Combined Cyber and Physical Attacks on the Maritime Transportation System

By

Fred S. Roberts, Dennis Egan, Christie Nelson, Ryan Whytlaw
CCICADA Center, Rutgers University

For more information: Fred Roberts, froberts@dimacs.rutgers.edu

Abstract

For years, there has been discussion about physical security in the maritime transportation system (MTS). That discussion has led to standards, regulations, etc. In recent years, there has been an increasing interest in cyber security in the MTS that has led to discussions about best practices for cyber security. It is likely that many future attacks on the MTS (and other systems) will be multi-modal, including both a cyber and a physical component. As a simple example, hacking into security cameras at a port increases vulnerability to a physical intrusion. Thus, a cyber attack could be a precursor to a physical attack, and in fact the opposite could also be the case. This paper presents scenarios of combined cyber and physical attacks and describes ways to understand their likelihood based on ease of attack and seriousness of potential consequences.

1. Introduction

For years, there has been discussion about physical security in the maritime transportation system (MTS). That discussion has led to standards, regulations, etc.

In recent years, there has been an increasing interest in cyber security in the MTS (DiRenzo, Drumhiller, Roberts, 2017). This has led to the discussions about best practices for cyber security.

It seems clear that "conventional warfare" of the future will include a cyber component as well as a physical component. Indeed, publicly available military strategy from China, for example (Segal, 2017, The State Council Information Office of the People's Republic of China, 2015), indicates that the Chinese military expects to seize information dominance at the beginning of a conflict through cyber attacks.

Similarly, it is likely that future attacks on the MTS will be multi-modal, including both a cyber and a physical component (Tucci, 2017). As a simple example, hacking into security cameras at a port increases vulnerability to a physical intrusion. Thus, a cyber attack could be a precursor to a physical attack, and in fact the opposite could also be the case.

This paper resulted from the question of how the U.S. Coast Guard (USCG), or a vessel or facility operator, can identify and evaluate potential synergies between cyber and physical vulnerabilities to result in a holistic security assessment - including consequence management? We address this question by presenting scenarios of combined cyber and physical attacks, and discussing ways to understand their likelihood based on ease of attack and seriousness of potential consequences.

Our ideas result from the input of a variety of subject matter experts (SMEs) from the U.S. Coast Guard, the U.S. Secret Service, the Transportation Security Administration, various U.S. ports, and a public utility commission. A list of SMEs is included as an Appendix.

2. A Simple Example: Fake News to Create a Distraction

We concentrate first on ports. The first set of scenarios are based on the ideas that "fake news" could be spread via social media. For example, multiple messages could say that something is happening at Pier F in the port. This would draw first responders to Pier F. (As one SME put it, an analogy is youth soccer: Everyone runs to the soccer ball.) The actual intent is to attack Pier L, which now may have less protection because first responders at the port mass at Pier F. Another version of this would be for an attacker to hack into a company's or agency's email system and generate an official-looking report about Pier F. Still a third version is to spread the news that a celebrity is at Pier F (numerous messages saying, e.g., that Justin Bieber is at Pier F). Here, the intention is not to draw first responders away from another location, but it is to draw a crowd at a given location and then to attack the crowd with a physical attack.

A port facility protection plan should prevent leaving one area unguarded as in the first two fake news scenarios. A response plan would also require understanding how defenders can mitigate a tsunami of false reports. Could they plan for ways to get out their own messages? Would those messages possibly have a fast enough impact based on a torrent of fake news messages?

There are physical versions of this idea of using cyber methods to create a distraction. For example, we learned of an example where Hezbollah attacked first responders in Israel by first setting off an IED in a car, drawing first responders to a muster point, and then attacking the muster point with a bigger bomb.

Another model is that an adversary could create a distraction in the water, drawing police boats and USCG vessels to the area, leaving another part of the port unprotected.

3. Cyber Attacks on Operating Systems in the Port

There are many conceivable ways that a cyber attack on an operating system in a port could result in making a following physical attack more likely to succeed. Some examples are:

- Shut the gates so people are trapped inside and first responders are trapped outside.
- Turn off the lights to make it easier for physical attackers.
- Turn off the alarms to make it easier for physical attackers to avoid detection.
- Disable the cameras to make it easier to avoid detection.
- Interrupt the power supply to create a distraction.
- Disable cyber-enabled traffic lights to create traffic jams so that emergency vehicles are unable to respond to a physical attack.
- Hack into emergency communication system and tell first responders to go to a different place.
- Spoof TWIC cards or other access control systems to let the "bad guys' in.

Many of these seem feasible. (We discuss them more next.) However, an adversary with this level of sophistication might find it is easier to do a more intrusive physical break-in as the preliminary attack prior to a more serious physical attack. This is a central point: When we consider, potential scenarios for combined cyber and physical attacks, *the likelihood of a given scenario needs to be taken into consideration.* More generally, one should *consider threat, vulnerability, and consequence in determining the risk of a given attack scenario.* Not surprisingly, the SMEs we talked to did not always agree as to likelihood or risk.

To get into more detail, we note that disabling cameras may have a high level of risk because they are often add-ons. The ability to hacking into the emergency communications system depends upon how it is configured. If is connected to the Internet, it is certainly possible. Jamming communications might be easier. One SME felt that port security would quickly determine that hacking into the emergency communications systems was indeed a hack and would limit first responders going to the wrong place. A Denial of Service Attack could turn off the lights or the alarms. A cyber attack on the power supply could have significant consequences since many terminal operations do not have backup generators.

At some operating ports, one system handles all gates. At others, there are individual gate controls. Which is less vulnerable? By sheer size, ports might not be so vulnerable to access control hacks; airports or schools or hospitals might be more vulnerable. Moreover, doors or gates locked by access control systems are supposed to have overrides for life safety, typically a mechanism to break the circuit. So this scenario might be less likely since the "bad guys" wouldn't buy much time and so the likelihood of their trying it might be small.

Do ports have plans to respond quickly to these various cyber scenarios that could be preliminary to a physical attack? The speed with which first responders could respond would depend upon the port's Facilities Security Plan. It might also depend on the MARSEC level.

4. Port Security can Create Vulnerabilities

Efforts to make our ports more secure might in fact create unexpected vulnerabilities. Large sports and entertainment venues use walkthrough metal detectors or other systems to screen patrons. The long lines waiting to be screened create vulnerabilities. After the 2013 Boston Marathon attacks, sports stadiums sought to minimize vulnerabilities by creating an outer perimeter with initial screening.

Similarly, at a cruise ship terminal with many ships leaving at roughly the same time, lines form outside the building. Passengers are initially vetted to see if they have a valid ID and are at the right terminal. An attacker should not get past the screener. (Unless they bought a cheap ticket just to get inside.)

The 2017 attack at the Ariana Grande concert in the Manchester Arena showed that patrons leaving an arena could be vulnerable. What if they were "drawn out" in a group by hacking into the arena's emergency communication system or "message board"? This has

raised the awareness in the venue security community about vulnerabilities of patrons leaving a venue.

In general, it is thought that debarking at cruise ship terminals does not have as many vulnerabilities as embarking. Passengers are released in groups to avoid standing in line at customs. There is good departing security. Operators think you are ok once you leave the dock. But what if a hacker could manipulate an alarm system to get them all to debark at the same time? There is still an under-appreciation of debarking vulnerabilities at ports.

Could a hacker manipulate an alarm system (e.g., fire alarm) and perhaps a communication system to get passengers to debark at the same time? That might depend upon whether the alarm system and communication system were online. Port fire alarm systems are not too sophisticated. They are designed to operate over a network and push a signal out to a monitoring agency. It might be a challenging hack to get into this system. Physically setting off the fire alarm might be more likely to succeed. Even if a "bad guy" could get the fire alarm going, would this create the desired problem? If a fire alarm goes off in a cruise ship port, there are many people trained to direct passengers where to go. Those people would more likely be used than an audible emergency message. So the scenario of additionally hacking into a communication system is not very likely to have the desired effect.

In some port systems, if a fire alarm goes off, certain doors open up. Thus a physical attack on the alarm system could create access to an attacker seeking to introduce malware into a port operations or cargo handling system. So, physical attacks can be the precursor to cyber attacks, not just vice versa, and one needs to be aware of this possibility.

5. Taking Advantage of Port Congestion

Port congestion is a big problem in all ports. Large container vessels add to the congestion problem. It used to be that several smaller vessels in port at the same time – using different terminals. Now there is one large one – requiring all of its unloading/loading at one terminal. The scheduling of trucks picking up or delivering containers is controlled by a cyber system. A simple denial of service attack could impact the ability to offload a large ship in a timely way. This would result in traffic jams in the port area. In turn, that could create the possibility of having a serious impact by throwing a bomb.

6. Autonomous Vehicles in Ports

Terror attacks using vehicles are on the rise, witness recent such attacks in Berlin, Nice, London, and New York. The lines of passengers lining up to embark on cruise ships could be vulnerable to this type of attack. But terrorists ended up dying in the process. What if they could control a vehicle remotely and not risk dying? Would that make this type of attack even more likely?

Car hacking in which "bad guys" remotely take control of your car to steal it or use it as a weapon is certainly already feasible. For instance, in 2013, Miller (Twitter) and Valasek (IOActive) demonstrated how to take control of a Toyota Prius and Ford Escape from a

laptop. They were able to remotely control smart steering, braking, displays, acceleration, engines horns, lights, etc. (Greenberg, 2013). This becomes a serious issue as in-car technology becomes more sophisticated. Indeed, there are already thousands of semi-autonomous cars – modern cars are more like bundles of computers on wheels. And fully autonomous cars are coming.

Already, many ports are operating with autonomous vehicles. At the Long Beach container terminal, a gantry crane operator brings a container to an autonomous truck. A computer lowers the container to the truck, which takes it to a storage area or a non-autonomous truck. Autonomous trucks even monitor their battery life and drive themselves to charging station for a recharge – operated by a robot. The Hampton Roads container terminal is completely automated, robotic, and intermodal (rails, cars, trucks). Cranes are run from an office. All vehicles are autonomous. Could an autonomous truck be used as a weapon in a port scenario? It is technically possible. An adversary could use low-cost jammers to jam the GPS that makes the autonomous vehicle work. GPS jamming is possible with low cost jammers available over the Internet (though illegally). Many devices are battery-operated or can be plugged into a cigarette lighter and cost as little as $20.The hacking might seem harder to do than hijacking a truck and driving it into the port to create havoc. Also, where autonomous trucks operate in a port, they are blocked from people, so would more likely damage infrastructure. This suggests that the risk of this scenario is not so high, both because it would be easier to do something different and because the consequences of the original scenario might not be that high, at least in terms of human life. However, automated vehicles in ports create other problems. Could a "bad guy" hack into the control system and arrange to put the "wrong" box on the wrong train, or take it to the storage facility and open it?

Unmanned aerial vehicles might be a much bigger risk to a port than unmanned trucks. Ports have a great deal of hazardous material readily attacked from the air (LNG, gasoline, etc.) Prof. Todd Humphreys of UT Austin has demonstrated how GPS signals of an unmanned aerial vehicle can be commandeered by an outside source (Cockrell School of Engineering, 2012). How do you mitigate against hackers taking over a drone and dropping it on hazardous material? You can't knock it out of the air because that itself could cause it to drop on hazardous material. Ports don't have authority to take over a drone and take it down.

A drone could also be a threat to a vessel entering or leaving a port. Could an attacker hack into a drone and have it land on the deck of a nearby cruise ship? You might cause some panic this way. A scenario with a large impact would be to load it with explosives and have it land on the deck and then create an explosion.

7. Hazardous Materials in Ports

As noted above, ports have or host a lot of hazardous materials. As a case in point, gigantic LNG ships enter directly into the city of Boston to dock at the LNG terminals in Boston Harbor. It is one of the few ports in the world (and only one in US) where this happens.

Could a cyber attack on an LNG ship cause it to careen off course and create an explosion? This is not likely – there are tugs on it and the Coast Guard keeps other vessels away.

However, once the ship is in the terminal, if an adversary could access its industrial control systems, they could cause a serious problem. There are pumps, valves, etc. (operational technology – OT) run by software/computers (IT systems). Hacking into those systems could conceivably lead to an explosion in light of the hazards from LNG. How likely is this scenario? At least one of our sources had this as his nightmare scenario.

Maybe this isn't so far-fetched. The Stuxnet is a malicious computer worm that targets industrial computer systems. It put a virus into a controller running centrifuges and damaged them – causing substantial damage to Iran's nuclear program (Zetter, 2014). Similarly, an adversary could hack into a sensor system, e.g., affecting tank level indicators, pressure sensors, temperature sensors, hazardous gas sensors. A leak or build-up of pressure or a fire might not be detected, thus possibly leading to an explosion. Recently, Naval Dome described how a hacker could penetrate numerous machinery control systems on a vessel. We discuss this in Section 10.

To add to the discussion of hacking into sensor systems, we note that sensor systems other than those used on a vessel could also be hacked. An explosion or fire started at some other port facility from a hack into a sensor system could serve as a distraction and make it easier to succeed with a physical attack. A bad actor could also hack into the system to set off a false alarm that could serve as a distraction. Could an adversary start a cyber attack by first physically starting some hazardous materials on fire or releasing noxious gases, creating a diversion? This might allow them to gain access to a facility and hack into it.

8. Cargo

Modern port operations, around the world, are heavily dependent on complex networked logistics management systems that track maritime cargo from overseas until it has reached a retailer. Yet, these systems are subject to cyber attacks that can cause significant problems.

The Port of Antwerp is one of the world's biggest. During 2011-2013: Hackers infiltrated computers connected to the Port of Antwerp, located specific containers, made off with their smuggled drugs and deleted the records. Attackers obtained remote access to the terminal systems; released containers to their own truckers without knowledge of the port or the shipping line. Access to port systems was used to delete information as to the existence of the container after the fact. The hackers began by emailing malware to the port authorities and/or shipping companies. After the infection was discovered and a firewall installed to prevent further infections, the criminals broke into the facility housing cargo-handling computers and fitted devices allowing wireless access to keystrokes and screen shots of computer screens. The first part of this was a cyber attack preceding a physical attack (stealing cargo). The second part was a physical attack (breaking in) preceding a cyber attack, which in turn preceded a physical attack (stealing cargo). (See Bell, 2013, CyberKeel, 2014, Pasternack, 2013, Wagstaff, 2014.)

There have been other examples of cyber attacks followed by physical attacks (stealing cargo). In 2012 it was revealed that crime syndicates had penetrated the cargo systems operated by the Australian Customs and Border protection. The penetration of the systems allowed the criminals to check whether their shipping containers were regarded as suspicious by the police or customs authorities. The consequence was that containers with contraband were abandoned whenever such attention was identified by the criminals. Others could be handled without worrying about the police. (See CyberKeel, 2014.)

The Iranian shipping line IRISL suffered from a cyber attack in 2011. The attack damaged data related to information such as cargo number, rate, loading information, date, place, etc. The result was that it was impossible to know where containers were, even whether they had been loaded, and whether they were onboard ships or onshore. The data was eventually recovered, but there were major disruptions in operations, including cargo sent to wrong destinations and lost cargo. The results were severe financial losses. (See CyberKeel, 2014.)

9. Blocking the Port Entryway

Could an adversary block entry to a port from the water through a cyber attack? The chokepoint for a port is the channel. Blocking it could create a big problem. Consider for example the Kill van Kull in New York – if an adversary could cause a vessel to run aground there, this would create a huge problem. If an adversary could do this, they could create a great deal of economic damage if the port remained closed for a period of time.[1]
In a bad case, the port could remain closed for a year or more. (It took 20 months to get the grounded Costa Concordia cruise ship off the rocks in 2013 – Mackenzie, 2013. An adversary could also divert port resources to clearing the blockage, and possibly create an opening for a following physical attack e.g., through a bomb in the port. At the least, they might create huge traffic jams, not allowing emergency vehicles to enter to counter that physical attack.

Autonomous vessels are coming. Could an adversary hack into such a vessel as it approaches a port and cause it to ram into another vessel or a bridge? Or run it aground, thereby blocking the entryway to a port? Could they choose one loaded with LNG for maximum damage? One SME told us this was not likely. There are alarms and warnings that you would have to bypass. Would port authorities overcome mistrust of automated systems to allow an autonomous vessel to operate in congested or treacherous waterways?

[1] Disruption of the MTS could cause billions of dollars in damage to the economy. During the month of January 2015, the ports on the West Coast of the United States were closed due to a labor stoppage and the impact on the economy was dramatic [Salmon, 2015]. Those economic impacts are sometimes calculated using computable general equilibrium methods or via simulation. Actual events and simulation studies have indicated losses of tens of billions of dollars from various broader impacts of port disruptions (see, e.g., Cohen 2002, Park 2008, Rose and Wei 2013, Werling 2014). Cyber disruptions could have similar outcomes. (For more on the latter, see Rose 2017.)

In San Francisco, for example, the eddy current can make your bow veer towards a bridge abutment and there is not much tolerance for variance from the intended path. Would the pilots union allow the vessel to enter the port without a pilot?

Another SME thought this scenario was feasible. One complex attack would be to spoof a ship's Automatic Identification System (AIS) to arrange it so awareness systems are not transmitting a problem. AIS tracks ships automatically by electronically linking data with other ships, AIS base stations, and satellites. This system enables ships to share positional data with other ships. It offers awareness about those operating within the MTS. An attacker could exploit weaknesses in AIS and falsify a vessel's identity or type, or its position, heading, and speed, as well as to hide problems. (See Mullin, 2014, Zora, Zora, and Kucan [2013.) Spoofing AIS and arranging no transmission could allow a "bad guy" to take over an autonomous vessel and run it hard aground. It is unlikely defenders could mitigate the impact of such an event if they saw it happening. You can't interdict very well on the water. There are few options except to ram the vessel running out of control – which could also cause an explosion.

Recently, Naval Dome, an Israeli company, showed that it was feasible to attack the ECDIS (Electronic Chart Display and Information System) of a vessel. They designed an attack to change the vessel's position during a "night-time passage through a narrow canal." Their attack left the ECDIS display looking completely normal while the actual situation was not and, if fully implemented, would have sent the vessel aground. The "position, heading, depth and speed" all looked different from what they really were. The attack took place through the captain's computer, "which is regularly connected to the internet through a satellite link, which is used for chart updates and regular logistic updates." (See AJOT, 2017.)

Baraniuk (2017) describes a cyber attack on the ECDIS system of a ship in an Asian port. Malware was introduced into the computers of a large 80,000 ton tanker when a crew member used a USB stick to print some paperwork. Later, a second crew member used a USB stick to update the ship's charts, and the ECDIS was infected. Luckily, this was caught and the main damage was delayed departure.

The hull stress monitoring system (HSMS) is designed to detect problems with stability and balance. If an attacker could cause an imbalance of cargo without the crew being aware, through an attack on the HSMS, it is possible that a vessel could be put under stress and eventually break up and sink. Pen Test Partners have demonstrated how this might happen. Many HSMS are PCs connected to a ship's network. Taking control of such a PC, a hacker could arrange to have containers loaded in such a way as to create imbalance without the crew's knowing about it. The hacker could take control of the load planning software that places heavier containers to place heavier containers at the top or all on one side. (See MarEx, 2017.) While this is all feasible, there would be difficulty in predicting where the ship might break up or sink. Thus, it might not be an effective way to arrange to block a tight shipping channel, making the risk of such an attack less likely – unless the goal was to simply demonstrate the ability to destroy a vessel and achieve the resulting economic damage.

An adversary might be able to block the port entryway without attacking a particular vessel. All ports operate at full capacity. Due to amount of incoming vessel traffic, the only way to schedule arrivals at a modern port is by computer. An adversary could attack the port traffic management system or the AIS on many of the incoming vessels. A few $500 portable devices placed in a few areas around the port could jam the AIS of incoming ships. Ships would anchor in place. Even if the authorities identified the jamming signal, it could be repeated the next day. The port would be closed. The adversary might even follow up by physically attacking one of the ships at anchor. Not everyone agrees that the taking out of multiple AIS systems scenario would be a big problem. There are tertiary systems to replace AIS, e.g., radar. Moreover, especially in a port where the weather is usually good, even line of sight would allow vessels to operate and enter the port.

An adversary might also stop traffic by setting a terminal on fire, or setting a moored ship on fire or causing an explosion at a berthed ship. Could an adversary accomplish this by hacking into the fire control system? Could they accomplish this by initiating the fire by taking over a drone (hacking into it) and fitting it with a taser?

10. Attacks on the Cyber-physical Systems on a Vessel

Today's vessels are highly dependent on cyber-physical systems. Vessels are less tightly regulated than facilities. On a vessel, just the number of control systems make it difficult to defend against an attack. In cyber security awareness, navigation systems and control systems and their vulnerabilities are gaining increasing attention.

For modern ships there is dependence on a proliferation of sophisticated technology – that is subject to cyber attack. This includes:

- ECDIS (Electronic Chart Display and Information System)
- AIS (Automatic Identification System)
- Radar/ARPA (Radio Direction and Ranging) (Automatic Radar Plotting Aid)
- Compass (Gyro, Fluxgate, GPS and others)
- Steering (Computerized Automatic Steering System)
- VDR (Voyage Data Recorder –"Black Box")
- GMDSS (Global Maritime Distress and Safety System)
- Numerous other advanced units and systems

ECDIS flaws might allow an attacker to access and modify files and charts on board or on shore. See the discussion above about Naval Dome's ECDIS attack. The result of modified chart data would be unreliable and potentially dangerously misleading navigation information. That could lead to a mishap resulting in environmental and financial damage. In January 2014, the NCC Group tried to penetrate an ECDIS product from a major manufacturer. Security weaknesses such as ability to read, download, replace or delete any file stored on the machine hosting ECDIS were found. Once such unauthorized access is obtained, an attacker could interact with the shipboard network and everything to which it

is connected, causing chaos. Such an attack could be made through something as basic as insertion of a USB key or through download from the Internet. (See CyberKeel, 2014.) An adversary doesn't need physical access to cause damage; they can get in via cellphones or satellite.

In October 2013, Balduzzi, Wihoit, and Pasta [2013] demonstrated how easy it is to penetrate a ship's AIS. Recently a Coast Guard Academy team used commercially available software to hack into AIS and turn it off. Per Cyberkeel [2014], such a hack could allow an attacker to impersonate marine authorities to trick the vessel crew into disabling their AIS transmitter. This would render the vessel invisible to anyone but the attackers themselves. AIS spoofing has apparently happened recently. There were suspected cases of mass-spoofing of AIS in the Black Sea in June 2017, with more than 20 ships affected. The GPS were giving false locations, some inland and some at airports. (See Blake, 2017).

Naval Dome has demonstrated how an attack could penetrate a vessel's machinery control system. It targeted the ballast system and was able to affect the valves and pumps (and stop them from working) while the display did not show any problems. Other systems such as generators, air conditioning, or fuel systems could also be controlled in this way. (See AJOT, 2017.)

Attacks on the hull stress monitoring system are also of potential concern, especially if combined with attacks on the load balancing system while loading cargo. See the discussion in Section 9.

11. Monitoring a Vessel from a Distance; Ransom-ware

There is increasing interest in being able to monitor the behavior of shipboard systems from elsewhere, e.g., company Headquarters. Now, engine manufacturers monitor their engines for reliability, but also to make sure they are not being abused - which would void a warranty. They might be watching sensors that give advance notice that something isn't working right, for example detecting vibrations before a bearing goes bad. Manufacturers might also take control of onboard computers to install software upgrades. The bottom line is that many outsiders have access to vessel systems. A bad actor could hack into your system from outside, especially if your shipboard systems are networked. For Headquarters or an engine manufacturer to monitor a vessel's systems, the vessel might send telemetry from the ship. As soon as they create the network connection, there could be a problem. One could try to completely separate a sensor network. But of course it is easier to put everything on the same network – thus causing potential problems. This opens the vessel up to ransom-ware attacks, to pay ransom to get some shipboard system working again. Monitoring from elsewhere also leads to a different combined attack scenario: Start with a physical attack on the remote monitoring facility that allows the adversary to take over the facility and send malicious code to your vessel.

Could a "bad actor" inject ransom-ware and actually stop a vessel? Something like this actually happened to a commercial freight operator. They had their administrative system separate from their machine control system; the attack impacted the former. An economic

effect (the ransom) was the desired outcome.[2] But what if the desired outcome was physical: stop the vessel in its tracks, making it easier to board it with a physical attack?

12. Cruise Ships: Passenger Systems and Vessel Systems

Today's cruise ship passengers want communication and entertainment systems akin to what they are used to ashore. Cruise ship operators are increasingly aware of the interplay between these systems and the critical IT systems on the vessel. There is a "tug of war" between reliability (which passengers demand of their systems) and vulnerability. A knowledgeable actor could take advantage of the vulnerabilities in the former to attack the latter. Today's cruise ship operators are fire-walling the servers for the passengers and those for the ship's operation, control, and hotel functions. There could be several hundred of the latter. Disrupting hotel services (water, power, AC) could make life unacceptable for passengers – a physical attack of sorts on passengers and a definite economic attack on the cruise ship industry. The industry thinks it understands how a "bad guy" might do this. Of most concern was that an attack like this could come through the passenger email system. But that has been largely dismissed because firewalls have been set up. There remains a vulnerability through authorized services that handle things remotely, e.g., desalinators and other equipment with lots of computer controls.

13. Hacking into a Cruise Ship's Navigation System

A 2012 demonstration by a UT Austin team showed how a potential adversary could remotely take control of a vessel by manipulating its GPS. The yacht "White Rose of Drax" was successfully spoofed while sailing on the Mediterranean. The team's counterfeit signals slowly overpowered the authentic GPS signals until they ultimately obtained control of the ship's navigation system. "The ship actually turned and we could all feel it, but the chart display and the crew saw only a straight line." (Bhatti and Humphreys, 2014, Zaragoza, 2014). It is important to note that the GPS and navigation systems impacted were

[2] Maersk Lines is the world's largest container shipping company and moves 20% of the world's freight. In June 2017, a cyber attack on Maersk made everyone in the MTS sit up and take notice and gives a small idea of the impact of ransomware. The NotPetya virus was involved in ransomware attacks on Maersk and various other companies. Operations at Maersk terminals in four countries were affected, there were delays and disruptions for weeks, and the cost was estimated at $200M-$300M. (Osborne, 2018). A July 2018 cyber attack on Cosco Shipping Lines that caused failure in its networks in the United States, Canada, Panama, Argentina, Brazil, Peru, Chili, and Uruguay, was not as successful as the Maersk attack. Presumably Cosco had learned from what happened to Maersk and had isolated its internal networks, thus minimizing damage from the attack. [See Mongelluzzo, 2018.] This example raises the importance of information sharing in cyber defense. In sectors other than maritime, there is robust exchange of information about new types of attacks, new types of defenses, etc. The maritime sector has lagged behind. See Egan, et al, (2017) for a discussion of possible reasons, and possible approaches to change things. A key issue here is what kinds of incentives to give to companies to share information about cyber attacks with competitors and the government, when revealing such information could cause them significant financial loss. What economic and other incentives can we design to make such information sharing more likely?

essentially the same as those used throughout commercial maritime operations and the Marine Transportation System, generally. "White Rose of Drax" was not a "soft target." However, a realistic analysis of the threat underscores the need for both proximity and persistent presence required for this attack to work. It can't be done remotely.

In February 2017, hackers reportedly took control of the navigation systems of a container vessel en route from Cyprus to Djibouti for 10 hours. "Suddenly the captain could not manoeuvre. … The IT system of the vessel was completely hacked." The attack was carried out by "pirates" who gained full control of the vessel's navigation system intending to steer it to an area where they could board and take over. (See Blake, 2017.) Certainly either of these examples demonstrates the possibility of hacking into the navigation system of a cruise ship.

Consider the scenario where a bad actor hacks into the navigation system on a cruise ship and causes it to change direction imperceptibly, eventually running it aground. This could be the precursor for a physical attack on the ship. Is this scenario feasible? Several of our SMEs described a failed GPS off of Cape Cod leading to the grounding of the Royal Majesty, heading from Bermuda to Boston in mid 1995. It resulted from failing to reconnect the navigation system to the GPS after maintenance. (See Blackett, 2004.) Jamming a ship's navigation system takes almost no sophistication. Spoofing it takes more.

One SME pointed out that if a bad actor spoofed a ship's GPS so that there are small changes in course, it is possible the crew would not notice. Especially at night if there were no visual cues. (There were such cues for the Royal Majesty.) The bad actor would need intimate knowledge of where the vessel is and reasonably close access. They would need to transmit false data. Each time they told it it was off course to the left (though not true), it would compensate by moving to the right. However, another SME pointed out that with modern ECDIS, the radar overlay would show your GPS is off. Another SME said that a physical attack is unlikely to be very successful since first responders would be there quickly.

Another SME pointed out that it would be a challenge for the bad actor to predict where the vessel would hit and therefore prepare for a physical attack. However, they could move the vessel to go into a shipping lane they want it to go into - perhaps making the physical attack easier. Another SME pointed out that an attacker could alter charts, hiding what shoal waters exist, leading to grounding of the vessel in a desired area. Just being able to run a cruise ship aground would have a major psychological impact. The result could be a major economic blow to the cruise ship industry. So even without human casualties, the would be a major effect of the cyber attack of grounding the ship.

14. Attacking Cruise Ship Passengers by Having them Move

Consider an attack on a cruise ship analogous to those in a port, where some hack on a ship's system leads to people gathering in large groups, creating vulnerability. (See Section 2.) Could a "bad guy" hack into the fire alarm system on a cruise ship, leading passengers to gather at mustering boat stations as a prelude to a physical attack there? This could happen through a planted explosive or attack by group arriving by boat or a suicide

bomber on board cruise ship. Is this a plausible scenario? It seems feasible to hack into a fire alarm system on a ship, at least in some cases. But wouldn't it be easier to let an inside actor attack a large group of passengers already in one place – e.g., dining room? Or wouldn't it be easier for a group of attackers to come alongside by boat and just start shooting at miscellaneous passengers? One SME doubted this kind of combined attack would work because security on cruise ships is so good.

Note that to maximize impact, an attacker would not have to follow the fake fire alarm with a physical attack. They could simply fake a fire alarm, announce they were responsible and say they could do it again. This could create psychological impact and potential economic damage to the cruise industry. Doing this multiple times would create an even bigger impact.

An attacker could also avoid the challenge of hacking into the fire alarm system on the vessel by starting a real fire to activate the fire alarm. However, this would require physical presence, whereas the precipitating cyber attack to set off the fire alarm could be done from a distance.

Could a fire alarm arising from a hack or a physical act be just a distraction for a cyber attack – loading something on a server to use later? Conceivably, according to an SME, but not likely because servers would be locked down and because fire drills don't take very long. However, another SME felt that attackers could move crew where they want them and away from the location of a desired cyber attack, which could be to any of a number of control systems on the vessel.

15. Ferries

Many of the cyber attacks described for cruise ships are also relevant for ferries. The combined attacks we have described might have another component, since passenger screening on ferries is less stringent than on cruise ships and vehicle screening is inconsistent. This allows for the possibility of a cyber attack followed by a physical attack through a passenger or a vehicle.

16. Cargo at Sea: Pirates

Pirates have been reported to have hacked into a cargo management system and identified where on a vessel valuable cargo is located. This enabled them to make a very fast and efficient raid on a vessel, going right to the container of interest. (See Hand, 2016.) Is this feasible?

One of our SMEs felt that it was feasible to hack into the cargo system and identify containers of interest and their location, but wondered how this would help the pirates since it is only the topmost containers they could access.

Another of our SMEs pointed out that the USCG had gotten quite good at getting into containers upon boarding a ship. Still another SME pointed out that the adversary could influence the loading of containers so that those of interest were placed to be accessible.

17. Autonomous Vessels

Our SMEs all felt that autonomous vessels were coming, soon. Such vessels will be programmed to decide where to go; will be tracked and monitored using diagnostics from Headquarters; will put out a problem message if they are unable to solve a problem, resulting in Headquarters sending instructions on where to go for repair. Do we trust the technological solutions so such vessels can go alone on the seas? Could a hacker take over the Headquarters computer and instruct the vessel to go to a place where it could be boarded by attackers?

The owners of an autonomous vessel are saving on crew costs but accepting some risk. One SME told us that shipboard systems and shipboard industrial control systems would be much harder to patch or have their software updated than many other systems. These systems might not be updated in real time, and hence become vulnerable to ransom-ware.

An attacker could jam or spoof the GPS or do a more sophisticated attack on the control system of the internal diagnostics of such a vessel. Could this affect heat or pressure or gas sensors, leading to an explosion, as in the example of Sec. 7 and in the discussion in Section 10 of an attack on the machinery control systems? This could cause economic damage, and possibly loss of life as well. If the goal of the attacker is psychological impact, they wouldn't do it in the middle of the ocean, where there is no media to film things. However, near a port, the vessel might not be entirely autonomous.

18. Closing Comments

Ultimately, the weak link in defense against combined cyber-physical attacks is still the human being. A successful attacker tries to influence behavior, leading to bad decisions. He or she would aim to introduce doubt, for example through false aids to navigation showing up on an electronic chart, spoofing a vessel track that may not correlate with radar, and creating a chain of things initiated by influencing the thinking of the bridge operator.

Our discussion has been limited to a single pair of events, one cyber, one physical. But there could be multiple events, or cascading events. More work is needed to develop scenarios for those. For example, an adversary could attack a cruise ship in a port and announce their intention to attack other cruise ships in other ports. What would the Coast Guard do? Would it close down those other ports, creating a vulnerability with large crowds waiting to embark? While it is not an MTS example, the following example of cascading events in an attack on the power grid, developed by the Cambridge Centre for Risk Studies and Lloyd's of London (Freedman, 2016), illustrates the point. Imagine hackers gaining access to the US electric power grid without security being alerted. They could do this through remote access systems, network monitoring systems, or personal devices of key personnel. Then the attackers lie low until some time in the future, when they would disable safety

systems, allowing them to affect the circuit breakers on multiple generators and damaging some of their bearings. As a result, many generators burn and are partially destroyed, and operators shut down other generators to investigate. A large population across many states is left without power. This affects street lights, water systems, transit systems, phone systems, ATMs, etc. It takes weeks to restore power and the economic cost is enormous. To add to this, in the interim, the attacker gains access to multiple other systems that depend upon power to protect access, allowing for further cyber attacks on water systems, transit systems, banking systems, etc. One should be able to envisage similar cascading effects/attacks on the MTS.

This paper has been limited in scope. Examples of other areas to investigate include combined attacks on locks, drawbridges, barges, oil rigs, inter-modal landside connections, etc.

Fundamentally, there does not seem to be anything special one would do to prevent a cyber attack intended as a precursor to a physical attack that one wouldn't do to prevent any cyber attack.

References

AJOT, 2017. Cyber penetration tests underscore maritime industry's nightmare security scenario. American Journal of Transportation , December 21, 2017. https://www.ajot.com/news/cyber-penetration-tests-underscore-maritime-industrys-nightmare-security-sc, accessed Dec. 26, 2017.

Balduzzi, M., Wihoit, K., Pasta, A., 2013. Hey Captain, where's your ship? Attacking vessel tracking systems for fun and profit, 11th Annual HITB Security Conference in Asia, October 2013. http://conference.hitb.org/hitbsecconf2013kul/materials/D1T1%20-%20Marco%20Balduzzi,%20Kyle%20Wilhoit%20Alessandro%20Pasta%20-%20Attacking%20Vessel%20Tracking%20Systems%20for%20Fun%20and%20Profit.pdf, accessed Feb. 21, 2015.

Baraniuk, C., 2017. How hackers are targeting the shipping industry. BBC News. https://www.bbc.com/news/technology-40685821, August 18, 2017, accessed Aug. 6, 2018.

Bell, S., 2013. Cyber-attacks and underground activities in Port of Antwerp. Bull Guard, Oct. 21, 2013. http://www.bullguard. com/ blog/2013/10/cyber-attacks-and-underground-activities-in-port-of-antwerp.html, accessed Feb. 21, 2015.

Bhatti, J., and Humphreys, T.E. 2014. Covert control of surface vessels via counterfeit surface GPS signals. Unpublished. https://pdfs.semanticscholar.org/6f20/450b32b71f2454e63292acb632d3619ee8ef.pdf, accessed Dec. 12, 2017.

Blackett, C., 2004. Analysis of the Royal Majesty grounding using SOL 3rd Bieleschweig Workshop on Systems Engineering, 12-2-2004. http://www.rvs.uni-bielefeld.de/Bieleschweig/third/Blackett-B3-2004.pdf, accessed Dec. 13, 2017.

Blake, T., 2017. Hackers took 'full control' of container ship's navigation systems for 10 hours. ASKET Ltd, Maritime Security News and Updates, Nov. 26, 2017. https://www.asket.co.uk/single-post/2017/11/26/Hackers-took-full-control-of-container-ships-navigation-systems-for-10-hours-AsketOperations-AsketBroker-ELouisv-IHS4SafetyAtSea-TanyaBlake-cybersecurity-piracy-shipping, accessed May 14, 2019.

Cockrell School of Engineering, 2012. Todd Humphreys' research team demonstrates first successful spoofing of UAV. The University of Texas at Austin Aerospace and Engineering and Engineering Mechanics News. June 12, 2012. http://www.ae.utexas.edu/news/504-todd-humphreys-research-team-demonstrates-first-successful-uav-spoofing, accessed Dec. 28, 2017.

Cohen, S. S. 2002. Economic Impacts of a West Coast Dock Shutdown. Unpublished report prepared for the Pacific Maritime Association, Berkeley Roundtable on the International Economy, University of California at Berkeley, Berkeley, CA: University of California at Berkeley.

CyberKeel, 2014. Maritime Cyber-Risks: Virtual Pirates at Large on the Cyber Seas. White Paper, CyberKeel, Copenhagen. October 15, 2014.

DiRenzo, J. III, Drumhiller, N., Roberts, F.S. (Eds.), 2017. Issues in Maritime Cyber Security. PSO-Westphalia Press.

DiRenzo, J. III, Goward, D.A., Roberts, F.S., 2015. The little-known challenge of maritime cyber security. Proceedings of the 6th International Conference on Information, Intelligence, Systems and Applications (IISA), IEEE, 2015, pp. 1-5. DOI: 10.1109/IISA.2015.7388071

Egan, D., Hering, D., Kantor, P., Nelson, C., Roberts, F., 2017. Information Sharing for Maritime Cyber Risk Management. In DiRenzo, J. III, Drumhiller, N., Roberts, F.S. (Eds.). Issues in Maritime Cyber Security. PSO-Westphalia Press, 2017, 271-302.

Freedman, A., 2016. Cyber grid attack: A cascading impact. Risk & Insurance, April 2016 issue. http://riskandinsurance.com/cyber-grid-attack-cascading-impact/, accessed Dec. 14, 2017.

Greenberg, A. 2013. Hackers reveal nasty new car attacks – with me behind the wheel. Forbes, Aug. 12, 2013. https://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/#18a55198228c, accessed Dec. 11, 2017.

Hand, M., 2016. Cyber-attack allows pirates to target cargo to steal. Seatrade Maritime News, July 7, 2016. http://www.seatrade-maritime.com/news/americas/cyber-attack-allows-pirates-to-take-a-roman-holiday.html, accessed Dec. 13, 2017.

Mackenzie, J., 2013. Wrecked cruise ship Costa Concordia raised off Italian rocks. Reuters, Sept. 16, 2013. https://www.reuters.com/article/us-italy-ship/wrecked-cruise-ship-costa-concordia-raised-off-italian-rocks-idUSBRE98F02T20130917, accessed Dec. 13, 2017.

MarEx, 2017. Hackers could sink a bulk carrier. The Maritime Executive, Dec. 20, 2017. https://www.maritime-executive.com/article/hackers-could-sink-a-bulk-carrier#gs.ZogtZZo , accessed Aug. 6, 2018.

Mongelluzzo, B., 2018. Cosco's pre-cyber attack efforts protected network. JOC.com, July 30 2018. https://www.joc.com/maritime-news/container-lines/cosco/cosco%E2%80%99s-pre-cyber-attack-efforts-protected-network_20180730.html, accessed Aug. 6, 2018.

Mullin, S., 2014. Cyber resilience in the maritime and energy sectors. Templar Executives, May 1, 2014, http://www. templarexecs.com/cyberresilience/, accessed Feb. 21, 2015.

Osborne, C., 2018. NonPetya ransomware forced Maersk to reinstall 4000 servers, 45000 PCs. Zero Day, Jan. 26, 2018. https://www.zdnet.com/article/maersk-forced-to-reinstall-4000-servers-45000-pcs-due-to-notpetya-attack/, accessed Aug. 6, 2018.

Park, J-Y. 2008. The economic impacts of dirty bomb attacks on the Los Angeles and Long Beach ports: Applying the supply-driven NIEMO (National Interstate Economic Model)." Journal of Homeland Security and Emergency Management 5 (1): Article 21.

Pasternack, A., 2013. To move drugs, traffickers are hacking shipping containers. Motherboard, Oct. 21, 2013. https://motherboard.vice.com/en_us/article/bmjgk8/how-traffickers-hack-shipping-containers-to-move-drugs, accessed Dec. 13, 2017.

Rose, A. (2017). Economic Consequence Analysis of Maritime Cyber Threats. In DiRenzo, J. III, Drumhiller, N., Roberts, F.S. (Eds.). Issues in Maritime Cyber Security. PSO-Westphalia Press, 2017, 321-356.

Rose, A., Wei, D. (2013). Estimating the economic consequences of a port shutdown: The special role of resilience. Economic Systems Reseach 25 (2), 212-232.

Salmon, K. "West Coast Port Congestion Could Cost Retailers $36.9 Billion in the Next 24 Months," Business Wire, Feb. 7, 2015, http://www.businesswire.com/news/home/20150207005007/en/West-Coast-Port-Congestion-Cost-Retailers-36.9#.VPiNIsbA7c8, accessed March 5, 2015.

Segal, A. 2017. How China is preparing for Cyberwar. Christian Science Monitor, March 20, 2017. https://www.csmonitor.com/World/Passcode/Passcode-Voices/2017/0320/How-China-is-preparing-for-cyberwar, accessed Dec. 10, 2017.

The State Council Information Office of the People's Republic of China 2015. China's military strategy. China Daily, 5-26-15. http://www.chinadaily.com.cn/china/2015-05/26/content_20820628.htm. Accessed 12-10-17.

Tucci, A. 2017. Cyber risk management: Preparing for new operational risks. Port Technology Edition 2017, Summer 2017.

Wagstaff, J., 2014. All at sea: Global shipping fleet exposed to hacking threat. Reuters, April 23, 2014. http://www.reuters.com/article/2014/04/23/tech-cybersecurity-shipping-idUSL3N0N402020140423, accessed Feb. 21, 2015.

Werling, J. 2014. The National Impact of a West Coast Port Stoppage. Inforum Report Commissioned by the National Association of Manufacturers and the National Retail Federation, https://www.nam.org/Data-and-Reports/Reports/The-National-Impact-of-a-West-Coast-Port-Stoppage-(Full-Report).pdf, accessed May 14, 2019.

Zaragoza, S. 2014. Spoofing a superyacht at sea. Know, University of Texas at Austin, May 5, 2014.

Zetter, K., 2014. An unprecedented look at Stuxnet, the world's first digital weapon. Wired, Nov. 3, 2014. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ , accessed Dec. 13, 2017.

Zorz, Z., Zorz, M., Kucan, B., 2013. Digital ship pirates: Researchers crack vessel tracking system. Net Help Security, October 16, 2013, http://www.net-security.org/secworld.php?id=15781, accessed Feb. 21, 2015.

Appendix: List of Subject Matter Experts Consulted

CAPT Michael Dickey, USCG
Mark Dubina, Port of Tampa Bay
Casey Hehr, Port of Long Beach (USCG – ret)
CAPT David Moskoff, SUNY Maritime
VADM Rob Parker, USCG-ret
Randy Parsons, Port of Long Beach
Daniel Searforce, Pennsylvania Public Utilities Commission
Drew Schneider, Port of Long Beach
CAPT Andrew Tucci, USCG
CDR Nick Wong, USCG
Michael Young, TSA and Secret Service – ret

Acknowledgements: The authors thank Linda Ness for helpful discussions. They thank the U.S. Department of Homeland Security, Office of University Programs, for partial support under grant number 2009-ST-061-CCI002-08 to Rutgers University, and Fred Roberts thanks the U.S. National Science Foundation for partial support under grant number DMS-1737857 to Rutgers University. The authors thank the subject matter experts listed in the Appendix; much of this paper results from the ideas generously shared by these people.