J. Benefit Cost Anal. 2019; 10(2):251–273
doi:10.1017/bca.2019.15

Fred S. Roberts

From Football to Oil Rigs: Risk Assessment for Combined Cyber and Physical Attacks

Abstract: Although cyber security has become widely recognized as a serious threat to our modern world, there are new threats to our security that combine cyber with other modes of "attack." This article explores the increasingly important theme in homeland and national security that future attacks will be multimodal, in particular including both a cyber and a physical component, where the cyber attack is intended to make it easier to succeed in the physical attack, and is not an end in itself. The article describes sample scenarios of combined cyber and physical attacks in two sectors where even just cyber security efforts have lagged behind: sports stadiums and the maritime transportation system. It presents an approach to comparing the risk of a combined cyber followed by physical attack and that of a "traditional" physical attack on the same target. It then analyzes the different stadium and maritime examples from the point of view of this risk assessment approach.

Keywords: cyber attack; security; stadium security; maritime transportation system; risk assessment.

1 Introduction

I was watching Super Bowl 47 in New Orleans and it was early in the third quarter with Baltimore leading San Francisco 28 to 6. All of a sudden, the lights went out at the stadium with over 70,000 people in attendance. My first thought was: cyber attack!

Our nation's sports stadiums host millions of patrons every year and form the basis for a multibillion dollar industry. Until recently, there was very little awareness of the dangers from cyber attacks at those stadiums. Some of the critical systems in those stadiums are controlled by computer networks. These include security cameras,

Fred S. Roberts, CCICADA Center, Rutgers University, USA, e-mail: froberts@dimacs.rutgers.edu

heating and cooling, elevators and escalators, access control systems for patrons and employees, lighting systems, electronic message boards, public address systems, power systems, and even traffic control in the parking lots. These systems are potentially vulnerable to failures of computer systems or deliberate cyber attacks.

It is not just stadiums that may be vulnerable. Any place where large crowds gather could be a target: airports, train stations, bus terminals, theatres, concert halls, amusement parks, convention centers, even restaurants. Such venues present an inviting target for terrorists, as illustrated by the November 2015 attack on the Stade de France in Paris, the May 2017 attack at an Ariana Grande concert at the Manchester Arena, and the October 2017 attack at a country music concert in Las Vegas.

The power failure at Super Bowl 47 was caused by a relay failing at Entergy New Orleans, not by a cyber attack. However, by the time planning started in 2013 for Super Bowl 48 at MetLife Stadium in New Jersey, a cyber attack was very much on the minds of the planners.

Consider a second example. The failure of a blowout preventer on an oil rig in the Gulf of Mexico in 2010 led to the devastating Deepwater Horizon oil spill, the largest oil spill in U.S. history. That was not due to a cyber attack. However, there have been cyber attacks on oil rigs. According to security company ThetaRay, a cyber attack on a floating oil rig off the coast of Africa managed to tilt the rig slightly and as a result it was forced to shut down. It took a week to identify and fix the problem (Wagstaff, 2014).

In another drilling rig event, in 2010, a drilling rig being moved at sea from South Korea to South America was infected by malicious software. Its critical control systems could not operate and it took 19 days to fix matters (Cyberkeel, 2014, Wagstaff, 2014). The cyber attack infected the computers controlling the blowout preventer, the system at fault for the Deepwater Horizon disaster. The results could have been disastrous.

Oil rigs are part of the massive maritime transportation system (MTS), which includes container ships, cruise ships, barges, ferries, cargo handling systems, port facilities, bridges, and so on. The MTS is critical to the world's economy. A vast majority of the world's commerce goes through the MTS. Interruptions of everyday commerce even for a day or two could create serious shortages of oil, food, pharmaceuticals, and so on, and lead to outages that affect millions of people and cost billions of dollars. During the month of January 2015, the ports on the West Coast of the USA 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 & Wei, 2013, Werling, 2014). Cyber disruptions could have similar outcomes. (For more on the latter, see Rose, 2017.)

A great deal of attention has been paid to the risk of cyber attacks on critical infrastructure such as the power grid, the banking system, and voting/elections. Sport and entertainment venues and the MTS are two cases of critical infrastructure where the risk has not received as much attention until quite recently. We discuss these two areas in detail in this article.

For a long time, the emphasis in the field of security has been on physical security. This is still the major emphasis at stadiums. As we have noted, there is increasing attention being paid to cyber security. However, a more modern way of thinking about security is to think of "combined" attacks that include both a physical and a cyber component. Often the cyber component is not the end in and of itself, but instead is intended to make it easier to achieve success in a physical attack. For instance, if one manages to hack into the electrical power system and turn off the lights in a stadium, this could just be a prelude to attacking the patrons physically. We will consider such combined cyber and physical attacks in what follows. The opposite could also be the case, where the cyber attack is the main goal, but a physical attack sets the stage for the cyber one. An example might be if the physical attack is to break into a computer facility in order to gain access to the computers running some critical stadium process (such as employee access, or fire control), then disabling that process and asking for a ransom to put it back to work. However, we concentrate on a cyber attack as precursor to a physical one.

Tucci (2017) makes a similar point about the MTS. He observes, for example, that hacking into a cyber-enabled security camera could expose a marine terminal to a physical attack. A physical intrusion could allow for installation of keyloggers or other devices that would allow a hacker access to a control system. The paper by Roberts et al. (2019) gives many other examples of both cyber attacks as precursors to physical ones or vice versa.

In both cases, we will discuss examples of cyber attacks, either real or hypothetical, as precursors of physical attacks. Many of these seem feasible. However, even an adversary with a sufficient level of sophistication to pull them off might find it is easier to do a different kind of attack (cyber or physical) leading to the same or worse outcome. 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 the traditional components threat, vulnerability, and consequence in determining the risk of a given attack scenario. Doing a traditional risk assessment of the attack scenarios we discuss is difficult for many reasons. There is a great deal of uncertainty as to the impact of an attack, the ability of the adversary to pull it off, and the mind-set of an adversary that we assume is looking for some combination of the goals of maximizing damage, maximizing probability of success, and minimizing probability of receiving punishment (including death). Traditionally, Risk = Threat × Vulnerability × Consequence. To calculate risk requires all three factors to be accurately estimated. But there are no data on the incidence of cyber attempts on U.S. sporting venues or the MTS (making Threat hard to estimate). Estimates that an attack will succeed (Vulnerability) are essentially speculation. Estimates of Consequences vary from small to large. If they are large, it is important to be able to estimate probabilities accurately, which unfortunately we cannot do with any degree of confidence.

This calls for a new approach to risk assessment for these combined attacks, one that is basically qualitative to start with. In this article, we develop some sample scenarios of combined cyber and physical attacks on sports and entertainment venues (Section 2) and the MTS (Section 3). We then sketch out an approach to risk assessment for such attacks (Section 4), and apply it to the example scenarios we describe (Sections 5 and 6).

2 Sports and entertainment venues

2.1 Some examples of cyber attacks on stadiums

There have been successful cyber attacks on stadiums and sporting events. For example, at the 2017 American Football Conference (AFC) National Football League Championship game, at Gillette Stadium in Foxboro, MA, an adversary hijacked and set off the fire-alarm system. Media were forced to evacuate the stadium (see Thomas, 2017; Cyber Operations, Analysis, and Research, 2017).

A cyber attack disrupted the opening ceremony at the Pyeonchang Winter Olympics in South Korea in February 2018. The cyber attack took out Internet access, affected broadcasting, shut down the Olympic website, and prevented spectators from printing out reservations – leading to many empty seats. What was interesting was that the hackers did not destroy the Olympics' computers. They just demonstrated the ability to do so and left the computers alone, just erasing backup files. This could be interpreted as a political message – which alone should scare people (see Perlroth, 2018).

The Southeast Asian Games are a multisport event for nations in Southeast Asia. A hacker disrupted 30 closed circuit television (CCTV) cameras inside and outside the Singapore Sports Hub just before the closing ceremony of the 2015 games. He used his laptop to gain access to all police CCTV cameras and altered their settings and passwords. This could have placed the lives of attendees at risk. (The attacker had previously been employed by the event and knew the IP addresses, usernames, and passwords. See Cyber Operations, Analysis, and Research, 2017; Hussain, 2016.)

2.2 Some example scenarios

2.2.1 Variants on the attack on the Ariana Grande Concert in Manchester

It is not hard to think of "scenarios" describing combined cyber and physical attacks on stadiums. For example, 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?” The message could tell people to leave the arena immediately, and head to a particular exit.

Alternatively, could a terrorist hack into the fire alarm system, set off the fire alarm, with the result being that the message board automatically sent a message to leave? Or could the fire alarm cause people to panic and leave, whether or not the message board said anything? The attack on the 2017 AFC championship game shows that this is certainly feasible.

These scenarios describe a combined cyber and physical attack. The cyber attack, hacking into the message board or fire alarm system, is just the precursor for the real attack, which is physical.

So how could one defend against this kind of attack? Is there a specific defense against hacking into the fire alarm system or the message board, or more generally against hacking into cyber-physical systems at stadiums, or is it more cost-effective to develop security initiatives to protect people leaving an arena, either at an ordinary time when an event ends or during an emergency? It is hard to see how one would make a quantitative comparison of costs and benefits of these two approaches. What we will try to analyze, however, is whether the risk of a combined attack is higher than the risk of just a physical attack not initiated by a cyber one. We return to this example in Section 5.1.

2.2.2 Using vehicles as weapons at a stadium

As another example, in recent years there has been an increase in use of vehicles as weapons in attacks, in Berlin, Nice, London, and New York. There is increased attention at stadiums on the potential for such attacks at parking lots and loading docks. In such attacks, the attacker usually is committing suicide or has a strong probability of being caught and possibly killed. But what if one could hack into a vehicle and use it for such an attack without actually being in it?

Today’s cars are essentially computers on wheels, with cyber-physical systems controlling much of how a car operates. This makes today’s cars already semiautonomous, taking decisions away from the driver, and thereby frequently aiding in preventing accidents. But could a criminal or terrorist take control of a car remotely through a cyber attack and use it to cause damage? This seems to be a serious challenge as in-car technology becomes more sophisticated. And it is likely to become even more of a challenge as we develop fully autonomous vehicles.

In 2013, Miller (Twitter) and Valasek (IOActive) demonstrated they could take control of a Toyota Prius and a Ford Escape from a laptop (see Greenberg, 2013, for more information). They were able to remotely control the smart steering, braking, displays, acceleration, engine, horn, lights, and so on.

So, is the scenario of an adversary hacking into a car in a crowded stadium parking lot and driving it into the crowd more of a risk than the scenario of a person himself or herself driving the car into the crowd? We return to this question in Section 5.2.

2.2.3 Hacking into a drone at a stadium

The proliferation of drones used for hobby or work or other applications has led to increasing concern about drones near or over sports and entertainment venues. While Federal Aviation Administration (FAA) regulations prohibit flying drones over sports stadiums, that has not prevented hobbyists and those intent on sending a message from doing so. In Fall 2017, a drone flew over Levi's Stadium in California during a football game between the San Francisco 49ers and the Seattle Seahawks, and dropped a payload of leaflets (with a political message). In the Spring of 2017, a drone flown over Petco Park during a San Diego Padres game crashed into a fan. Other incidents have happened at the stadiums of the Dallas Cowboys, Texas Rangers, and the Universities of Nebraska, Missouri, Texas, and Kentucky (see Laris, 2018). In 2015, a drone smashed into the seating area at the U.S. Open Tennis tournament in the U.S. National Tennis Center in Flushing Meadows, NY. Luckily, there were no injuries (see Talanova, 2015).

In these cases, the intent was not to cause harm. However, the potential for deliberate harm certainly exists and presents a serious issue for all owners and operators of large sporting venues. Yet, federal law prohibits most law enforcement agencies from disarming or disabling drones, even if they are in restricted airspace (see Laris, 2018).

Current restrictions (by the FAA and Federal Communications Commission) on drone detection, drone defense, and so on make the only feasible use of drone detection for a stadium the identification of nuisance drones, e.g., those used by hobbyists. National Football League stadiums are starting to invest in such systems, with the goal of identifying the presence of a drone and locating the controller so as to be able to arrest the operator.

Consider an attack where a drone is flown into the stadium to land in the stands. This is a physical attack, not a cyber attack, but there is a scenario that precedes a drone attack with a cyber one, where a “bad guy” hacks into a drone being used for recreation and directs it over a stadium to crash into the crowd and cause direct injury or injury from panic.

Is this joint attack feasible? Professor Todd Humphreys of the University of Texas at Austin has demonstrated how global positioning system (GPS) signals of an unmanned aerial vehicle can be commandeered by an outside source (Cockrell School of Engineering, 2012). So feasibility has already been demonstrated. But is this combined scenario more of a risk than the original physical attack by drone? We return to this question in Section 5.3.

3 The MTS

3.1 Some examples of cyber attacks on the MTS

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. 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 (see Osborne, 2018).

A July 2018 cyber attack on Cosco Shipping Lines that caused failure in its networks in the USA, 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).

Combined cyber attacks on cargo handling systems at the Port of Antwerp and elsewhere are described in Section 3.2.5.

Today's vessels are heavily dependent on cyber systems to navigate, steer, and communicate their positions and other information. Cyber attacks on relevant cyber systems have already taken place. We discuss attacks on the Automatic Identification System (AIS) of vessels in Section 3.2.2 and on the Electronic Chart Display and Information System (ECDIS) of vessels in Section 3.2.3.

3.2 Some example scenarios[1]

3.2.1 Attacks on cyber-physical systems in a port

Modern seaports are sprawling complexes that are heavily dependent on cyber-physical systems (systems that are built from and depend upon the synergy of computational and physical components) to control the gates, the lights, the alarm systems, the cameras, the power supply, the traffic lights, the emergency communication system, and so on. Hacking into any of these systems could create a situation making it easier to have a physical attack – a cyber attack as a precursor to a physical attack, not necessarily as an end in itself. Turning off the lights or cameras or alarms

[1] Most of the example scenarios given in this section were first developed in the papers DiRenzo et al. (2015) and Roberts et al. (2019). The author thanks his colleagues Joe DiRenzo, Dana Goward, Dennis Egan, Christie Nelson, and Ryan Whytlaw for their ideas.

could make it easier for attackers to get in. Sending a faked emergency message could create a distraction, drawing first responders to a distant part of the port and making another part of the port more vulnerable to a physical attack due to most first responders being elsewhere.

Are these scenarios feasible? There is considerable evidence that they are (see Tucci, 2017). But what is the risk of them? Wouldn’t it be easier just to take out the lights or the cameras by physical means? This is the kind of analysis that would be needed in order to do a proper risk assessment, and it involves trying to understand both the capabilities of the “bad guys” and their priorities. We return to this topic in Section 6.1.

3.2.2 Blocking the entryway to a port through attack on the AIS of a vessel

Per International Maritime Organization agreement, AIS transceivers are required on all passenger ships and commercial (nonfishing) ships of a certain size, close to a million ships world-wide. AIS enables ships to share positional data with other ships, providing awareness about those operating within the MTS (Zorz et al., 2013). An attacker could exploit weaknesses in AIS and falsify a vessel’s identity or type, or its position, heading, and speed (Templar Executives, 2014). As pointed out in Cyberkeel (2014) and Balduzzi et al. (2013), such an attack could also create a phony vessel (recognized as real) at any location, trigger a false collision warning system alert (resulting in a course adjustment or worse), or create a false weather report leading a ship to change course. It could also impersonate authorities and trick the crew into disabling their AIS, which would make the ship invisible to authorities and others (except attackers). It could also flood mariner authorities or other vessels with AIS data – a “denial of service” attack (DiRenzo et al., 2015).

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, with AIS giving false locations (see Blake, 2017).

The entry to port through water is often a “chokepoint.” If an adversary could cause a vessel to run aground in the channel leading to the port, this could conceivably block operations at the port for days or weeks or even months. (It took 20 months to get the grounded Costa Concordia off the rocks in 2013 – Mackenzie, 2013.) Closing of a port has significant economic impacts well beyond the port itself. Estimates of the cost of closing a port for a day are not so precise, but most calculations suggest that it is at least a billion dollars a day (see references in the introduction to Section 3). Could this be accomplished via combined cyber and physical attack? One way to accomplish this might be to spoof such a ship’s AIS, arranging no transmission at all, or falsifying the vessel’s identity, type, position, heading, and speed (see Templar Executives, 2014, Zorz et al., 2013). Then the perpetrator could take over the vessel and run it hard aground.

3.2.3 Hacking into a ship’s navigation system

Modern vessels depend critically on the ECDIS and increasingly do not even carry paper charts. Such navigation systems have been hit by cyber attacks. Malware was introduced into the computers of a large 80,000-ton tanker when a crewmember used a USB stick to print some paperwork. Later, a second crewmember 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 (see Baraniuk, 2017).

In 2017, Naval Dome, an Israeli company, showed how much damage it was possible to achieve through an attack on ECDIS. They designed an attack to change a vessel’s position during a “night-time passage through a narrow canal.” The ECDIS display was left looking completely normal but the position, heading, depth, and speed were all displayed in variance from what they actually were. This could have sent the vessel aground (see AJOT, 2017).

Also in 2017, hackers (pirates) reportedly took control of the navigation systems of a container vessel en route from Cyprus to Djibouti. “Suddenly the captain could not manoeuvre. … The IT system of the vessel was completely hacked.” The pirates intended to steer the vessel to an area where they could board and take over (see Blake, 2017).

In 2012, a University of Texas at Austin team showed how to remotely control a vessel by manipulating the part of its electronic navigation system controlled by its GPS. The yacht “White Rose of Drax” was controlled so that “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; UT Austin, 2013).

As a combined scenario, suppose bad actors could hack into the navigation system on a cruise ship. They could cause it to change direction imperceptibly, eventually running it aground. That in turn could be the precursor for a physical attack on the ship.

3.2.4 Hacking into autonomous vessels

Today’s container ships are already essentially autonomous. So much of their operation is run by automated systems that even the largest container ships have minimal crews. Fully autonomous vessels are coming. The systems on such vessels will be monitored from company headquarters. This will allow computers to get early warning of system problems and initiate fixes from headquarters (HQ). But could a hacker take over the HQ computer and thereby hack into the control system on an autonomous vessel, perhaps disabling a sensor designed to identify increasing temperature, pressure, or hazardous gas? This could lead to an explosion and major damage to the vessel itself.

3.2.5 Pirates and cargo

Cargo on today's vessels is tracked from well before it leaves a port of debarkation until it arrives at its final destination. The cargo tracking systems are sophisticated and of essential importance in making the MTS work. There have already been a variety of cases of hacking into cargo tracking systems. A widely cited example involves the Port of Antwerp, one of the world's biggest. During 2011–2013, hackers infiltrated the port's cargo handling system computers. This enabled them to locate specific containers of interest, make off with smuggled drugs, release the containers to their own trucks, and delete the records so their tracks were covered and the shipping companies and the port didn't know it was happening. The hack was achieved by emailing malware to the port authorities and shipping companies. Later, after the hack was discovered and a firewall installed, the criminals found another way to continue, by breaking into the facility and fitting devices allowing wireless access to keystrokes on port/shipping company computers. The first example was a cyber attack that was arranged to make it easier to obtain a physical outcome (stealing cargo) and the second involved a physical attack (break-in) to enable a cyber attack (monitoring keystrokes) to enable the physical attack (stealing) (see Bell, 2013; CyberKeel, 2014; Pasternack, 2013; Wagstaff, 2014; Roberts et al., 2019).

Other examples of cyber attacks on cargo handling systems involved the computers of Australian Customs and Border Protection in 2012 and the computers of the Iranian shipping line IRISL in 2011 (see CyberKeel, 2014).

In a different kind of cyber crime, pirates reportedly hacked into a cargo management system to identify where on a vessel valuable cargo was located. This enabled them to make their raids on vessels faster and therefore less risky, as they could go immediately to the container of interest, causing greater economic consequences than in a "normal" raid where they just took what was easy to take (see Hand, 2016; Baraniuk, 2017). Some people have cast doubt as to whether this really happened. Just because you know where on a vessel a given container of interest is, how can you quickly get to it when other containers might be piled on top of it? Of course, perhaps it is also feasible to hack into the cargo handling system and arrange for a container of interest to be piled on top. The relative risk of such a combined cyber and physical raid will be discussed in Section 6.5.

4 A risk assessment approach

There does not seem to be a relevant literature on risk assessment for combined attacks where one attack is intended to make a second attack more successful. The Federal Emergency Management Agency (FEMA) has provided guidance on complex, coordinated terrorist attacks, with a section on risk assessment (Department of Homeland Security, 2018). However, the discussion is about attacks “that involve synchronized and independent team(s) at multiple locations, sequentially or in close succession, initiated with little or no warning, and employing one or more weapon systems: firearms, explosives, fire as a weapon, and other nontraditional attack methodologies that are intended to result in large numbers of casualties.” This doesn’t seem relevant and the risk assessment discussion is very generic, referring to the need for communities to identify potential threats and hazards, describe scenarios for how these threats and hazards might affect the community, and understanding their potential consequences. There is a literature on event trees that involves related events and finding the probability of a sequence of events by multiplying probabilities of events along a branch (see, e.g., U.S. Bureau of Reclamation, Security, Safety, and Law Enforcement Office – Dam Safety, 2015). There is a literature on multi-hazard assessment that includes discussion of cascading effects, when one type of threat could be the result of another. However, that literature is mainly concerned with things like one natural event like an earthquake triggering another natural event like a landslide (see, e.g., Liu et al., 2015). Finally, there is a literature on risk assessment for “combined events,” but that is essentially concerned with multiple events occurring essentially simultaneously, but somewhat independently (see, e.g., Helander, 2017).

There has been a long literature on the question of whether terrorists can be assumed to be acting rationally, which includes a discussion of the hypothesis that terrorists are maximizing expected utility in their decision-making. Some relevant references on this topic are Caplan (2006), Davis and Cragin (2009), Kydd and Walter (2006), Nalbandov (2013), and Rosoff and John (2009). Rational behavior does not require calculation of detailed utility values, especially when decisions need to be made under considerable uncertainty. The same can be said of risk assessment. What we sketch here is an approach that is essentially qualitative in nature, and that assumes the adversary will act rationally at least in a qualitative sense.

Specifically, we explore the simple case where an attacker is deciding between two alternative attacks. In particular, one is a joint attack J that starts with a cyber attack A that ends with/leads to a physical attack B. The other is a “traditional” physical attack T that aims at the same kind of damage, so where B and T are fairly similar. We seek a relative risk assessment, is J more of a risk to us as a defender than T, or vice versa? This comes down to an assessment of whether an attacker will be more likely to choose J over T, or vice versa.

In principle, the first step is the same whether J is a joint attack or not. Specifically, we will assume that, all things being equal, the (rational) attacker prefers J over T if the (estimated) probability P_J that J will succeed is greater than the (estimated) probability P_T that T will succeed; prefers J over T if the (estimated) cost K_J of J is less than the (estimated) cost K_T of T; and prefers J to T if the (estimated) consequence

Table 1 Eight cases comparing combined cyber and physical attack J to physical attack T.

Case no.	Probability of success	Cost	Consequence
1	$P_J > P_T$	$K_J < K_T$	$C_J > C_T$
2	$P_J > P_T$	$K_J < K_T$	$C_J < C_T$
3	$P_J > P_T$	$K_J > K_T$	$C_J > C_T$
4	$P_J > P_T$	$K_J > K_T$	$C_J < C_T$
5	$P_J < P_T$	$K_J < K_T$	$C_J > C_T$
6	$P_J < P_T$	$K_J < K_T$	$C_J < C_T$
7	$P_J < P_T$	$K_J > K_T$	$C_J > C_T$
8	$P_J < P_T$	$K_J > K_T$	$C_J < C_T$

C_J of J is greater than the (estimated) consequence C_T of T. (How consequence is measured is not relevant for this discussion. P is proxy for vulnerability, C stands for consequence, and K is a very simplified way for threat.) Of course, parameters such as P_J, K_J, C_J, and so on are really distributions, but we will treat them as point values. Where the new complexity comes in is in calculating (at least a ballpark) level for P_J, K_J, and C_J for combined events. For instance, if J is A followed by B, if it were possible to do a quantitative assessment, we would need to figure out the probability P_A that A is a success and then the conditional probability $P_{B/A}$ that B is a success given that A is a success. P_J is $P_A \times P_{B/A}$. However, all we try to accomplish here is to get a ballpark idea of whether $P_A \times P_{B/A} > P_T$. To understand P_A, we need to understand whether or not A is feasible, which is likely to involve ideas from subject matter experts, both cyber security experts and either stadium or maritime experts. Understanding $P_{B/A}$ will also require input from stadium or maritime experts. In both cases, what we present below has benefited from discussions with such experts.

We will also assume that the major goal of the adversary is to create some damage (physical, economic, psychological), and so even if C_J is less than C_T, the adversary might still prefer J to T if $P_J > P_T$ and $K_J < K_T$.

To begin, we consider the eight cases shown in Table 1.

Cases 1 and 8 are straightforward. In Case 1, the adversary would seem to prefer J over T, so the risk of J is greater than the risk of T. In Case 8, the adversary would seem to prefer T over J, so the risk of J is less than the risk of T. The other cases are interesting and require a second level of analysis, for example, the investigation of the absolute differences $|P_J - P_T|$, $|K_J - K_T|$, and $|C_J - C_T|$.

Again, we will simply be qualitative in our analysis – quantitative analysis of such gaps is questionable at best – and so we simply describe them as “small” or “large.” These would in some sense be determined by a threshold p, k, or c, respectively, and by the idea that we would consider the difference between two values to be unimportant if the values are within threshold. Of course, the thresholds are not really going to be independent of each other. Based on our assumption that the adversary will be satisfied with some damage, even if not as much as possible with an alternative attack, we can assume that c is relatively large, and that in most cases of interest, $|C_J - C_T| < c$. Thus, in most cases, we would conclude for example that Cases 1 and 2 are essentially equivalent for the adversary, and so the adversary would seem to prefer J over T in Case 2, or that at least the risk of J is higher than that of T. Similarly, Cases 7 and 8 are essentially equivalent for the adversary, and so they would seem to prefer T over J in Case 7. Similarly, Cases 3 and 4 are essentially equivalent and also Cases 5 and 6. There are some subtleties, however. For example, one can imagine a situation in Case 7 where the adversary would choose J over T if $|P_J - P_T|$ and $|K_J - K_T|$ are both relatively small, so long as $C_J - C_T$ is sufficiently large.

If the values in two of the columns of the table are within threshold we may want to let the inequality in the remaining column determine whether or not J is judged more likely than T. The same is true if we are unsure of whether the inequality is > or < in two of the columns of the table. Thus, for example, if $|K_J - K_T| < k$ and $|C_J - C_T| < c$, we would conclude that J is preferred to T if and only if $P_J > P_T$. Similarly, if we are not sure if $K_J > K_T$ or the reverse, and unsure if $C_J > C_T$ or the reverse, we would conclude that J is preferred to T if and only if $P_J > P_T$. The exception to this might be in cases where we don't know whether or not $C_J > C_T$ or the reverse, but think they are probably close. Then if the column we do feel comfortable about has $P_J < P_T$ or $K_J > K_T$, we might still think that the adversary would prefer J, if the major goal of the adversary is to create some sort of damage.

In the following, we will return to the scenarios J described earlier and for each describe what an alternative T would be and discuss which of these cases would seem to apply. The discussion is intended to illustrate possible reasoning using ideas sketched above, and not intended to be definitive in any way. We aim mostly to explore the types of reasoning that might be used to compare risk. A much more detailed analysis would be required in each case, with input from subject matter experts. The discussion is based mostly on ideas from experts obtained in preparing the article Roberts et al. (2019).

5 Applications of the ideas to example scenarios: sports and entertainment venues

5.1 Variants on the attack on the Ariana Grande Concert in Manchester

As noted in Section 2.1, the attack on the 2017 AFC championship game shows that it is certainly feasible to hack into the fire alarm at a stadium. This could lead to an automatic message on the message board. It seems likely that hacking into the message board itself is also quite feasible. Thus, a cyber attack that would get people to leave all at the same time seems like it could be accomplished fairly easily, making p_A relatively high. In turn, a successful cyber attack A would make the likelihood of a successful physical attack on departing patrons at least as high as the likelihood of a successful physical attack on the departing patrons at the end of a game, so $P_{B/A} \geq P_T$. It is reasonable to guess that the joint attack would lead to at least as many casualties as the ordinary physical attack, and might even lead to more casualties in the joint case, since there could very well be panic and people getting hurt even without the physical attack, so $C_J \geq C_T$. Even though $P_{B/A} \geq P_T$, it is possible that $P_J = P_A \times P_{B/A} < P_T$, but as long as P_A is quite high, most likely, P_J and P_T are close. Thus, $|P_J - P_T| < p$. Moreover, there is an added cost to the cyber attack so $K_J > K_T$, but it is likely that the added cost of the cyber part of J is small, relatively speaking, so $|K_J - K_T| < k$. Since $|P_J - P_T| < p$, $|K_J - K_T| < k$, and $C_J \geq C_T$, this suggests that the adversary will prefer J and that the case of the combined attack has a higher risk than the case of the noncombined attack, although maybe not much higher.

5.2 Using vehicles as weapons at a stadium

A vehicle ramming attack has become attractive to attackers because it can be done by individuals with limited training or experience. That is certainly not the case if the attack is performed through hacking into a vehicle. So the risk becomes very different because one type of attack calls for much more sophistication than the other. The probability of success of the joint attack may thus be lower than that of the person-driven attack because of this, but maybe not. Maybe it's easier to defend against the person-driven attack because of behavioral and other screening in the parking lot, making it harder to succeed. That suggests that we don't know whether or not $P_J > P_T$. If the value of the life of a driver is considered, we have $K_J < K_T$. We also don't know if $C_J > C_T$ or the reverse. Hence, we would be best off assuming that J would be chosen because it is less costly, and so J would be rated a higher risk. On the other hand, if we assume that the attacker doesn't care about human life, then maybe $K_J > K_T$ because the hacking part of J might take more of an investment. Still, as long as we think that C_J and C_T are relatively close, we would think J to be more likely the adversary's preferred choice because of the adversary's preference to some damage even if the attack is less likely to succeed or more costly. In short, based on best guesses, whether or not we think the adversary values human life, we conclude that the combined attack involving hacking into a car should be rated a higher risk.

5.3 Hacking into a drone at a stadium

The probability of a drone getting past drone defense at a stadium, whether it is being flown by an operator or instead it is hacked and flown by a hacker, might be relatively similar. Thus, $P_{B/A}$ and P_T are close. However, the probability P_A of successful hacking is likely to be quite a bit less than 1, in which case $P_J = P_A \times P_{B/A}$ is likely less than P_T, perhaps quite a bit less. Depending upon the cost of buying a drone as opposed to buying equipment to hack into the drone, we might have $K_j > K_T$ or $K_J < K_T$. However, the costs are probably modest in both cases, so most likely $|K_J - K_T| < k$. The consequences in both cases are likely about the same, so $|C_J - C_T| < c$. This suggests that the adversary is likely to prefer T because the probability of success is higher. We conclude that the joint attack is probably less of a risk than the original attack. There is another consideration here. If a "bad guy" were to control a drone, he or she could load it with an explosive device, leading to much more damage. This would not be doable through hacking into someone else's drone. So there is a scenario T′ different from T that would be much preferred by a "bad guy" even to the T that we started with and certainly to the J as described. This suggests that the risk of the joint attack J is probably low.

6 Applications of the ideas to example scenarios: The MTS

6.1 Attacks on cyber-physical systems in a port

There are differences in difficulty and feasibility of cyber attacks for different systems in a port, and also differences in how effective such attacks would be in allowing for a physical attack. One key question in assessing the risk of these attacks involves the question: 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. Clearly in all cases, $P_{B/A} > P_T$ – that is the whole point of knocking out cameras, lights, emergency communications, alarms, gates, and so on. If P_A is high and $|P_{B/A} - P_T|$ is high, then it is likely that $P_J > P_T$. Let us take various cyber attacks A one at a time. Since cameras are often add-ons, it is likely that P_A is high. Once cameras are knocked out, the probability of success of a physical attack on a part of a port should go up significantly. Hence, one has to guess that $|P_{B/A} - P_T|$ is high and $P_J > P_T$. It is also possible that the cost of the physical attack will go down if it is aided by lack of a camera system, but in any case it should not be much different than without the cameras, so $|K_J - K_T| < k$. Finally, the consequences of the physical attack without cameras are likely to be at least as high as they would be with cameras in tact, i.e., $C_J > C_T$. In short, it would seem that the joint attack initiated with taking out the cameras in a port is of higher risk than one not initiated that way.

Things are a bit different with attacks on the lights or the alarm system. A Denial of Service Attack could take out the lights or the alarm system. However, port security might more quickly realize there was a problem than with an attack on the cameras. It is still likely, as with cameras, that $P_J > P_T$, $|K_J - K_T| < k$, and $C_J > C_T$. Thus, the risk is higher with the joint scenario – although perhaps not as high as the risk of the joint scenario initiated by taking out the cameras, where the difference $|P_J - P_T|$ might be higher since P_A may be higher with the cameras.

What about a cyber attack on the emergency communications system as the preliminary attack, sending first responders away from the location of a following physical attack? The ability to hack into the emergency communications system depends upon how it is configured. If it is connected to the Internet, it is certainly possible. Jamming communications might be easier. One subject matter expert 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. In either case, P_A is moderately high. But because port security would be alert to a potential attack quickly, the difference between $P_{B/A}$ and P_T would not be so great, and it could very well be that $P_A \times P_{B/A} < P_T$. This suggests that this kind of joint attack could be much less of a risk than the attacks initiated with a cyber attack on the cameras, lights, or alarm system, and perhaps even less of a risk overall than the plain physical attack.

Finally, consider a joint attack initiated by unlocking the gates by cyber. 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 attackers wouldn't buy much time and so the likelihood of their trying it might be small. We would likely have $P_J < P_T$, as with the emergency communications case, and the risk of this kind of joint attack would again be much less than the risk of a joint attack starting with taking out the cameras, lights, or alarm system.

6.2 Blocking the entryway to a port through attack on the AIS of a vessel

In October 2013, Balduzzi et al. (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. You could also spoof a ship's AIS to arrange it so awareness systems are not transmitting a problem.

The complex attack of concern is to spoof a ship’s AIS to arrange it so awareness systems are not transmitting a problem, by falsifying information about the vessel so as to hide problems. This cyber attack would then allow a “bad guy” to take over the vessel and run it aground. It is unlikely defenders could interdict the vessel once it was happening even if they caught on. There are few options except to ram the vessel running out of control – which could also cause an explosion. Let us compare this joint attack to the attack T of physically taking over the vessel in the approach to a port and trying to run it aground. It is not easy to think of a scenario for T that would make the probability of success P_T very high, so it is likely that P_J is quite a bit bigger than P_T. The cost K_J is likely also quite a bit lower than K_T for any conceivable T. The consequence of running the vessel hard aground would be similar in either case. So clearly J seems much more likely than T, and the risk of J is judged higher than the risk of T. However, how high is the risk even for J? In a port, a pilot vessel is likely to be taking control of the vessel, and the pilot would likely give early warning of deviation from expected/traditional trajectory. This makes the probability of success of J seem smaller than perhaps a first analysis suggests, and so perhaps *J* does not have a very high risk.

6.3 Hacking into a ship’s navigation system

In the combined scenario of interest, bad actors could hack into the navigation system on a cruise ship, and cause it to change direction imperceptibly, eventually running it aground. That in turn would be the precursor for a physical attack on the ship. Let us compare that to physically attacking the cruise ship while it is in motion. In Section 3.2.3, we show that there is considerable evidence that it is possible to successfully hack into the ECDIS system and cause a vessel to careen off course. It is quite possible that if the attackers spoofed a ship’s ECDIS, they could alter charts, hiding what shoal waters exist, leading to grounding of the vessel in a desired area. So the probability of success of the cyber part of the joint attack could be fairly high. However, the physical attack on a grounded ship might not be so likely to succeed, since first responders would likely be on the scene quickly. Thus, if T is an attack on the vessel in the open ocean, the probability $P_{B/A}$ might not be much greater than P_T, and we might even have $P_{B/A} < P_T$. Even if $P_{B/A} > P_T$, $P_A \times P_{B/A}$ might be less than P_T if P_A is not so high. The consequences of each kind of attack could be large, both in terms of loss of life and damage to the vessel, but also in the impact on the cruise ship industry of a successful attack, so it is likely that $|C_J - C_T| < c$. The cost K_J would be less than the cost K_T, since it would be easier to attack a grounded vessel. If we think that $P_J < P_T$, then determination of whether or not J is risker than T would come down to the tradeoff between the lower probability of success of J and the lower cost of J. If we are not sure whether or not $P_J < P_T$, then the lower cost of J suggests that J would be judged a higher risk than T. It should be noted that even if A succeeds but J fails, the result could be a major economic blow to the cruise ship industry. So even without human casualties, there would be a major effect of the cyber attack of grounding the ship. It should also be noted that using an attack on the navigation system to move the ship out of a well-traveled shipping lane might make it easier to succeed in attacking it. This suggests that this alternative joint scenario is perhaps more likely than the given one, making assessment of the risk of the joint scenario ending in grounding not as high as it might have been if there were no such alternative scenario. Assessment of risk should always take into account whether or not the adversary has a “better” alternative.

6.4 Hacking into autonomous vessels

Here we consider a scenario where a hacker attacks the control system on an autonomous vessel through a computer at corporate headquarters, disabling a sensor designed to identify increasing temperature, pressure, or hazardous gas, leading to an explosion and major damage to the vessel itself. Is this feasible? Maybe so. 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). The company Naval Dome has demonstrated how an attack could penetrate a vessel’s machinery control system and stop the valves and pumps from working (see AJOT, 2017). Doing so through a corporate HQ computer seems feasible. So we have a joint attack J where the cyber attack A leads automatically to a physical explosion B. Let us compare this scenario to finding a way to physically disable a sensor as part of a two-pronged physical attack T, with a physical attack X to disable a sensor followed by the explosion B. It is likely that $P_{B/A}$ and $P_{B/X}$ are similar, while P_A may be quite a bit higher than P_X, and so P_J may be quite a bit higher than P_T. The cost K_J might also be much less than the cost K_T. The consequences C_J and C_T are likely the same. This suggests that J is much more likely than T and that the risk of J is considerably higher.

6.5 Pirates and cargo

Here we discuss the joint attack where pirates first hack into the cargo management system to arrange for easy accessibility of containers with valuable cargo, making their physical attack to steal cargo faster and less risky to them. Is this really feasible? A recent article (Maritime Executive, 2017) points out that penetration testing experts Pen Test Partners show how hackers could manipulate the loading data of its hull stress monitoring systems. In this demonstration, the goal was to show how hackers could deliberately cause an imbalance of cargo on a vessel that could lead to it eventually breaking up and sinking. But the same idea would apply to the deliberate placement of cargo of interest. So, if T is an attack of boarding a ship and physically stealing cargo, $P_{\mathrm{B/A}}$ and P_{T} are the same and P_{J} is less than P_{T}, since P_{A} is less than 1. However, for pirates with sophisticated hacking ability, P_{A} might be relatively high, and so P_{J} and P_{T} might be relatively close. Also, K_{J} may be a bit higher than K_{T}, taking into account the cost of the cyber attack. However, C_{J} is much higher than C_{T}. We are in Case 7, but as noted earlier, in this case, the adversary could choose J over T if $|P_{\mathrm{J}} - P_{\mathrm{T}}|$ and $|K_{\mathrm{J}} - K_{\mathrm{T}}|$ are both relatively small, so long as $C_{\mathrm{J}} - C_{\mathrm{T}}$ is sufficiently large. Here, it is likely that a cyber-sophisticated adversary would choose J over T, and we conclude that J could be more of a risk than T.

7 Closing remarks

Combined cyber and physical attacks, whether on a large sports and entertainment venue, the MTS, or some other infrastructure, are clearly a risk one must take into account. A very initial approach to risk assessment of such attacks like the one we have presented here shows that. The development of scenarios of such joint attacks is a first step in laying the groundwork for additional analysis. That needs to continue. Moreover, there is clearly need for a more sophisticated theory of risk for such attacks to be developed.

Acknowledgements: This article was part of a project funded by the Searle Freedom Trust in an award to George Washington University. The author thanks Dennis Egan, Christie Nelson, and Ryan Whytlaw for many discussions that led to the paper Roberts et al. (2019) in which many of the MTS sample scenarios were described. He also thanks the following subject matter experts who provided a great deal of information about MTS scenarios: 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-ret; CDR Nick Wong, USCG; and Michael Young, TSA-ret and Secret Service-ret.

References

AJOT. 2017. "Cyber Penetration Tests Underscore Maritime Industry's Nightmare Security Scenario" *American Journal of Transportation*. https://www.ajot.com/news/cyber-penetration-tests-underscore-maritime-industrys-nightmare-security-sc.

Balduzzi, Marco, Kyle Wilhoit and Alessandro Pasta. 2013. "Hey Captain, Where's Your Ship? Attacking Vessel Tracking Systems for Fun and Profit," In *11th Annual HITB Security Conference in Asia,* October 2013. Available at 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 February 21, 2015)

Baraniuk, Chris. 2017. "How Hackers Are Targeting the Shipping Industry." Available at: https://www.bbc.com/news/technology-40685821. (accessed August 6, 2018)

Bell, Steve. 2013. "Cyber-attacks and Underground Activities in Port of Antwerp." Available at: http://www.bullguard.com/blog/2013/10/cyber-attacks-and-underground-activities-in-port-of-antwerp.html. (accessed February 21, 2015)

Bhatti, Jahshan and Todd E. Humphreys. 2014. "Covert Control of Surface Vessels Via Counterfeit Surface GPS Signals." Unpublished. https://pdfs.semanticscholar.org/6f20/450b32b71f2454e63292acb632d3619ee8ef.pdf. (accessed December 12, 2017)

Blake, Tanya. 2017. "Hackers Took 'Full Control' Of Container Ship's Navigation Systems For 10 Hours." *ASKET Ltd. Maritime Security News and Updates*, November 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.

Caplan, B. 2006. "Terrorism: The Relevance of the Rational Choice Model." *The Political Economy of Terrorism*, 128: 91–107.

Cockrell School of Engineering. 2012. "Todd Humphreys' Research Team Demonstrates First Successful Spoofing of UAV." *The University of Texas at Austin Aerospace and Engineering Mechanics News*, June 12, 2012. http://www.ae.utexas.edu/news/504-todd-humphreys-research-team-demonstrates-first-successful-uav-spoofing. (accessed December 28, 2017)

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

Cyber Operations, Analysis, and Research. 2017. "Cyber-Tabletop Exercises for Sports-Entertainment Venues." Argonne National Laboratories. Available at https://coar.risc.anl.gov/cyber-tabletop-exercises-for-sports-entertainment-venues/. (accessed August 2, 2018).

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

Davis, Paul K. and Kim Cragin (Eds.). 2009. "Social Science for Counterterrorism. Putting the Pieces, Together." *RAND Corporation Monograph Series, 170*. http://www.rand.org/pubs/monographs/2009/RAND_MG849.pdf.

Department of Homeland Security, 2018. Planning Considerations: Complex, Coordinated Terrorist Attacks, July 2018, Available at https://www.fema.gov/media-library-data/1532550673102-c4846f270150682decbda99b37524ca6/Planning_Considerations-Complex_Coordinated_Terrorist_Attacks.pdf. (accessed October 14, 2018)

DiRenzo, Joseph III, Nicole K. Drumhiller, and Fred S. Roberts, eds. 2017. Issues in Maritime Cyber Security. Washington, DC: PSO-Westphalia Press.

DiRenzo, Joseph III, Dana A. Goward and Fred S. Roberts. 2015. “The Little-Known Challenge of Maritime Cyber Security,” in *Proceedings of the 6th International Conference on Information, Intelligence, Systems and Applications (IISA),* pp. 1–5, IEEE. https://doi.org/10.1109/IISA.2015.7388071.

Greenberg, Andy. 2013. “Hackers Reveal Nasty New Car Attacks – With Me Behind the Wheel.” *Forbes*, August 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 December 11, 2017)

Hand, Marcus. 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.

Helander, Juho. 2017. “Identification and Analysis of External Event Combinations for Hanhikivi 1 PRA.” *Nuclear Engineering and Technology*, 49: 380–386.

Hussain, Amir. 2016. “Engineer Gets 8 Months’ Jail For Hacking Into Police CCTV Cameras At Sea Games 2015.” *The Straits Times*, August 16, 2016. http://www.straitstimes.com/singapore/courts-crime/engineer-gets-8-months-jail-for-hacking-into-police-cctv-cameras-at-sea-games.

Kydd, Andrew and Barbara Walter. 2006. “The Strategies of Terrorism.” *International Security*, 31: 49–80.

Laris, Michael. 2018. “Stadium and Team Owners See Drones As Major League Threat.” *Chicago Tribune*, May 11, 2018. http://www.chicagotribune.com/sports/breaking/ct-spt-drones-theats-to-sports-stadiums-20180511-story.html#.

Liu, Zhongqiang, Farrokh Nadim, Alexander Garcia-Aristizabal, Arnaud Mignan, Kevin Fleming and Byron Quan Luna. 2015. “A Three-Level Framework for Multi-Risk Assessment.” *Georisk: Assessment and Management of Risk for Engineered Systems and Geohazards*, 9(2): 59–74, https://doi.org/10.1080/17499518.2015.1041989.

Mackenzie, James. 2013. “Wrecked Cruise Ship Costa Concordia Raised off Italian Rocks.” Reuters, September 16, 2013. https://www.reuters.com/article/us-italy-ship/wrecked-cruise-ship-costa-concordia-raised-off-italian-rocks-idUSBRE98F02T20130917. (accessed December 13, 2017)

Maritime Executive. (2017). “Hackers Could Sink A Bulk Carrier.” *The Maritime Executive*, December 20, 2017. https://www.maritime-executive.com/article/hackers-could-sink-a-bulk-carrier#gs.ZogtZZo.

Mongelluzzo, Bill. 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.

Nalbandov, Robert. 2013. “Irrational Rationality of Terrorism.” *Journal of Strategic Security*, 6: 92–102, http://dx.doi.org/10.5038/1944-0472.6.4.5. (accessed October 16, 2018)

Osborne, Charlie. 2018. “NonPetya Ransomware Forced Maersk To Reinstall 4000 Servers, 45000 PCs.” *ZDNet*, January 26, 2018, https://www.zdnet.com/article/maersk-forced-to-reinstall-4000-servers-45000-pcs-due-to-notpetya-attack/. (accessed August 6, 2018)

Park, Jiyoung. 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), https://doi.org/10.2202/1547-7355.1312.

Pasternack, Alex. 2013. "To Move Drugs, Traffickers Are Hacking Shipping Containers." *Motherboard*, October 21, 2013. https://motherboard.vice.com/en_us/article/bmjgk8/how-traffickers-hack-shipping-containers-to-move-drugs. (accessed December13, 2017)

Perlroth, Nicole. 2018. "Cyberattack Caused Olympic Opening Ceremony Disruption." *New York Times*, February 12, 2018, https://www.nytimes.com/2018/02/12/technology/winter-olympic-games-hack.html.

Roberts, Fred S., Dennis Egan, Christie Nelson and Ryan Whytlaw. 2019. "Combined Cyber and Physical Attacks on the Maritime Transportation System", *Journal of the NATO Maritime Interdiction Operational Training Centre* (to appear).

Rose, Adam. 2017. "Economic Consequence Analysis of Maritime Cyber Threats." In DiRenzo, Joseph III, Nicole K. Drumhiller and Fred S. Roberts (Eds.) *Issues in Maritime Cyber Security*: 321–356. Washington, DC: PSO-Westphalia Press.

Rose, Adam and Dan Wei. 2013. "Estimating the Economic Consequences of a Port Shutdown: The Special Role of Resilience." *Economic Systems Research*, 25(2): 212–232.

Rosoff, Heather and Richard S. John. 2009. "Decision Analysis by Proxy for the Rational Terrorist," In *Proceedings of the 21st International Joint Conference on Artificial Intelligence (IJCAI-09), Workshop on Quantitative Risk Analysis for Security Applications (QRASA),* Pasadena, California, July 11–17.

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

Templar Executives. 2014. "Cyber Resilience in the Maritime and Energy Sectors." *Templar Executives*, May 1, 2014, https://www.templarexecs.com/cyberresilience/. (accessed February 21, 2015)

Talanova, Julia. 2015. "Drone Slams into Seating Area at U.S. Open; Teacher Arrested." *Cnn.com*, September 5, 2015. https://www.cnn.com/2015/09/04/us/us-open-tennis-drone-arrest/index.html. (accessed August 6, 2018)

Thomas, Jeanna. 2017. "Gillette Stadium Evacuated for Fire Alarm Prior to Steelers vs. Patriots." *SBNation*, January 22, 2017. http://www.sbnation.com/2017/1/22/14350196/boston-man-sets-off-fire-alarms-at-steelers-hotel-before-championship-game-vs-patriots. (accessed August 2, 2018)

Tucci, Andrew. 2017. "Cyber Risk Management: Preparing for New Operational Risks." *Port Technology International Journal*, 74: 90–92.

U.S. Bureau of Reclamation, Security, Safety, and Law Enforcement Office – Dam Safety. 2015. Risk Management: Best Practices and Risk Methodology: Chapter A-5, Event Trees, May 7, 2015. Available at https://www.usbr.gov/ssle/damsafety/risk/methodology.html. (accessed May 14, 2019)

UT Austin. 2013. "UT Austin Researchers Successfully Spoof an $80 Million Yacht at Sea." *UT News*, July 29, 2013, https://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea/. (accessed June 26, 2019)

Wagstaff, Jeremy. 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 February 21, 2015)

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

Zetter, Kim. 2014. "An Unprecedented Look at Stuxnet, The World's First Digital Weapon." *Wired*, November 3, 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/. (accessed December 13, 2017)

Zorz, Zeljka, Mirko Zorz and Berislav Kucan. 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 February 21, 2015)