretical understanding of cyber security over a technically-focused education. For the existing workforce, government and private sector employers must invest in a program of continuous learning for their work forces that is tailored to their generational and individual aptitudes and broadens their understanding of cyber security threats, vulnerabilities, and necessary mitigations. As noted in the question and answer period, employees can be the cornerstone of cyber defense, or the weakest link, the outcome depends upon the investment decisions of senior executives in government and the private sector.

The conclusions of the panel suggest multiple research opportunities. What is the most effective organizational structure for an effective government or private sector cyber security program? What is the optimum university level curriculum for future cyber security specialists? What is the right relationship between industry and academia in defining an effective cyber education? What are the appropriate demographic delineations within the workforce and what are the most effective training/educational techniques for each group?

Developing an effective cyber security continuum within the Coast Guard and maritime sector is vital to the defense of our MTS and by extension our national economy. Success requires the immediate attention of Coast Guard and industry senior executives, academia, and education researchers.

Panel: Maritime Cyber - An Industry Perspective
Mike Edgerton

Abstract

The panel provided an industry perspective on maritime cybersecurity. Key issues identified included the fact that private sector drivers for security and risk assessment and treatment are different from government's, that the private sector's level of cybersecurity maturity is relatively low, and that risk management is focused on liability and insurance rather than regulatory compliance.

Panel Overview

This panel consisted of presenters who represent the commercial perspective of maritime cybersecurity. They included:

- Mr. Max Bobys, HudsonAnalytix, Inc.;
- Mr. James Dean, TrueCourse Advisory Services, LLC; and
- RADM John Crowley, USCG (Ret.), Executive Director of the National Association of Waterfront Employers (NAWSE) and Chair of the National Maritime Security Advisory Committee.

The panel was facilitated by Mr. Mike Edgerton, Vice President of HudsonTrident, Inc. Each panel member provided a presentation regarding their perspective on maritime cybersecurity and the private sector.

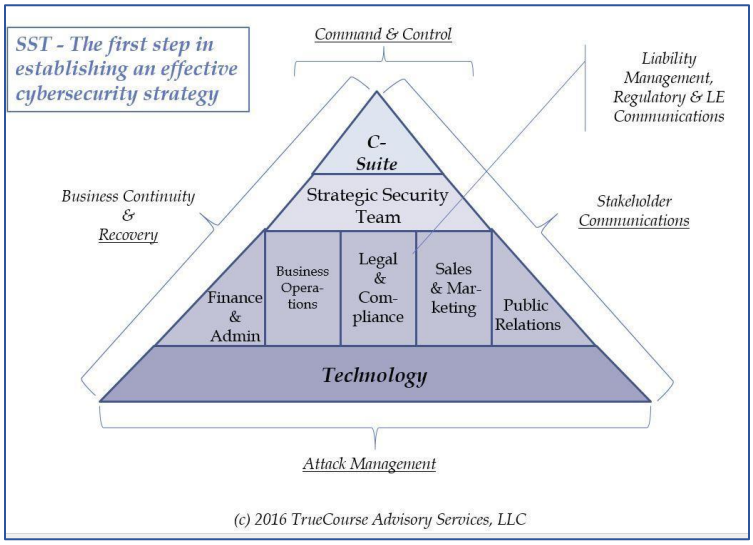
RADM Crowley's presentation noted that cybersecurity has not been defined in the Maritime Transportation Security Act and whether it poses a national security threat has not been clearly established. RADM Crowley also highlighted the importance of non-industrial or operational systems in the port environment to include systems with a focus on data such as personnel records, financial systems, and systems with cargo information (Terminal Operating Systems). This is important because much of the focus on maritime cyber security has been on industrial control systems (such as SCADA) or operational systems where cyber attacks can lead to physical impacts versus industry's concern regarding the integrity and security of data.

Mr. James Dean's presentation supplemented RADM Crowley's key points by adding additional detail to the premise that maritime cybersecurity includes data integrity as well as the physical impacts of attacks on industrial controls and operational systems. Further, Mr. Dean provided an overview of some of the weaknesses identified in the industry regarding the ability to address cybersecurity. These include:

- Lack of training and awareness;
- Lack of information sharing;
- Lack of cyber contingency plans;
- Lack of patch management;
- Significant unaddressed vulnerabilities both afloat and ashore; and

- Best practices not being implemented.

Mr. Dean provided a model that could be used by the private sector to address and manage cyber risk:



Mr. Max Bobys provided four key issues that are of concern to the private sector:

- Competitive imperatives mean executives must accept a certain level of cyber-attack risk;
- The implications of cybersecurity are pervasive, and this impedes the adoption of risk-based strategies. Cyber risk touches every business function and process;
- Cyber risk is difficult to quantify. There's no single quantitative metric such as value at risk for cybersecurity, making it much harder to communicate the urgency to senior managers and engage them in required decisions; and
- It's hard to change institutional behavior.

Mr. Bobys also presented the industry's perspective in managing and treating risk with a focus on the potential role of insurance, while nascent, in addressing maritime cyber security. Mr. Bobys also reiterated some of the findings noted by the previous speakers that the industry was relatively unprepared and recommended that a maturity model approach would be appropriate the absence of external government or international regulations or standards. A maturity model approach allows managers to prioritize and sequence activities thereby making the development of a cybersecurity program more manageable. The maturity model approach divides cyber security into a series of domains and then measures an organization's level of maturity against international leading practices such as the National Institute of Science and Technology:

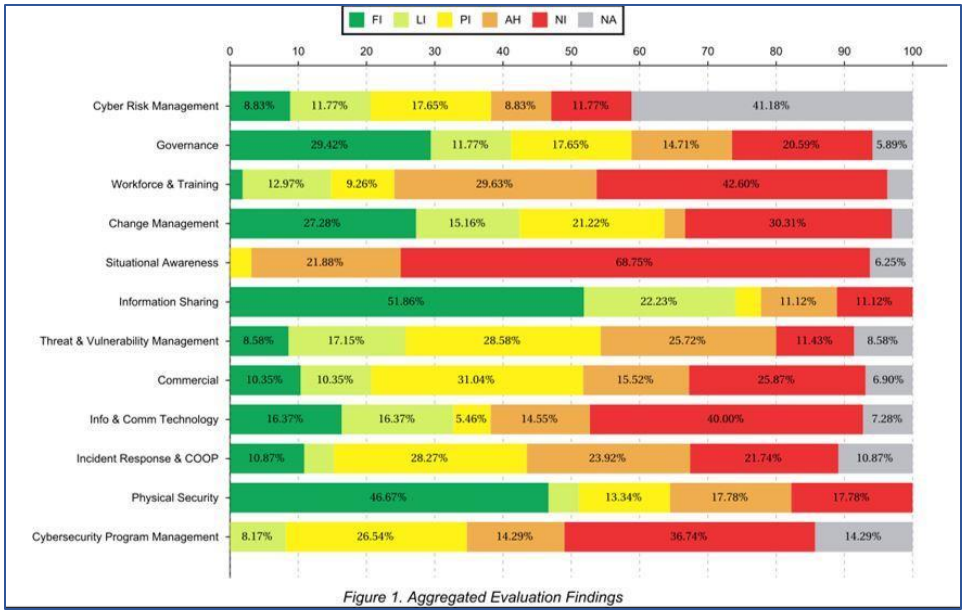


Figure 1. Aggregated Evaluation Findings

The following key issues were identified as key learning points:

- The precise nature of cybersecurity as a threat and risk in the maritime domain is not clear;
- For the private sector, the integrity of the data within information systems is important in addition to the security of industrial and operational controls;
- The private sector will be influenced by the requirements of insurance providers and clients as well as any regulations or standards that are put in place; and
- Top management must be engaged in order to ensure that cybersecurity is addressed throughout the enterprise.

Potential research questions include:

- Potential governance solutions to cybersecurity in the private sector: Incentivization versus compliance.
- How to manage reporting of cyber incidence while protecting brand and reputation: What is the role of anonymization technology and how can companies be prompted to participate?
- Who is in charge of maritime cyber security? The Coast Guard has drawn fairly tight lines around their area of concern which is largely anything that can impact the enforcement and compliance with MTSA. What about security of systems that are outside the purview of the USCG such as cargo data, personnel and financial data? Is there a "whole of government approach" or another non-governmental model?

Biographical Statement:

Mike Edgerton

Mike Edgerton is responsible for HudsonTrident's security and resilience practice. A retired military officer, Mike has specialized in security, emergency response, and intelligence for over 30 years, including 8 years as Principal of an international security consultancy in the Middle East. He is the author of the book, "A Practitioner's Guide to Effective Maritime and Port Security".

Panel: Maritime Cyber Risk - The Holistic View
Mark R. Heckman, University of San Diego

Abstract

Panel 6 covered the topic "Maritime Cyber Risk: The Holistic View". The panelists discussed various aspects of how the interconnection of many disparate maritime systems, of different stages of technological advance, can lead to additional risks, and how to handle those risks as the systems evolve. The panel moderator was Capt. Paul Tortora of the USNA. Panelists were Dr. David Nicol of the University of Illinois, Dr. Mark Heckman from the University of San Diego, Dr. Isaac Porche of the RAND Corp., and Mr. Andrew Pasternak, U.S Department of Homeland Security.

Presentations

Captain Paul Tortora, the moderator, began by taking "moderator privilege" to mention two cyber courses required at the Naval Academy. Freshmen take an introductory cyber course

where they learn such fundamentals as operating system principles, basic coding/scripting, how to set up secure networks, introductory cryptography, and participate in an attack/defense lab. Juniors all take a course in cyber physical systems and cyber engineering. Students in the freshman course are taught that the cyberspace environment as a whole functions on different, interconnected levels: individual and cyber identity (cyber persona), information (logical), physical network and geographic component (physical environment). This contributes to the type of complexity that the panel is grappling with.

Andrew Pasternak started his talk by explaining the mission of the Office of Cyber and Infrastructure Analysis of the DHS National Protection and Programs Directorate: strengthening the security and resilience of U.S. critical infrastructure, which includes the Maritime sector. The thrust of Pasternak's talk was on assessing the physical consequences of cyber-attacks on ports.

At least for now, ports are somewhat resilient to physical impacts of cyber incidents. The sector is loosely interconnected so that many disruptions are only local and temporary, and shipping companies and other stakeholders can often find physical workarounds. The effect of a disruption is primarily the loss of business by the affected terminals and the local providers. But consequences to a region, such as when there is only one significant port in a region, as with San

Juan in Puerto Rico, can be severe. Scenarios with consequences at the National level, Pasternak, said, are theoretically possible, but less likely.

It is important when assessing the physical impacts of cyber incidents to put them into context. Assessments must consider multiple variables, including the identity of the victims, the location, recovery time, and the physical mitigation measures available, such as re-routing ships, shipping by air, or finding domestic sources. When performing assessments, it is important to remember that there is really no such thing as port security. There is only the security of the different entities in the port, such as terminal operators, vessels, and service providers. These do not form a whole. The security of each entity and the impacts must be separately assessed.

David Nicol tried to answer the question, "how should stakeholders adequately protect currently installed systems of various stages of technological advances, while planning for even more advanced and interconnected maritime systems in the future?" For the sake of practicality, Nicol added an additional constraint of using currently available technology. Nicol pointed out that this is a very complex question due to the multiple independent commercial entities in a port "who owns the problem?", the fragility where subsystems interface that leads to the introduction of unanticipated vulnerabilities, a variety of legacy hardware and software, and a lack of understanding of the overall system risk due to a small failure because dependencies are often not obvious and failures can cascade. Nicol used the example of an expired digital certificate that leads to unexpected behavior of higher-level software that suddenly stops. In addition, a maritime cyber system may contain vulnerable subsystems that one would not expect, such as email and web servers, which are known to have many vulnerabilities, or else users with a need to download files and software updates from outside can introduce malware into the system.

Nicol said that industry best practices, such as those from NIST, if correctly and diligently applied, can lead to a great deal of improvement in the security posture of maritime cyber systems. But those best practices are often ignored because of ignorance, inattention, or inconvenience. Nicol finished by warning of the creation of new cyber compliance requirements for the maritime sector that will institutionalize the best practices. But that "will not solve the problem". What will help is better computer hygiene, using available technology. For example whitelisting applications and outbound connections, sandboxing applications, and enforcing rigorous limitations on connections to systems devices.

Isaac Porche said he wanted to find a solution to the problem of maintaining legacy systems while enabling upgradeability with enhanced cybersecurity, but he admitted that he could not find a solution. Increasing connectivity, Porche said, creates a need for interoperability, which increases complexity, leading to vulnerabilities in systems. The Internet of Things is a prime example of that today.

The attack surface – points of entry to an attacker – include man, machine, and links between them. The many components in a system greatly increase the attack surface. And unanticipated functionality in complex software is a major source of vulnerabilities.

Given all of these factors, what can we do with respect to the question that Porche set out to answer? Porche has several suggestions:

- Embrace heterogeneity – Diversity and a lack of connectivity in systems can increase resilience
- Avoid digitizing everything – Analog is often just as good, or better, than digital, and less vulnerable.
- Do a lot of penetration testing – "Cybersecurity is a contest of human capability". Let your smart people try to break things and fix it before the bad guys have a chance. Do this at all phases of the system lifecycle.
- Deploy new or patched software faster than the bad guys do – Acquisitions and operations are a key factor in success here.

Mark Heckman started his talk with a fable. There were once two restaurants that were both found by the health inspector to satisfy the policy that "every customer gets a clean plate". One restaurant washed dirty plates as they came in from the dining room and put the clean plates in a stack. Whenever a clean plate was needed, staff would take it from the stack. The other restaurant used a "just in time" plate washing strategy. Dirty plates were stacked, and whenever a clean plate was needed, staff would take a plate from the stack and wash and dry it. Then the restaurants and their staffs merged. The question Heckman posed was, "do customers still always get clean plates"?

Obviously, the answer is no. Some of the staff will stack clean plates and others will stack dirty plates; some staff will wash plates they take off the stack and others will not. The composition of the two plate washing systems, each of which satisfied the clean plate policy, does not satisfy the policy.

Heckman said the security composition problem is well-known in security circles: a system consists of multiple components, each component has security properties, but what are the security properties of the system as a whole? Sometimes, as with the restaurant example, the combination of components is destructive to the policies enforced by the components. And sometimes a composition can lead to the creation of new properties, called emergent properties, which did not exist individually in any of the components and that create new security holes.

Maritime systems are compositions of many different components. New vessels, for example, increasingly consist of many different digital subsystems. And a port consists of systems that belong to many different stakeholders, each of which has their own security needs that may be different than another's. How can the composition of all of these disparate systems be shown to enforce some reasonable notion of security.

The only proven method for solving the composition problem, Heckman said, is that described in the Trusted Network Interpretation (TNI) of the U.S. Department of Defense's Trusted Computer System Evaluation Criteria (TCSEC, also called the "Orange book"). It uses a divide and conquer approach, where the overall system security requirements are broken into subtasks, which are distributed to system components. This permits components to be developed independently, while simplifying efforts to reason about the security properties of the system as a whole when the components are combined.

But, as Heckman pointed out, we don't currently have any TCSEC-evaluated systems to use (the program was abandoned in 2000). Nevertheless, some of the techniques used in the TNI,

such as the focus on system policy to drive design, and divide and conquer, can be used today. The alternative is the current ad hoc approach with endless patch and pray cycles.

Research Questions

Most of the panelists noted that a maritime system is really a composition of many subsystems or components. Pasternak identified a need to find a method for assessing risk, especially when the actual risk is influenced by physical, non-cyber factors. Nicol suggested that ways must be found to encourage or mandate the consistent and comprehensive use of industry standards and best practices throughout the maritime sector. How best to do this, though, is a research question. Porche suggested that the drive to make everything digital and interconnected may be creating high security risk without an equivalent reward, but it is a research question as to how to find the best balance between new digital and old analog approaches. Heckman identified that potential security problems can be created simply by connecting otherwise secure components, and that the best way of avoiding this problem is to start by considering the desired security properties of an entire system, then to delegate portions of the security requirements to different components. But he did not identify a way that this could reasonably be accomplished, especially with many different stakeholders all pursuing their own interests. That, too, is an open research question.

Panel: Cyber Work at the DOE National Laboratories
Craig Moss

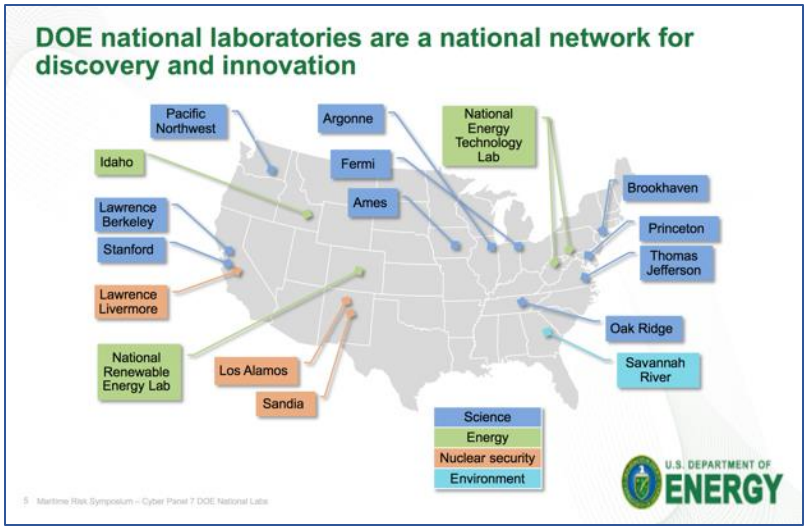
Abstract

The DOE National Laboratories mission is to advance science and technology to fulfil our sponsors missions, of which the Department of Homeland Security (DHS)/United States Coast Guard (USCG) is one of those sponsors. Additionally, leveraging research and infrastructure that exists at the National Laboratories can expand the reach of the USCG and the eleven current Centers of Excellence (COE). The goal of this panel is to communicate maritime cyber security capabilities including operational, infrastructure and research at four National Laboratories (Argonne National Laboratory, Lawrence Livermore National Laboratory, Oakridge National Laboratory, and Pacific Northwest National Laboratory) then discuss possible ideas for collaboration across the USCG/COE. These collaborations may include access to infrastructure, inclusion in research, or information about operational procedures. Note that the collaborations could go from the USCG/COE to the National Laboratories or from the National Laboratories to the USCG/COE.

The DOE Laboratory System

The mission of the Department of Energy (DOE) is to ensure America's security and prosperity by addressing its energy, environmental and nuclear challenges through transformative science and technology solution. The DOE is responsible for the stewardship of seventeen laboratories making up a preeminent federal research system, providing the Nation with strategic scientific and technological capabilities.

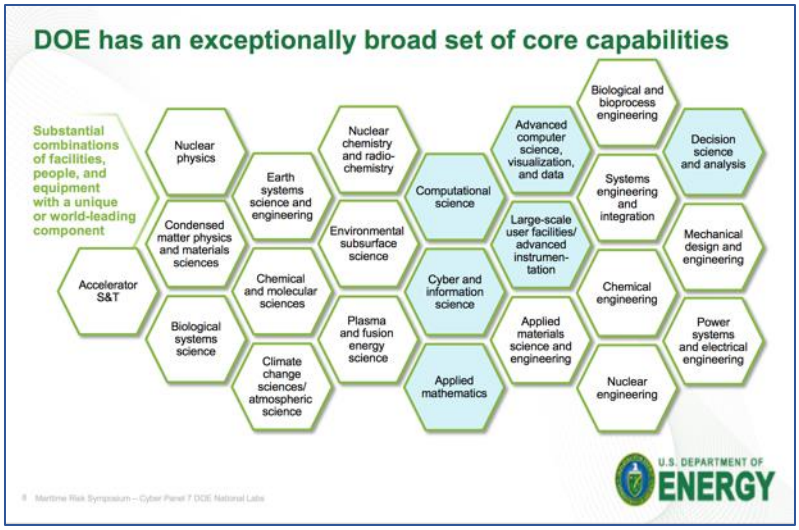
This complex of national laboratories:



- Executes long-term government scientific and technological missions, often with complex security, safety, project management, or other operational challenges;
- Develops unique, often multidisciplinary, scientific capabilities beyond the scope of academic and industrial institutions, to benefit the Nation's researchers and national strategic priorities; and;
- Develops and sustains critical scientific and technical capabilities to which the government requires assured access.

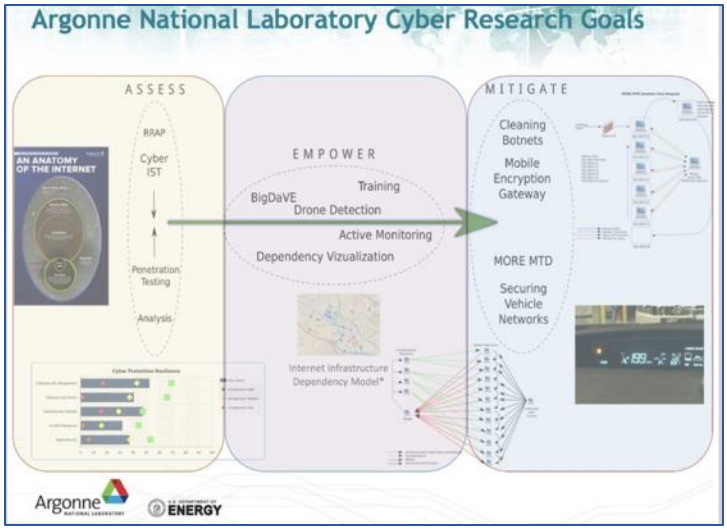
Cyber security research is a priority for DOE principally with a focus on the protecting critical energy infrastructure. Cyber security for energy infrastructure follows a multi-disciplinary approach involving many of the research capabilities across the DOE National Laboratory complex. Cyber security research for energy infrastructure is essentially the same as cyber security research for most other domains, to include maritime.

Research at the National Laboratories is not only performed for DOE but also other sponsors representing the whole of government look to the DOE National Laboratories to support their specific research and develop needs. To demonstrate this dynamic we will explore the cyber security research being performed at four of the National Laboratories, Argonne, Lawrence Livermore, Oak Ridge, and Pacific Northwest to understand their larger focus and research efforts.

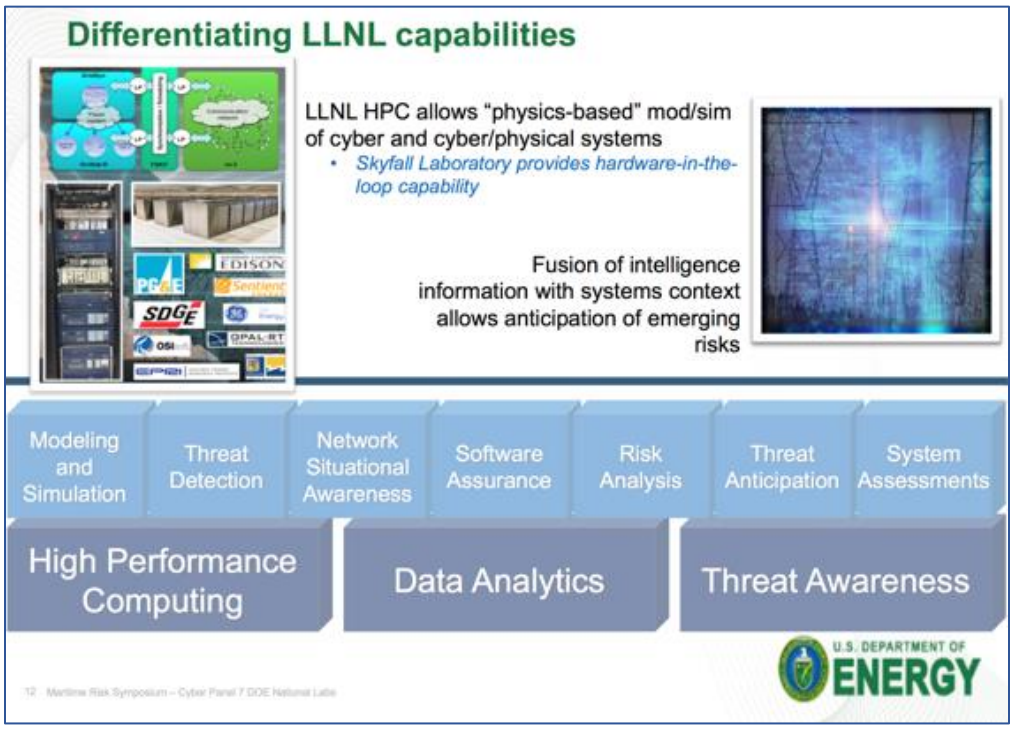


Argonne National Laboratory (ANL)

Maritime Systems embody many aspects of traditional information systems and industrial control systems. As such, many different mitigating strategies such as protecting network ingress and egress; defense in depth; and other industry best practices can provide useful starting points towards increasing security posture and approaching resiliency. Understanding the requirements of information processing and storage yields insights into constraints faced while preserving business requirements and minimizing effects to commercial maritime operations. Argonne National Laboratory's (ANL) past experience within both industrial control systems and risk analysis/management have offered insights into protecting and improving systems while meeting operational requirements. Furthermore, collaborative work between ANL automotive engineers and cybersecurity analysts on Controller Area Networks (CAN) can provide insights into risk-laden areas within their inclusion, and deployment, within maritime vessels. This holistic view of maritime information systems leads to a more complete understanding of cybersecurity risk within the domain and will drive security improvements



Lawrence Livermore National Laboratory (LLNL)

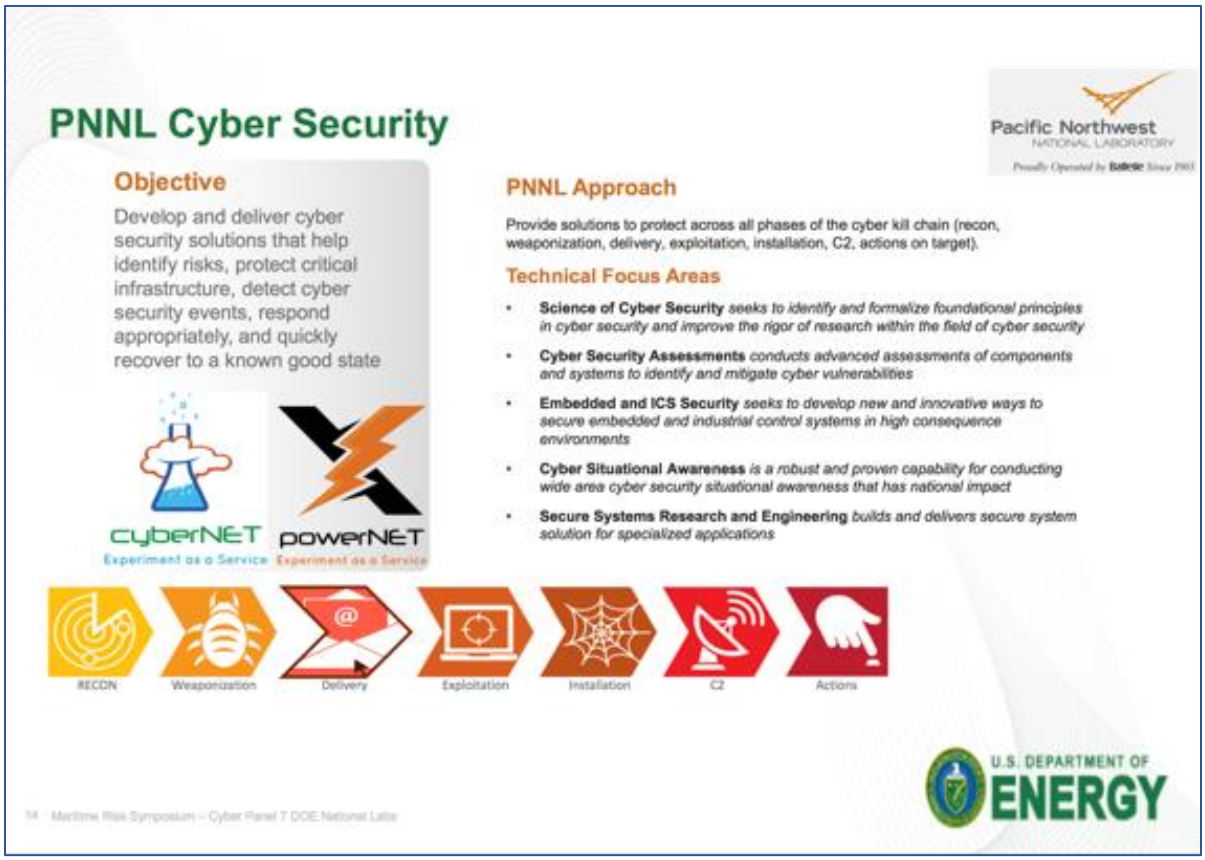


Oak Ridge National Laboratory (ORNL)

Because it is impossible to create perfectly secure systems, resilience is critical. We have to understand what can go wrong, how it can go wrong, answer the question "what next," and understand how networked systems can enable (or hinder) that. At ORNL we have been focused on "blended threat models" in the vehicle, industrial control, and energy delivery systems. These models take into consideration both the information (IT) and operational (OT) sides of the system, as well as seeking to understand how attacks on the physical systems enable attacks on the networked systems, and vice-versa. Maritime systems exemplify these challenges, with their reliance on GNSS, electronic navigation charts, and internal networks. By understanding how blended

attacks evolve we can identify physical side channels and other observables that enable the rapid identification of anomalous behavior, intrusions, tampering, and attacks. ORNL projects such as Beholder (using a timing side channel) and Heartbeat (using the power consumption side channel) are examples, while projects such as Hyperion (automated static analysis of compiled software) can be used to detect "sleeper" malware before it can activate.

Pacific Northwest National Laboratory (ORNL)



Enhancing Maritime Cybersecurity: Key Themes and Research Questions From Maritime Risk Symposium 2017 and Further Thoughts on the Way Forward

Fred M. Rosa, Jr. and John E. Crowley, Jr.

Introduction

The United States is dependent on the global Maritime Transportation System (MTS) to move approximately 90% of its overseas trade and handle more than $1.3 trillion in cargo each year. Any significant MTS disruption – in terms of scale and/or duration – would have a major, if not devastating, negative impact not only on the domestic economy, but also on the capacity of the global supply chain to effect the just-in-time delivery of goods on which the American public is heavily dependent.[1]

Over the past ten years, the risk of such an MTS disruption has been increasing due to the emergence of many different capable state and non-state cyber threat actors, coupled with the maritime sector's growing dependence on cyber-enabled information, communications, and industrial control systems.[2] In the early aftermath of the 9/11 attacks, the maritime component of the U.S. domestic counter-terrorism program focused primarily on kinetic threats to vessels and ports. Today, however, the U.S. Intelligence Community regards cyber threats as among the foremost threats to national security,[3] and the scope of maritime security efforts has expanded to include the relevant vulnerabilities and associated potential threats against the cyber-enabled technologies essential to MTS operations.[4]

In November 2017, Tiffin University hosted the eighth annual Maritime Risk Symposium (MRS) focused on maritime cybersecurity.[5] MRS 2017 convened more than 200 government, industry, academic and other key stakeholders from the local, state, and national level, as well as a number of their international counterparts, for wide-ranging discussions on this critical topic.

---

[1] U.S. Government Accountability Office, *Maritime Critical Infrastructure Protection: DHS Needs to Enhance Efforts to Address Port Cybersecurity* (GAO-16-116T) (Washington, DC, 2015), i.

[2] U.S. Department of Homeland Security, National Protection and Programs Directorate, Office of Cyber and Infrastructure Analysis, "Consequences to Seaport Operations from Malicious Cyber Activity" (Washington, DC, 2016), 1-5.

[3] U.S. Congress, Daniel R. Coats Statement for the Record of the Senate Armed Services Committee, "Worldwide Threat Assessment of the U.S. Intelligence Community," 115th Cong., 2nd sess., March 6, 2018 (Washington, DC, 2018), 5-6.

[4] Drew Tucci, Joe DiRenzo III, and Scott Blough, "Cyber Shoal Waters: Understanding and Meeting Emerging Cyber Threats to the Marine Transportation System," *Maritime Reporter and Engineering News*, 79, no. 10 (October 2017): 1-5.

[5] Tiffin University, Program for the 8th Annual Maritime Risk Symposium, November 13-14, 2017 (Tiffin, OH, 2017), 3-10, https://www.tiffin.edu/criminaljustice/maritime-risk-symposium-2017/agenda.

This paper provides an overview of the program's final session that sought to capture the most important themes addressed during the symposium as well as the most significant research questions that emerged during the discussions.

Before distilling key MRS 2017 outcomes, the authors would offer their fundamental perspective on MTS cybersecurity – a perspective primarily focused on three major current impediments to further progress in addressing this challenge.

1. The essence of the first impediment is straightforward. There remain widely disparate views relating not only to the definition and scope of cybersecurity, but also to the nature and scale of the risks associated with a failure to adequately counter this challenge. Without reasonable concurrence on the right framework of fundamental questions – a framework that evolves at the rapid pace of technology and connectivity – forging agreement among the many stakeholders on a fully comprehensive strategy and required solutions is presumably impossible.

2. The second impediment has a close nexus to the first. Here in the United States, and particularly in the maritime realm, there is a general lack of coherent understanding as to the roles of the many federal holders of cyber authority, expertise, information and capability. With respect specifically to the maritime realm, the Departments of Commerce, Defense, Homeland Security, Interior, Justice and Transportation, as well as the Intelligence Community and various component agencies and independent entities, all have an oar in the confused cyber waters. As a result, while the Coast Guard, the Federal Bureau of Investigation (FBI), and the Department of Homeland Security (DHS) are generally recognized as the lead cyber actors on the waterfront, there is no single agreed-upon lead for the maritime community to follow on an ongoing basis, and then turn to when cyber defenses fail.

3. Finally, today virtually everyone in the maritime realm is familiar with cyber risk and acknowledges the need for cybersecurity. Yet few understand the many technical, economic, legal, regulatory, management, insurance, and other dimensions of this complex global challenge, or the persuasive case for mobilizing on an urgent basis to meet this challenge. The third impediment is simply that, without a compelling call to action by key stakeholders in both the public and private sectors, the required mobilization is unlikely to happen – at least not before a possible future high-consequence maritime cyber event.

SYMPOSIUM HIGHLIGHTS

The MRS 2017 wrap-up session featured an impressive panel of four distinguished experts:

- Major General Randy "Church" Kee, U.S. Air Force (Ret.), Executive Director, Arctic Domain Awareness Center (ADAC), University of Alaska;
- Rear Admiral Kevin Lunday, U.S. Coast Guard, Commander, Coast Guard Cyber Command, and Assistant Commandant for Command, Control, Communications, Computers, and Information Technology (C4IT);
- Dr. Fred Roberts, Director, Command, Control and Interoperability Center for Advanced Data Analysis (CCICADA), Rutgers University; and
- Captain Drew Tucci, U.S. Coast Guard, Commander, Sector Long Island Sound, and one of the chief architects of the first-ever U.S. Coast Guard *Cyber Strategy* (June 2015).

This final session kicked off with the following question: what were the most significant maritime cybersecurity themes noted during the symposium? The highlights that emerged from the ensuing discussion by panel experts and other participants are perhaps best organized in five theme baskets: risk management; vulnerability assessments; cyber-physical convergence; cyber actors; and preparedness and response.

Risk Management

It is well established that the maritime sector has centuries of experience in managing various categories of risk. Major cyber-related risk, however, is a comparatively new phenomenon that presents unique challenges in terms of maritime risk management. There is a clear need for useful ways to model and quantify cyber risk – and then integrate the results into the full-spectrum framework for all the many other risks that require proactive management by maritime enterprises.

The concept of resilience has emerged as a complement to risk in understanding, measuring, and addressing maritime cybersecurity. There is also a clear need for innovative approaches to modeling and quantifying resilience. Without such a capability, it is difficult to assess whether measures intended to enhance the resilience of a maritime asset or system – many of which measures involve substantial costs – are actually having a positive impact and, if so, to what extent.

Vulnerability Assessments

Vessel, waterfront facility, port and other key infrastructure, and supply chain vulnerability assessments are vital to ongoing efforts to improve maritime cybersecurity. They are key to managing risk and have generally been required for the implementation of national maritime security measures as currently defined under the law. These assessments – which are increasingly common in the maritime realm, but far from universal – should be rigorous and comprehensive, and the results should be significant inputs to the ongoing risk management process.

Cyber Actors

Perceptions of the cyber domain – including its security dimensions – are typically dominated by complex digital technologies and associated software. Clearly, no one would be talking about cyber without the electrons. Yet, an equally important factor in the security equation is arguably the human element: the full range of many different cyber actors, from acknowledged experts, technology innovators, outside service providers and enterprise protection team members, to IT managers, system administrators, and, finally, ordinary users. Understanding that this human element can be the weakness or the strength in enterprise cybersecurity, and investing wisely in this element, are both essential to cyber readiness.

Such an approach should include: appropriate education and training at all levels of every organization; well-conceived strategies for targeting relevant behaviors to be encouraged or discouraged; and the development and deployment of user-friendly security tools tailored to cyber actors' respective roles. Gaming is a promising tool for improving cybersecurity, whether through use as a training aid for basic skills, an enhancement to cyber exercises, or a means to raise executive awareness about maritime cyber threats, plausible disruption scenarios, and associated risks.

Cyber-Physical Convergence

Today's maritime threat landscape includes a convergence of traditional physical threats with more recently emerging cyber threats that can play out together in a wide range of different scenarios. While potent security threats can certainly still play out entirely within either a physical or a cyber "silo," instances of cyber-physical convergence have definitely introduced new complexities to the maritime security equation.

Notional convergence examples include:

1. Cyber attacks intended to steal intellectual property or hold information or operational technology systems for ransom being facilitated by exploiting physical security vulnerabilities (e.g., defeating perimeter access controls to install a key logger for obtaining network administrative passwords);

2. Piracy, sabotage, cargo thefts or other unlawful physical acts being facilitated by cyber techniques (e.g., a network security breach to disable security cameras or manipulate cargo data); and

3. Cyber tools being used to highjack industrial control systems to directly cause harmful and/or damaging physical effects (e.g., taking ship's service and emergency generators off line while a vessel is transiting a treacherous waterway).

Unfortunately, within maritime enterprises, emerging cyber-specific preparedness and response efforts have too often been confined to the technical spaces, and too few of those in traditional physical security roles ever visited those enterprise spaces – and the converse has too often also been the case. When called upon to address enterprise security problems involving both physical and cyber dimensions, experts from these respective silos have tended to offer varied and at times parochial solutions. Given the significant implications of cyber-physical convergence all across the threat spectrum, this dynamic clearly needs to change at the enterprise level, both ashore and afloat. Today, maritime security programs should be planned, implemented, and integrated by teams of qualified professionals with expertise in both cyber and physical security.

Preparedness and Response

Above the enterprise level, here in the United States and in many countries around the world, there are established mechanisms, typically including significant public-private partnerships, for preparing for and responding to a wide array of major maritime contingencies. Examples include hurricanes, vessels sinking at sea, offshore facility pollution incidents, regional grid failures, and terrorist attacks on port areas. Planning for such contingencies has always been a daunting undertaking, but over the past several decades that process has been further complicated by the introduction of cyber dimensions.

Particularly in complex and expansive modern port environments, it is critically important that the legacy universe of maritime first responders, emergency managers, industry players and many other recognized stakeholders, on the one hand, and the appropriate cyber actors in the public and private sectors, on the other hand, are introduced to one other in the mix of ongoing preparedness efforts and actual response activities. This is obviously best accomplished in advance of any

significant real-world contingency through regular and well-conceived table-tops and field exercises that afford all MTS stakeholders a meaningful sense of the likely security challenges a future complex crisis may entail.

Two key questions in this context are: (1) how all of the relevant actors can be effectively integrated with each other, particularly in the planning, information sharing, exercise, and decision-making functions; and (2) whether the current coordination / collaboration mechanisms (or structures) are optimal in both the preparedness and the response / recovery phases.

From a strictly cyber perspective, this process of integration should also include initiatives focused on those personnel who operate primarily in the cyber domain on behalf of various different interconnected stakeholders in the customer and supply chains, yet who have not previously interacted with each other to any significant extent. For example, in light of their routine voluminous data exchanges, cyber teams for major vessel carriers should engage and coordinate security measures with their counterparts at freight forwarding companies that regularly use their carrier. Such exchanges, coupled with the steady growth in connections and integrated external sensors in corporate networks everywhere, dramatically increase the number of cyber attack surfaces that major vessel carriers must defend. Another example crosses the public-private sector divide. Should cyber actors working for government entities be prepared to share more of their sensitive cyber intelligence information with maritime industry counterparts than they are currently, either on a routine ongoing basis or at least in major contingencies that involve significant cyber dimensions?

RESEARCH QUESTIONS

The other goal set for the wrap-up session was to cull out the most significant research questions that emerged during symposium discussions. The eight questions set forth below provide an overview and synthesis of the specific research topics recommended by participants at the close of the symposium. All of the possibilities involve policy and process dimensions, while several also include a systems engineering and/or technology focus.

1. **C-Suite Leadership:** Participants frequently referred to C-suite responsibility to manage cyber risk. With the objective in mind to assist executives in challenging and complex decision-making, it is important to: formulate a methodology to evaluate and characterize the cyber awareness and related decision-making of effective C-suite teams; develop tools to address the identified gaps and weaknesses of these teams; and share best practices in cyber decision-making. As part of this research effort, how can the potential consequences of credible cyber risks be captured and conveyed in ways that ultimately prove informative – and compelling – at the C-suite (and boardroom) level?

2. **Internal Organization for Cyber:** What are the leading staff structure models for maritime entities to consider with respect to the assignment of policy and operational decision-making responsibility for cyber-specific matters? Given government and corporate sector lessons learned over the past several decades, is there an optimal approach to taking due account of the relationships and overlaps between the cyber and other functional areas? Such an

approach would presumably encompass, but not necessarily be limited to, operations, finance, information and operational technology, knowledge management, physical security, strategic planning, risk management, and business continuity.

3. **Modeling Risk and Measuring Resilience:** How should the government and private sector operators, respectively, evaluate cyber security? Risk management has been the traditional approach to understanding a broad range of risks and informing business process decisions. Resilience is now an increasingly-used concept and reference point to better understand certain risks, both natural and man-made. What is the standard cybersecurity terminology for ensuring that the many cyber actors clearly understand one another when discussing this complex and dynamic domain? Moreover, given that there are various assessment models and algorithms for different categories of risk in wide use, how does cyber fit into these existing frameworks (or vice-versa)? Finally, can certain risk indices be validated and/or new ones developed to evaluate whether actions intended to increase resilience, including cyber resilience, are actually doing so?

4. **Certifications:** Assuming that appropriate certifications are a useful approach to enhancing maritime cybersecurity, what specific criteria define the value added of such certifications? Moreover, what assets, facilities, operations and/or personnel should be certified? For example, should vessels be certified as "cyber-ready for sea" and port facilities as "cyber-ready for cargo operations"? Should there also be certifications for IT equipment providers and cybersecurity services? Who should develop and issue such certifications? And, finally, what professional standards should be applied, and what mechanism would ensure those standards remain current?

5. **Implications of Technology:** What are the maritime cybersecurity implications, both in the near term and also into the foreseeable future, of emerging new technologies, such as autonomous vessels, quantum computing, blockchain, and artificial intelligence? Are there related maritime policy decisions that should be contemplated now in anticipation of the projected impacts of these technologies?

6. **GPS Vulnerability:** U.S. maritime infrastructure (as part of the Transportation Systems Sector) as well as 10 of the other 15 critical infrastructure sectors are all dependent on the Global Positioning System (GPS) – a vulnerable system for which there is no current back-up, even though there are proven alternatives available. Why has the United States not resolved this critical issue? Assuming there is a compelling reason to provide redundancy by implementing a back-up system for generating precise electronic timing and location signals, what system or systems would align best with maritime-specific requirements, both afloat and ashore?

7. **Training and Education:** What innovative approaches could be used to improve existing and/or introduce new cyber-specific educational and training opportunities? There is a significant need to enhance maritime cybersecurity by providing all current cyber actors with the competencies they need and also to grow a capable workforce with the skillsets to tackle future cyber threats.

8. **Timeline for Research Impacts:** In view of the typical years-long research cycle – from commissioning research efforts to actually seeing real-world changes based on that research – are there ways to expedite and/or redesign the research process to reflect the lightning pace of both technology change and the evolution of threats in the cybersecurity arena?

FURTHER THOUGHTS ON THE WAY AHEAD

Reflecting back on the key themes and research questions gleaned from the symposium, the authors would offer a number of further thoughts on maritime (principally, MTS-related) cybersecurity that may warrant consideration going forward.

The Challenge

Any human endeavor should involve a clear understanding of the goal, as well as the nature and scope of the activities intended to achieve that goal. In grappling with the essence of the cybersecurity endeavor, it is worthwhile to note that what was known early on as information technology is now described as "cyber systems," and that prior references to security software and firewalls have long since given way to the much broader "cybersecurity."

Today's cybersecurity challenge actually had its genesis decades ago when the internet was invented, designed and constructed.[6] This revolutionary advance in information transfer technology was designed to transmit and provide access to large volumes of digitized information swiftly and reliably all across the globe. Throughout this history, an internal battle within the internet realm has pitted wide and open access to information against control over or restrictions on dissemination of all or certain subsets of information. Moreover, the internet was definitely not designed for security (or even regulation), and that design characteristic has been increasingly exploited by a wide range of cyber actors for unlawful or other nefarious purposes.[7]

Not long ago, "information security" meant keeping "secret information" secure within electronic communications and protecting networks with password changes and remote drive restrictions. Today, these remain valid imperatives, and many would assert that they have not been adequately adhered to. Yet the scope of what is now known as "cybersecurity" has since expanded significantly to encompass securing Wi-Fi, Bluetooth and Cloud communications; protecting industrial control systems; and preventing exploitation of the internet of things. As cyber attacks continue to increase dramatically despite the billions of dollars allocated to defensive measures, is it time to ask if society has failed to grasp the critical essence of the cybersecurity challenge?[8]

Today, there are more and more remote-controlled and autonomous machines, with "no hands aboard" merchant ships looming on the near-term horizon.[9] And the cyber threat implications of applied machine learning, artificial intelligence, and quantum computing are just beginning to come into focus. Particularly if, before long, information availability and transparency come to

[6] Gil Press, "A Very Short History of the Internet and the Web," *Forbes*, January 2, 2015, 1.

[7] Craig Timberg, *The Threatened Net: How the Web Became a Perilous Place* (Washington, DC: Washington Post, 2015), chap. 1, Diversion Books.

[8] Daniel M. Gerstein, "Putting the Security into Cybersecurity," *The National Interest*, September 30, 2017, 2.

[9] Jalal, Bouhdada, "Maritime Cybersecurity: Securing Assets at Sea," *Security Week News*, May 1, 2018.

mean "direct human brain to machine interface," can society possibly be ready for that development with yesterday's and today's thinking?

Clearly, traditional tools such as vulnerability assessments, threat identification, perimeter defenses, continuous diagnostics and monitoring, etc. will retain their role in bolstering cybersecurity for the foreseeable future. But if society doesn't make the "leap ahead" in security represented by more of a focus directly on internet functionality, if certain aspects of "availability and transparency" continue to be regarded as negatives when they are indispensable elements of success in realizing the full potential of the internet and now cloud information, how will a successful cybersecurity strategy ever be formulated? This fundamental question is squarely in the wheelhouse of research institutions, yet the current priority accorded the work underway in this context appears inadequate. To squarely address the cybersecurity challenge, that should change.

Set forth below are three alternative approaches to framing aspects of that challenge in ways that could ultimately contribute to superior solutions:

1. The first example relates to the manner in which threats originate in one node and then travel the "internet commons" to one or more other often geographically distant nodes. Today, cyber systems operate in a virtual free-for-all environment. Should national policies mandate a more proactive and supportive role for the government entities engaged in this domain? Is there an innovative international governance and enforcement regime for the internet that has the potential to assure universal and peaceful uses of digital information without compromising the privacy of digital packet content? If threats are countered more effectively out in cyberspace, can global cybersecurity be significantly enhanced? Are those researchers currently exploring the applicability of such well-established international legal principles as those embodied in the law of armed conflict and the law of the sea on the right course towards a major contribution to the ultimate solution?[10]

2. Another example relates to the expanding use of the internet. Does the global trend towards having more than 30 billion smart devices connected to the internet by 2020[11] reflect wise public policy? If not, is the trend essentially irreversible, or is there an advantageous alternative paradigm for using connected devices that would take the inherent tension in seeking 100% security with an open and transparent system fully into account?

3. A third example focuses on the question of whether the internet should be a "one infrastructure backbone fits all" proposition. Perhaps global society should opt for a transition to "multiple internets," with security regimes carefully tailored to the unique purpose of all such follow-on versions as a top-tier design requirement. Alternative regimes would presumably be differentiated in part by their respective tradeoffs between and among such design criteria as cyber

[10] North Atlantic Treaty Organization, Cooperative Cyber Defence Centre of Excellence, International Group of Experts, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge, United Kingdom: Cambridge University Press, 2017), 1-7.

[11] Statista, "Internet of Things (IoT) Connected Devices Installed Base Worldwide From 2015 to 2025" (Hamburg, Germany: Stroer Contact Group GmbH, 2018), chart, available at *https://www.statista.com.*

infrastructure security, information accessibility, process transparency, and end-user privacy interests.[12]

The U.S. Department of Commerce National Institute of Standards and Technology (NIST) has made significant contributions to cybersecurity over the past several decades through the development of well-respected guidelines and best practices that focus primarily on how to secure cyber nodes that link to the internet.[13] Numerous other governmental entities and academic institutions here in this country and abroad have also made similar noteworthy contributions. Perhaps the time has come for these pioneering organizations to refocus more of their efforts toward the pursuit of innovative new concepts with the potential to deliver more effective and efficient cybersecurity solutions.

Terms of Reference

In today's MTS cyber realm, the practical day-to-day goal involves striving to achieve acceptably-managed risk. Going further to define "maritime cybersecurity" is fundamentally a two-step process. The logical initial focus is the word "cybersecurity," followed by consideration of the simpler qualifier "maritime."

Unfortunately, there is no reasonably consistent common understanding in general terms of what cybersecurity is all about. Granted, most of the various extant working definitions of "cybersecurity" generally parallel, or at least draw key elements from, the following NIST formulation:

> *[P]revention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.*[14]

Yet, there appears to be no widely-accepted definition of the term that adequately reflects the inherent contradiction in cybersecurity: the tension between universal access and the increasing need for digital vigilance. The absence of such a definition arguably hinders communications among experts and impedes their cooperative development of superior cybersecurity solutions.[15]

Consideration of the qualifier "maritime" introduces even more uncertainty based on scope. The maritime sector is anything but a homogenous set of cyber actors with the same information technology and network systems that perform the same functions, face the same threats, and entail the same risks. And with respect to considering the "cybersecurity" subset associated with the maritime realm, does "maritime cybersecurity" stop at the water's edge (or the port terminal's

[12] Nicole Perlroth, "Reinventing the Internet To Make It Safer," *New York Times*, December 3, 2014, F7.

[13] U.S. Department of Commerce, National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1* (Washington, DC, 2018), iv-vi.

[14] U.S. Department of Commerce, National Institute of Standards and Technology, Computer Security Resource Center, Definition of "Cybersecurity" (Washington, DC: 2018), https://csrc.nist.gov/Glossary.

[15] Robert K. Ackerman, "Creating a Common Language of Cybersecurity," *Signal* (Official Publication of the Armed Forces Communications and Electronics Association), August 2017, 21-22.

gate), or does it extend all the way inland to the distant cargo shippers and the MTS supply chain providers?

With so much uncertainty about the nature and scope of "maritime cybersecurity," how should the maritime realm organize itself to optimize its efforts to achieve any reasonable level of managed risk? To recap the context for this challenge, the maritime subset of the cyber domain is complex, fragmented, dynamic, and fraught with uncertainty, populated by myriad cyber and other relevant actors with different roles, knowledge, resources, and motivations.

In this context, it is often exceedingly difficult for individual public or private sector cyber actors, especially those with formal security responsibilities, to decide how best to proceed. Meaningful answers to the important questions set forth below appear essential to tangible further progress in enhancing maritime cybersecurity.

1. Which actors should provide what components of comprehensive cybersecurity?;

2. In practical terms, and ideally informed by a robust enterprise risk management process, how much cybersecurity should any given private sector actor seek to buy?;

3. How should the public sector seek to improve its ongoing efforts to support private sector maritime cybersecurity efforts?;

4. What assurance is there that today's security capabilities will address tomorrow's rapidly evolving threats?;

5. Who pays or is otherwise liable when there are significant MTS cybersecurity failures?; and

6. How should the many inescapable international aspects of the maritime cybersecurity challenge be reflected in proposed initiatives and follow-on solutions?

National Strategy

Relevant national strategy is appropriately considered (and developed) in a hierarchical framework defined by specific topics and their often complex interrelationships. In this context, the initial focus is overarching national security strategy ideally intended to address all significant security threats across the full spectrum. The current *National Security Strategy* issued in December 2017 does reflect the importance of cybersecurity in countering threats in all operational domains, yet – consistent with recent past precedent – does not address cybersecurity to any significant extent.[16]

Below the apex of the hierarchy, there are at least two relevant national strategy tracks: "cyber" and "maritime." At least conceptually, there should be: (1) a cybersecurity subset of national security strategy that specifically addresses any unique maritime aspects of cybersecurity; (2) conversely, a maritime subset of national security strategy that specifically addresses any unique cyber aspects of the maritime realm; and (3) consistency wherever there is substantive overlap between the two tracks.

[16] Executive Office of the President, *National Security Strategy of the United States of America* (Washington, DC: 2017), 12-13.

Turning first to the maritime track, in the immediate aftermath of 9/11, in addition to the imperative of securing commercial aviation, there was also broad recognition in Washington that one of the priority tasks was addressing the MTS as a potential terror attack vector. The initial outcome was the comprehensive Maritime Transportation Security Act (MTSA) in 2002 that mandated a wide range of security measures by certain government agencies and industry players.[17] The next significant development in this context was the issuance by the Bush Administration in September 2005 of the first-ever comprehensive *National Strategy for Maritime Security*.[18]

Reflecting a heightened appreciation of both the critical importance and the extreme vulnerability of the maritime sector, the new strategy drew on the extensive experience of the U.S. Coast Guard, many other Federal, State, Local, Tribal and Territorial law enforcement agencies, and hundreds of maritime industry actors in implementing MTSA requirements. Subsequently adopted by the Obama Administration and presumptively still in effect under the Trump Administration, the strategy is generally regarded as having facilitated substantial progress in securing the maritime realm against terrorist threats.[19]

Now, more than a dozen years later, that strategy does not begin to address the many ways in which today's realities have dramatically transformed the maritime threat landscape.[20] Cybersecurity is certainly one, but not the only, major impetus for revising this dated strategy. The resurgence of great power conflict, climate changes (especially in the Arctic), and the even greater reliance of the U.S. economy on the maritime transportation-enabled "just-in-time" global supply chain all clearly stand out among the many other factors. It is also imperative, however, that cyber dimensions be integrated throughout an updated maritime security strategy.

Shifting to the cyber track, the first key directive issued by the current Administration was Executive Order 13800 entitled *"*Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*"* released in May 2017.[21] While the executive order does not address any of the unique aspects of the maritime cyber domain, the directive is a strong policy statement that calls for all senior executive branch officials to use their relevant authorities and capabilities to "support the cybersecurity risk management efforts of the owners and operators of the Nation's critical infrastructure."[22]

Drawing on the experience gleaned from implementing Executive Order 13800, the Administration just recently published its *National Cyber Strategy* in September 2018.[23] The *Strategy* is built on four pillars, the first of which addresses securing all critical infrastructure, including transportation. Worthy of note in this context is the particularly strong emphasis on maritime cybersecurity as reflected in the excerpt below.

---

[17] Maritime Transportation Security Act, Pub. L. 107-295 (2002).

[18] Executive Office of the President, *National Strategy for Maritime Security* (Washington, DC: 2005).

[19] U.S. Government Accountability Office, *Maritime Security: National Strategy and Supporting Plans Were Generally Well-Developed and Are Being Implemented* (GAO-08-672) (Washington, DC: 2008), 1-5.

[20] Executive Office of the President, *National Strategy for Maritime Security*, 1-6.

[21] "Executive Order 13800 of May 11, 2017, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," *Code of Federal Regulations*, no. 2017-10004: 22391-22397.

[22] Ibid, 3.

[23] Executive Office of the President, *National Cyber Strategy* (Washington, DC: 2018).

> *Given the criticality of maritime transportation to the United States and the global economy and the minimal risk-reduction investments to protect against cyber exploitation made thus far, the United States will move quickly to clarify maritime cybersecurity roles and responsibilities; promote enhanced mechanisms for international coordination and information sharing; and accelerate the development of next-generation cyber-resilient maritime infrastructure.*[24]

At the departmental level, the Department of Homeland Security published its current *Cybersecurity Strategy* in May 2018.[25] The comprehensive strategy, which is primarily centered on mitigating systemic risk and strengthening collective defense, does focus extensively on critical infrastructure, but has essentially no maritime-specific content.

At the maritime agency level, the Coast Guard published its *Cyber Strategy* back in June 2015.[26] The document outlines three primary lines of effort: (1) defend Coast Guard cyberspace in collaboration with the Departments of Defense and Homeland Security; (2) enable Coast Guard operations through cyber capabilities; and (3) protect MTS critical infrastructure, primarily by using Coast Guard authorities and partnerships to promote maritime industry cyber readiness.

While the Coast Guard document is a significant positive development, it is more of a work plan than a fully comprehensive strategy in the traditional sense (especially in its treatment of MTS cybersecurity). Moreover, the document is too narrow in scope to serve as a stand-alone national maritime cybersecurity strategy. The superior approach in any case would be to develop a new 2.0 national maritime security strategy that appropriately integrates cyber dimensions and is fully consistent with extant cyber-specific national security guidance. A key element in developing a 2.0 approach should be the assignment of clear roles and missions to the various government agencies that have authorities and expertise of significance relevance to maritime cyberspace.

Cyber Readiness

Below the strategic level, a host of public and private actors operate in myriad roles all along the waterfront and out at sea. It is difficult to envision, let alone contemplate achieving and maintaining, a cyber-ready MTS without the strong shared commitment of all these actors to support prevention, response, and recovery efforts in their respective operational roles. Attaining this strong shared commitment is essential to achieving "cyber readiness," which may differ in nature and scope for each reasonably foreseeable disruptive event.

The Congress and successive Administrations have charged the many public actors within the federal sphere to improve their individual agency readiness, enhance interagency cooperation, and

[24] Ibid, 8-10.
[25] U.S. Department of Homeland Security, *Cybersecurity Strategy* (Washington, DC: 2018), 11-14.
[26] U.S. Coast Guard, *Cyber Strategy* (Washington, DC: 2015), 9-10.

collaborate more closely with the private sector, to include information sharing.[27] Yet, as highlighted by MRS 2017 participants, an important question is how well U.S. government

entities – particularly, the Departments of Homeland Security, Justice and Defense, and the Coast Guard and Federal Bureau of Investigation (FBI) at the agency level – together with the various relevant public-sector coordination and collaboration mechanisms at all levels, have adapted to the emergence of serious cyber threats to maritime security.

The Coast Guard is the lead federal maritime security agency and the principal orchestrator of relevant maritime public-private partnerships.[28] Another key question in this context is to what extent has the Coast Guard been able to bring its impressive legacy array of authorities, expertise, resources and relationships for full-spectrum maritime security specifically to bear on the cyber readiness challenge?

The Coast Guard has a dedicated Cyber Command, stood up in 2013 as a service component of the joint Department of Defense U.S. Cyber Command.[29] This unit spearheads implementation of the Coast Guard's *Cyber Strategy*, working closely with NCCIC, FBI, the Intelligence Community, and other key interagency cyber and maritime players. Cyber Command serves as a key enabler for all Coast Guard missions, primarily through its operation and defense of the service-wide enterprise platform, shared cyber intelligence, reports of cyber incidents, support for the response to and recovery from serious incidents, and promotion of greater maritime industry cyber awareness.

In addition, the Coast Guard has been partnering with the NIST National Cybersecurity Center of Excellence (NCCoE), as well as significant industry stakeholders and trade associations, to develop sector risk profiles to assist specific segments of the marine industry in implementing the NIST *Framework*.[30] Sector risk profiles released to date include: Maritime Bulk Liquids Transfer (2016); Offshore Operations of Oil and Natural Gas Industry (2018); and Passenger Vessel Industries (2018). Work on a fourth profile relating to navigation and automated systems onboard vessels and facilities is currently underway.

Specifically with respect to at-sea cybersecurity, the Coast Guard has emphasized working through the International Maritime Organization (IMO) to develop appropriate guidelines.[31] The

---

[27] Kate Charlet, "Understanding Federal Cybersecurity," Harvard University, Kennedy School, Belfer Center for Science and International Affairs (Boston, MA: 2018), 7-9, 19-34.

[28] U.S. Government Accountability Office, *Coast Guard: Actions Needed to Enhance Performance Information Transparency and Monitoring* (GAO-18-13), (Washington, DC: 2017), 1-2.

[29] David Thompson, "Coast Guard Cyber Command 'Just As Important As Cutters and Aircraft'" (Interview of RADM Kevin Lunday, USCG), *Federal News Radio*, December 8, 2017, https://federalnewsradio.com/dhs-15th-anniversary/2017/12/coast-guard-cyber-command-just-as-important-as-cutters-and-aircraft/; J.R. Wilson, "CGCYBER and Coast Guard Cybersecurity," Defense Media Network, March 14, 2018, https://www.defensemedianetwork.com/stories/coast-guard-cybersecurity/.

[30] Amy Midgett, "Release of Offshore Operations and Passenger Vessel Cybersecurity Framework Profiles," *Coast Guard Maritime Commons* (blog), January 12, 2018, http://mariners.coastguard.dodlive.mil/2018/01/12/1-12-2018-release-of-offshore-operations-and-passenger-vessel-cybersecurity-framework-profiles/.

[31] Kevin Kuhn, "Cyber Risk Management in the Maritime Transportation System," *Homeland Security Today.US*, February 9, 2018, https://www.hstoday.us/channels/us-coast-guard/cyber-risk-management-maritime-transportation-system/.

Coast Guard approach reflects not only the inherent international character of ocean shipping and many offshore operations, but also the abundant opportunities for inbound vessels to convey threats directly into the national MTS. This reality clearly calls for implementation of a globally consistent approach. The most significant at-sea outcome to date was the publication in July 2017 of the IMO "Guidelines on Maritime Cyber Risk Management" – a resource for the international maritime community that tracks generally with the initial version of the NIST *Framework*.[32]

Shifting ashore, every Coast Guard sub-regional command throughout the country has an Area Maritime Security Committee (AMSC) that serves as a collaborative forum for government and industry partners to coordinate and integrate their efforts to enhance port-level security.[33] Most of the AMSCs have set up cyber sub-committees that promote ongoing collaboration, serve as information-sharing mechanisms, and host periodic table-tops and exercises. However, another important question in this context is whether the Coast Guard AMSCs are the optimal forum, particularly in terms of structure, capacity and expertise, to spearhead port-level efforts – let alone those of other maritime industry players – to enhance maritime cybersecurity?

For its part, the FBI has lead federal responsibility for the investigative response to all significant cyber incidents (particularly those involving terrorism, theft of trade secrets, or foreign intelligence activity).[34] To carry out this role, the FBI has developed significant cyber expertise, educated itself on private sector use of information technology, and established Cyber Task Forces all across the country that include a maritime focus where appropriate. In fact, many maritime industry actors are more likely to turn to the FBI than the Coast Guard with respect to cybersecurity issues.

Two of the many other federal entities with a maritime cybersecurity role are worthy of particular note. Within DHS, Customs and Border Protection (CBP) has lead responsibility to protect its Automated Commercial Environment (ACE) system, which is vital to the smooth and uninterrupted flow of maritime commerce.[35] Shipping entities use this data interface to report all imports and exports, and CBP and numerous other government agencies use this system for regulatory and fiscal purposes, including clearing cargoes and levying customs tariffs. The other entity is United States Cyber Command.[36] Given its recent elevation to combatant command status, coupled with the guidance in the just-released *National Cyber Strategy*,[37] it is expected

[32] International Maritime Organization, "Guidelines on Maritime Cyber Risk Management" (MSC-FAL.1/Circ. 3), (London, United Kingdom: 2017), 1-3.

[33] U.S. Coast Guard, *Area Maritime Security Committees: Challenges, Accomplishments and Best Practices – 2016 Annual Report* (Washington, DC: 2017), 1-7.

[34] U.S. Congress, Scott S. Smith Statement for the Record of the Senate Armed Services Committee, "Roles and Responsibilities for Defending the Nation from Cyber Attack," 115th Cong. 1st sess., October 19, 2017 (Washington, DC: 2017), 1-7.

[35] U.S. Customs and Border Protection, "Automated Commercial Environment and Automated Systems" (Washington, DC: 2018), https://www.cbp.gov/trade/automated.

[36] U.S. Cyber Command, *Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command* (Fort Meade, MD: 2018), 7-9.

[37] Executive Office of the President, *National Cyber Strategy*, 20-24.

that this military organization will begin playing a more proactive role in protecting domestic maritime (and all other) critical infrastructure, both in the public and private sectors.

All that said, are the many relevant agencies and associated interagency mechanisms for coordinating the response to cybersecurity threats up to the task of handling what probably lurks on the near-term horizon? Is there the necessary emphasis on shared commitment by public sector entities? Are the roles and missions reflecting their shared commitment clear to the non-federal stakeholders? Not only is the ongoing trend towards increased cyber-only attacks almost certain to continue, but more sophisticated and destructive cyber-physical attacks in port areas that require rapid response decisions across government are readily foreseeable.[38]

As one cyber readiness example, is the "all-purpose" *National Cyber Incident Response Plan* (NCIRP) developed pursuant to Presidential Policy Directive 41[39] able to draw on sufficient organic sector-specific expertise to optimize the response to a major maritime cybersecurity incident? Is the existing Maritime Operational Threat Response (MOTR) process[40] – originally stood up to facilitate interagency coordination in maritime cases involving potential kinetic threats – capable of assuming a support role with respect to cyber incidents with maritime dimensions? Or is Coast Guard Cyber Command or some other sector-specific mechanism in place to support the NCIRP in critical maritime cyber cases?

Current realities on the waterfront are such that, for now (and probably well into the foreseeable future), private sector and operating maritime enterprises will be the center of gravity for achieving cyber readiness. They need to continue striving to secure their respective networks by the best available means – a daunting task, especially as the proliferation of mobile devices and cloud services is rendering their legacy "castles and moats" increasingly irrelevant.[41] C-suites, boards and senior managers need to: make cyber a high priority; insist on measures to establish an organizational culture of cyber awareness and responsibility; and allocate the resources necessary to implement an appropriately comprehensive program that integrates the right defensive technologies with the best cybersecurity practices. While even optimized programs will not assure 100% security, they will almost certainly deliver continued improvements, particularly given that the preponderance of today's cyber incidents are still linked to inside actors, even while external vectors pose increasingly serious threats.[42]

Thus, the operational roles at the individual actor level must continue to receive priority focus. The question that remains is how that individual actor commitment is instilled and then

[38] U.S. Department of Homeland Security, "Consequences to Seaport Operations from Malicious Cyber Activity" (Washington, DC: 2016), 1-17.

[39] Executive Office of the President, Presidential Policy Directive 41 of July 26, 2016, *United States Cyber Incident Coordination* (Washington, DC: 2016), 1.

[40] U.S. Department of Homeland Security, "Global MOTR Coordination Center (GMCC)" (Washington, DC: 2011), 1, https://www.dhs.gov/global-motr-coordination-center-gmcc.

[41] Charlie Gero, "Moving Beyond Perimeter Security: A Comprehensive and Achievable Guide to Less Risk" (Cambridge, MA: Akamai Technologies Enterprise and Advanced Projects Group, 2018), 1-4, https://www.bankinfosecurity.com/whitepapers/moving-beyond-perimeter-security-comprehensive-achievable-guide-to-w-4425.

[42] Richard Hummel, "Securing Against the Most Common Vectors of Cyber Attack" (North Bethesda, MD: SANS Institute), 2017, 5.

integrated – within and across diverse maritime enterprises – to support shared and overall readiness. On the private-sector side, there remain many impediments to actors forming a shared commitment. Yet private sector-specific information sharing mechanisms in certain sectors – most notably, financial services – are functioning effectively within the DHS National Cybersecurity and Communications Integration Center (NCCIC).[43] The sectors represented within the NCCIC saw value in shared information and analysis, as well as the subsequent expedited coordination with the federal government for response purposes. The maritime sector, however, has not adopted a similar approach for various reasons that are not fully clear.

These and other similar issues warrant careful review and analysis as the Coast Guard, together with its many public and private sector partners, continues to implement its *Cyber Strategy* and improve overall MTS cyber readiness.

Third Pillar of Coast Guard Strategy

In addressing the third pillar of its *Cyber Strategy* – protecting MTS critical infrastructure – the Coast Guard published draft Navigation and Vessel Inspection Circular (NVIC) 05-17 on maritime cybersecurity in July 2017 and sought comments from the maritime public.[44] The draft NVIC sets out the expectation that MTSA Part 105 facilities assess cyber vulnerabilities within the structure of their existing Facility Security Plans (FSPs). Enclosure (1) of the NVIC walks through the standard FSP and how cyber vulnerabilities should be incorporated. Enclosure (2) follows NIST guidelines for establishing appropriate governance to address the vulnerabilities. The comment period closed in October 2017, and the final version has not yet been promulgated.

The draft NVIC appears to raise the importance of the NIST guidelines for maritime facilities and "expects" them to be used in developing FSPs. However, the document specifically "does not impose legally binding requirements" and captures the Coast Guard's "current thinking." Such an approach may create an unnecessary degree of ambiguity while not improving the level of cybersecurity: ambiguity because FSPs are legally required, and without improvement because the NIST guidelines are already available to industry. Assuming the Coast Guard has not identified with particularity a cybersecurity construct that can be validated as improving risk management, the better overall alternative for now may be seeking to advance cybersecurity incrementally.

There are many incremental targets for the Coast Guard to consider in pursuit of its strategy to protect MTS critical infrastructure, a number of which were highlighted during MRS 2017 discussions. Among the most promising options are: (1) further develop the risk management model for maritime cybersecurity; and (2) continue to build on current AMSC activity to improve expertise and training related to facility cybersecurity efforts.

With respect to risk management, the Coast Guard could provide helpful direction related to various key questions. What risk management model(s) does the Coast Guard endorse for use by

[43] *Homeland Security News Wire* (Mineola, NY), "Improving Critical Sectors' Cybersecurity by Bolstering Sharing, Acting on Information," December 4, 2017.

[44] U.S. Coast Guard, Draft Navigation and Vessel Inspection Circular No. 05-17: "Guidelines for Addressing Cyber Risks at Maritime Transportation Act (MTSA) Regulated Facilities" (Washington, DC: 2017), *1-2*.

the maritime community? Is there a current Coast Guard estimate of cyber-specific port vulnerability comparable to estimates that have historically preceded facility assessments? Against what threats should facilities evaluate risk? And is the intended Coast Guard focus limited to the MTS, or does it extend more broadly to certain other cyber aspects with a significant MTS nexus?

The second incremental improvement option involves continuing to do more to leverage the AMSCs. As discussed above, the Coast Guard has already begun efforts to establish AMSC "roundtables" for port partners to enhance their awareness of cybersecurity challenges, best practices, and available resources. Yet, there is no applicable standard for AMSC cyber subcommittees, for appropriate involvement of cyber experts, or for common incident terminology and process as pertaining to cyber response. Enhancing cybersecurity resilience is widely recognized as an important priority for ports and facilities, and the Coast Guard is well-postured to play an even more significant role in advancing this cause.

Enterprise Risk Management

Full-spectrum Enterprise Risk Management (ERM) is an approach widely-used in both the public and private sector for developing comprehensive assessments of risks and opportunities.[45] It is an organizational tool for executive decision-making. It is also a tool for stakeholders, particularly in publicly-traded businesses, to evaluate others' business decision-making. The fundamental approach is to systematically evaluate singular threats and opportunities against others, recognizing that decision-makers need to identify priorities among their respective threats and opportunities.

Over the past several decades, the development of cyber technology has presented businesses with many opportunities to make better decisions and also review decisions more effectively. Fortunately, ERM can be used by businesses to inform decisions regarding the continued development and use of cyber technology, as well as the implementation of appropriate cyber safeguards. ERM can also be used by oversight authorities to assess policy and regulatory options that are of public interest.

Key questions at this juncture include the extent to which ERM is the "right" tool for businesses seeking to address cybersecurity challenges. And are there public interests at stake that call for some measure of transparency in such ERM use by private sector entities? How can ERM be optimized for these cyber purposes? Finally, can ERM contribute to realizing the Coast Guard's stated objective in its draft NVIC?

Information and Analysis Sharing Organizations (ISAOs)

Cyber systems and cybersecurity entail new and unique challenges for public and private sector managers. Many urge that an important way to address these challenges is to share information among cyber managers so that information can be analyzed to update and improve cybersecurity measures. The most significant development in this context was arguably the recent establishment of the Information Sharing and Analysis Organization – Standards Organization

[45] New York University, "Understanding Enterprise Risk Management: An Overview" (New York, NY: 2016), 3-18, https://www.nyu.edu/content/dam/nyu/financialOperationsTreas/documents/Resources/erm.

(ISAO-SO).[46] Chartered and funded by the Department of Homeland Security, this initiative was undertaken pursuant to Executive Order 13691, "Promoting Private Sector Cybersecurity Information Sharing" issued in February 2015. The purpose of ISAO-SO is to support relevant communities of interest in forming information sharing organizations and developing an effective ecosystem comprised of these public-private partnerships.

A sharing organization can take any form and at a very basic level reflects the key premise of the preexisting private sector Information Sharing and Analysis Centers (ISACs).[47] A number of cyber communities of interest have formed organizations to in part share information, and a necessary element in their formation is sufficient trust to support that sharing. A recurring question is whether the maritime community of interest has that necessary trust among potential stakeholders and is motivated to be effective in sharing cyber information.

The Maritime and Port Security Information Sharing and Analysis Organization (MPS-ISAO) stood up in late 2016 with the goal of enhancing cyber resilience throughout the industry by sharing threat information, best practices, and emerging technology.[48] Its ultimate success will be determined by the participation of stakeholders, their trust in each other and the organization, and the real world impact of the information disseminated.

The critical importance of trust in this context cannot be overstated, yet is only one of the qualities of a successful ISAO. Maritime (and other) critical infrastructure organizations that operate cyber systems and have information to share must address a number of important questions. Among them are what information is relevant, what relevant information is business sensitive, what information if shared may contribute to cyber solutions, and with whom and how should actionable information be shared? Some see resolving such questions as straightforward, whereas others find wrestling with the questions a significant disincentive to sharing information.

The first instinct for many cyber managers is to share every incident they discover that may be an attempt to intrude or corrupt. There is skepticism, however, as to whether such reports will lead to significant findings and whether proprietary information can be adequately protected. One possibility, not frequently discussed, would entail development of a cyber "black box" that would automatically and anonymously report cyber events for analysis by experts.

The public understands the importance of the maritime community to the economy and expects the community to work together in elevating the security posture of this sector. Congressional mandates alone will not work because trust cannot be legislated. Today there is useful information sharing within certain functional groups of the marine industry even if not widely recognized. Such groups that are sharing should consider the possibility of expanding their

[46] U.S. Department of Homeland Security, "Information Sharing and Analysis Organizations (ISAOs)" (Washington, DC: 2018), 1-2, https://www.dhs.gov/isao.

[47] National Council of ISACs (Information Sharing and Analysis Centers), "About ISACs" (Washington, DC: 2018), https://www.nationalisacs.org/media.

[48] Maritime and Port Security Information Sharing and Analysis Organization, Press Release: "The Maritime and Port Security ISAO Convenes Inaugural Cybersecurity Summit at NASA/Kennedy Space Center, February 22-24, 2017" (Beltsville, MD: 2017), PRWeb.com.

efforts, as well as adopting a more public platform sufficient to demonstrate the resolve of the community. For its part, DHS should ensure the ISAO-SO supports functional groups within sectors and the integration where appropriate of common cross-functional information sharing initiatives. Another worthwhile DHS target for improvement would be the effectiveness of its Automated Indicator Sharing (AIS) program for disseminating cyber threat intelligence directly to private sector entities.[49]

GPS Vulnerability

All across the planet – extending not only throughout the maritime realm, but all other operational domains – there is almost universal reliance on GPS.[50] Developed, deployed, and maintained by the United States, this satellite-based system continuously transmits signals with the precise time and location information that synchronizes and enables virtually all of modern society's functions. In today's new threat environment, however, this near-universal dependence is an increasing concern, both militarily and economically. Current GPS can be jammed, spoofed, and/or destroyed – and there is only very limited backup capability available.[51]

Here in this country, there are currently a number of initiatives underway intended either to harden or augment the existing GPS system, or to develop a redundant capability.[52] One option that has actually been implemented by various other countries on a regional basis employs on-the-shelf e-Loran navigation technology to provide effective and affordable, though less precise, redundant capability. Whether e-Loran, another redundancy option, or a combination of measures proves the best approach, it is vital to ensure that this vulnerability is addressed on an expedited basis.

Global Research Network

One of the primary goals of MRS 2017 was to stimulate research intended to advance maritime cybersecurity and also generate specific research questions for consideration. Here in the United States, there are a number of academic institutions engaged in maritime cybersecurity research, including American Military University, California Maritime Academy, Johns Hopkins University, Naval Postgraduate School, Rutgers University, University of San Diego, University of Southern California, and others. There is also significant academic research being conducted overseas at such leading institutions as Lancaster University and Plymouth University in the United Kingdom. Beyond the academic realm, there are also numerous government agencies, professional societies, trade organizations and corporate entities engaged in this work around the globe. Examples include the American Bureau of Shipping (ABS), the Baltic and International

[49] U.S. Department of Homeland Security, United States Computer Emergency Readiness Team (US-CERT), "Automated Indicator Sharing (AIS)" (Washington, DC: 2018), https://www.us-cert.gov/ais.

[50] Victor M. Mendez and Robert O Work, Department of Transportation and Department of Defense Letter of December 8, 2015 to the U.S. House of Representatives,"Importance of the Global Positioning System (GPS) and the Need for a Complementary Positioning, Navigation, and Timing (PNT) Capability for the Nation" (Washington, DC: 2015), 1-2, *https://rntfnd.org/wp*.

[51] Sarah Scoles, "Spoof, Jam, Destroy: Why We Need a Backup for GPS," *Science*, March 2, 2018, https://www.wired.com/story/spoof-jam-destroy-why-we-need-a-backup-for-gps/.

[52] Kym Gillhooly, "Defense Department Moves to Augment GPS with Alternatives," *FedTech Magazine*, May 11, 2018, https://fedtechmagazine.com/article/2018/05/defense-department-moves-augment-gps-alternatives.

Maritime Council (BIMCO), Bureau Veritas (BV), and the European Network and Information Security Agency (ENISA).

Given the fundamentally international nature of the maritime cybersecurity challenge, does it make sense to establish a global research network? Its fundamental purpose would be to stimulate, facilitate and, in certain instances, coordinate cybersecurity research efforts with a maritime focus. Such an initiative could provide an effective and efficient mechanism for informally discussing and sharing information on such topics as critical challenges, research questions, available and required subject matter expertise, potential sponsors, test venues, worthwhile research outcomes, etc. Following the example of other similar research initiatives, such as the Global Resilience Research Network recently established by Northeastern University's Global Resilience Institute,[53] such a network could be largely virtual and informal, perhaps featuring a single annual conference hosted by members on a rotating basis.

Were such an initiative to go forward, the network might seek consultative status with IMO, the specialized United Nations agency for maritime affairs. IMO is the preeminent international governmental body with respect to maritime international law, regulations and operating practices, and as noted earlier its Maritime Safety Committee has issued guidelines for maritime cyber risk management. If the research network achieved consultative status, future IMO deliberations would no doubt benefit from academic and other research expertise channeled through the network.

CONCLUSION

Maritime security (including cybersecurity) is a global "common good" – an extant condition from which virtually all human beings benefit, yet for which there is often no definitive and comprehensive arrangement to ensure that the condition is maintained.[54] Reviewing the many views and insights gleaned during MRS 2017 discussions, as well as further thoughts informed by those discussions, one overarching recommendation for enhancing maritime cybersecurity readily emerges.

The global cyber brain trust (and its many sponsors) need to invest the requisite funding and human capital to expedite exploration of new paradigms for cybersecurity.[55] These new paradigms should guide a shift in emphasis away from relying primarily on countless internet consumers to defend their fortified nodes largely on their own (particularly in the private sector) to a more holistic and better integrated strategy that seeks to secure and police internet pathways without unduly restricting information availability or jeopardizing legitimate privacy concerns.

Such paradigms will assuredly prove extraordinarily difficult to develop. Complicating factors include the incredible number and multi-faceted diversity of major stakeholders; the nature of

[53] Northeastern University, Global Resilience Institute, "Global Resilience Research Network" (Boston, MA: 2018), https://globalresilience.northeastern.edu/network/.

[54] Stanford Encyclopedia of Philosophy, "The Common Good" (Stanford, CA: 2018), https://plato.stanford.edu/entries/common-good/.

[55] Jonathan Rigby and David White, "A New Paradigm for Cybersecurity: Moving from Protecting Perimeters to a Holistic System for Enterprise-Wide Information Protection," *Corporate Counsel Business Journal*, 22-39, January 5, 2016, 27-28 and 31.

today's vast internet infrastructure (most of which is owned by the private sector); the breathtaking speed at which new digital technologies are developed and implemented with major impacts, coupled with the typical lag in fielding associated security measures; the many uncertainties with respect to applicable law; and the overlay of international dimensions (including active and widespread transnational cyber crime and ongoing conflict between cyber-adept nation states). All that said, the challenge is one that must be joined – even anticipating further achievable improvements within the existing cybersecurity framework. Quite simply, the current paradigm is not only far from ideal, but highly problematic in many ways.

A well-conceived alternative paradigm would arguably promote an essential shared commitment to maritime cybersecurity all across both the public and private sectors by defining clear and complementary roles for all key stakeholders pursuant to a comprehensive and fully-integrated partnership approach. Assembling and empowering the right brain trust to tackle this challenge could provide the essential foundation for a compelling call to action in this critical context.

The key themes and research questions generated by MRS 2017 will ideally serve not only to heighten awareness of the many potent cyber threats to maritime operations and infrastructure around the globe, but also to inspire and inform key aspects of ongoing domestic and international efforts to enhance maritime cybersecurity. The founders of the MRS initiative, as well as Tiffin University as host of the eighth event in this respected series, should be commended for their orchestration of these contributions.

###

Fred M. Rosa, Jr., a retired U.S. Coast Guard Rear Admiral, is Senior Advisor for Homeland Security at the Johns Hopkins University Applied Physics Laboratory (APL) and a Senior Fellow with the George Washington University Center for Cyber and Homeland Security (CCHS). He served as panel chair for the final MRS 2017 session.

John E. Crowley, Jr., also a retired U.S. Coast Guard Rear Admiral, is Executive Director of the National Association of Waterfront Employers (NAWE) and the Chair of the National Maritime Security Advisory Committee (NMSAC).

By way of disclaimer, the views expressed by the authors are solely their own and do not reflect the views of any government agency or any institution with which the authors are affiliated.

The authors wish to thank all of the MRS 2017 speakers, panelists, and other participants whose many worthwhile contributions were a primary source of insights and inspiration for this paper.

References

Ackerman, Robert K. "Creating a Common Language of Cybersecurity" *Signal* (Official Publication of the Armed Forces Communications and Electronics Association), August 2017.

Bouhdada, Jalal. "Maritime Cybersecurity: Securing Assets at Sea." *Security Week News,* May 1, 2018.

Charlet, Kate. "Understanding Federal Cybersecurity." Boston, MA: Harvard University, Kennedy School, Belfer Center for Science and International Affairs, 2018.

Cybersecurity Information Sharing Act. Pub. L. No. 114-113. 2015.

Executive Office of the President. *National Cyber Strategy.* Washington, DC, 2018.

Executive Office of the President. Presidential Policy Directive 41 of July 26, 2016, *United States Cyber Incident Coordination.* Washington, DC, 2016.

Executive Office of the President. *National Strategy for Maritime Security*. Washington, DC, 2005.

"Executive Order 13691 of February 15, 2013, Promoting Private Sector Cybersecurity Information Sharing," *Code of Federal Regulations*, no. 2016-09187.

"Executive Order 13800 of May 11, 2017, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," *Code of Federal Regulations*, no. 2017-10004.

Gero, Charlie. "Moving Beyond Perimeter Security: A Comprehensive and Achievable Guide to Less Risk." Cambridge, MA, Akamai Technologies Enterprise and Advanced Projects Group, 2018. https://www.bankinfosecurity.com/whitepapers/moving-beyond-perimeter-security-comprehensive-achievable-guide-to-w-4425.

Gerstein, Daniel M. "Putting the Security into Cybersecurity." *The National Interest,* September 30, 2017.

Kym Gillhooly. "Defense Department Moves to Augment GPS with Alternatives." *FedTech Magazine,* May 11, 2018. https://fedtechmagazine.com/article/2018/05/defense-department-moves-augment-gps-alternatives.

Gilmore, Scott. "The World Needs a Digital Geneva Convention to Fight Cyber Attacks." Rogers Media: Toronto, Ontario, Canada, 2018.

Hawkins, Derek. "The Cybersecurity 202: 'We Have to Work Together.' Government Struggling with Cyberthreat Information, Officials Say." *Washington Post*, July 23, 2018.

Homeland Security News Wire. "Improving Critical Sectors' Cybersecurity by Bolstering Sharing, Acting on Information." December 4, 2017.

Hummel, Richard. "Securing Against the Most Common Vectors of Cyber Attack." North Bethesda, MD, SANS Institute, 2017.

International Maritime Organization. "Guidelines on Cyber Risk Management" (MSC-FAL.1/Circ.3). London, United Kingdom, 2017.

Kramek, Joseph. "The Critical Infrastructure Gap: U.S. Port Facilities and Cyber Vulnerabilities." Washington, DC, Brookings Center for 21st Century Security and Intelligence, 2013.

Kuhn, Kevin. "Cyber Risk Management in the Maritime Transportation System." *Homeland Security Today.US*, February 9, 2018. https://www.hstoday.us/channels/us-coast-guard/cyber-risk-management-maritime-transportation-system/.

Maritime and Port Security Information Sharing and Analysis Organization. Press Release: "The Maritime and Port Security ISAO Convenes Inaugural Cybersecurity Summit at NASA/Kennedy Space Center, February 22-24, 2017." Beltsville, MD, 2017. PRWeb.com.

Maritime Transportation Security Act. Pub. L. 107-295. 2002.

Mendez, Victor M. and Robert O Work. Department of Transportation and Department of Defense Letter of December 8, 2015 to the U.S. House of Representatives,"Importance of the Global Positioning System (GPS) and the Need for a Complementary Positioning, Navigation, and Timing (PNT) Capability for the Nation." Washington, DC, 2015. https://rntfnd.org/wp.

Midgett, Amy. "Release of Offshore Operations and Passenger Vessel Cybersecurity Framework Profiles." *Coast Guard Maritime Commons* (blog), January 12, 2018. http://mariners.coastguard.dodlive.mil/2018/01/12/1-12-2018-release-of-offshore-operations-and-passenger-vessel-cybersecurity-framework-profiles/.

National Council of ISACs (Information Sharing and Analysis Centers). "About ISACs." Washington, DC, 2018). https://www.nationalisacs.org/media.

New York University. "Understanding Enterprise Risk Management: An Overview." New York, NY, 2016. https://www.nyu.edu/content/dam/nyu/financialOperationsTreas/documents/Resources.

North Atlantic Treaty Organization. Cooperative Cyber Defence Centre of Excellence. International Group of Experts. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge, United Kingdom: Cambridge University Press, 2017.

Northeastern University, Global Resilience Institute. "Global Resilience Research Network." Boston, MA, 2018. https://globalresilience.northeastern.edu/network/.

Osborn, Phillip. "Cyber Border Security – Defining and Defending a National Cyber Border." *Homeland Security Affairs*, 15, Article 5 (October 2017).

Perlroth, Nicole. "Reinventing the Internet to Make It Safer." *New York Times*, December 3, 2014.

Press, Gil. "A Very Short History of the Internet and the Web." *Forbes*, January 2, 2015.

RAND Corporation. "A Framework for Exploring Cybersecurity Policy Options." Santa Monica, CA, 2016.

Rigby, Jonathan and David White. "A New Paradigm for Cybersecurity: Moving from Protecting Perimeters to a Holistic System for Enterprise-Wide Information Protection." *Corporate Counsel Business Journal*, 22-39, January 5, 2016.

Schmitt, Michael. "In Defense of Sovereignty in Cyberspace." New York, NY: New York University School of Law, 2018.

Scales, Sarah. "Spoof, Jam, Destroy: Why We Need A Backup for GPS." *Science*, March 2, 2018. https://www.wired.com/story/spoof-jam-destroy-why-we-need-a-backup-for-gps/.

Scott, Rick. "Maritime Cybersecurity: A New Approach Is Needed." *Marine Reporter and Engineering News*, April 2018.

Ship Technology. "Rough Waters Ahead When It Comes to Cyber Risks." May 17, 2018.

Stanford Encyclopedia of Philosophy. "The Common Good." Stanford, CA, 2018. https://plato.stanford.edu/entries/common-good/.

Statista. "Internet of Things (Iota) Connected Devices Installed Base Worldwide From 2015 to 2025." Hamburg, Germany: Sorter Contact Group GmbH, 2018. Available at https://www.statista.com.

The Conversation. "Why 50,000 Ships Are So Vulnerable to Cyber Attacks." June 13, 2018.

Thompson, David. "Coast Guard Cyber Command 'Just As Important As Cutters and Aircraft'" (Interview of RADM Kevin Lunday, USCG). *Federal News Radio*, December 8, 2017.

https://federalnewsradio.com/dhs-15th-anniversary/2017/12/coast-guard-cyber-command-just-as-important-as-cutters-and-aircraft/.

Tiffin University. Program for the 8th Annual Maritime Risk Symposium, November 13-14, 2017. Tiffin, OH, 2017. Accessed September 14, 2018. https://www.tiffin.edu/criminaljustice/maritime-risk-symposium-2017/agenda.

Timberg, Craig. *The Threatened Net: How the Web Became a Perilous Place.* Washington, DC: Washington Post, 2015. Diversion Books.

Tucci, Drew, Joe DiRenzo III, and Scott Blough. "Cyber Shoal Waters: Understanding and Meeting Emerging Cyber Threats to the Marine Transportation System." *Maritime Reporter and Engineering News*, 79, no. 10 (October 2017).

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

U.S. Coast Guard. "Reporting Suspicious Activity and Breaches of Security (CG-5P Policy Letter No. 08-16). Washington, DC: 2016.

U.S. Coast Guard. Draft Navigation and Vessel Inspection Circular No. 05-17: "Guidelines for Addressing Cyber Risks at Maritime Transportation Act (MTSA) Regulated Facilities." Washington, DC, 2017.

U.S. Coast Guard. *Area Maritime Security Committees: Challenges, Accomplishments, and Best Practices – 2016 Annual Report.* Washington, DC, 2017.

U.S. Coast Guard. "Release of Offshore Operations and Passenger Vessel Cybersecurity Framework Profiles." Washington, DC (Coast Guard Maritime Commons Blog), 2018.

U.S. Congress. Scott S. Smith Statement for the Record of the Senate Armed Services Committee, "Roles and Responsibilities for Defending the Nation from Cyber Attack," 115th Cong. 1st sess., October 19, 2017. Washington, DC, 2017.

U.S. Congress. Daniel R. Coats Statement for the Record for the Senate Armed Services Committee, "Worldwide Threat Assessment of the U.S. Intelligence Community." 115th Cong., 2nd sess., March 6, 2018.

U.S. Customs and Border Protection, "Automated Commercial Environment and Automated Systems" (Washington, DC: 2018), https://www.cbp.gov/trade/automated.

U.S. Cyber Command. *Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command.* Fort Meade, MD, 2018.

U.S. Department of Commerce. National Institute of Standards and Technology. Computer Security Resource Center. Definition of "Cybersecurity." Washington, DC, 2018. https://csrc.nist.gov/Glossary.

U.S. Department of Commerce. National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. Washington, DC, 2018.

U.S. Department of Homeland Security, United States Computer Emergency Readiness Team (US-CERT). "Automated Indicator Sharing (AIS)." Washington, DC, 2018. https://www.us-cert.gov/ais.

U.S. Department of Homeland Security. "Global MOTR (Maritime Operational Threat Response) Coordination Center (GMCC)." Washington, DC, 2011. https://www.dhs.gov/global-motr-coordination-center-gmcc.

U.S. Department of Homeland Security. "Information Sharing and Analysis Organizations (ISAOs)." Washington, DC, 2018. https://www.dhs.gov/isao.

U.S. Department of Homeland Security. National Protection and Programs Directorate. Office of Cyber and Infrastructure Analysis. "Consequences to Seaport Operations from Malicious Cyber Activity." Washington, DC, 2016.

U.S. Department of Homeland Security. *Cybersecurity Strategy*. Washington, DC, 2018.

U.S. Government Accountability Office. *Coast Guard: Actions Needed to Enhance Performance Information Transparency and Monitoring* (GAO-18-13). Washington, DC, 2017.

U.S. Government Accountability Office. *Maritime Critical Infrastructure Protection: DHS Needs to Enhance Efforts to Address Port Cybersecurity* (GAO-16-116T). Washington, DC, 2015.

U.S. Government Accountability Office. *Maritime Security: National Strategy and Supporting Plans Were Generally Well-Developed and Are Being Implemented* (GAO-08-672). Washington, DC: 2008).

U.S. Government Accountability Office. *Urgent Actions Are Required to Address the Cybersecurity Challenges Facing the Nation* (GAO-18-645T). Washington, DC: 2018.

U.S. Maritime Administration. "U.S. Maritime Advisory 2018-006: Cyber Exploitation Worldwide." Washington, DC, 2018.

Wilson, J. R. "CGCYBER and Coast Guard Cybersecurity." Defense Media Network, March 14, 2018, https://www.defensemedianetwork.com/stories/coast-guard-cybersecurity/.