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

Fred S. Roberts

The George Washington University Regulatory Studies Center

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 multi-billion 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, HVAC, 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.

---

1 This working paper reflects the views of the author, and does not represent an official position of the GW Regulatory Studies Center or the George Washington University. The Center’s policy on research integrity is available at http://regulatorystudies.columbian.gwu.edu/policy-research-integrity.

2 Fred S. Roberts is Director of the Command, Control, and Interoperability Center for Advanced Data Analysis and Distinguished Professor of Mathematics at Rutgers University.
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 US 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.\(^3\)

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.\(^4\) 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, etc. 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, etc., 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 United States were closed due to a labor stoppage and the impact on the economy was dramatic.\(^5\) 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.\(^6\) Cyber disruptions could have similar outcomes.\(^7\)

---

\(^3\) Wagstaff, 2014.
\(^5\) Salmon, 2015.
\(^7\) 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 maritime transportation system 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 paper.

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 maritime transportation system. 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 (2018) 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 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 x Vulnerability x Consequence. To calculate risk requires all three factors to be accurately estimated. But there is no data on the incidence of cyber attempts on US 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 paper, we develop some sample scenarios of combined cyber and physical attacks on sports and entertainment venues (Sec. 2) and the maritime transportation system (Sec. 3). We then sketch out an approach to risk assessment for such attacks (Sec. 4), and apply it to the example scenarios we describe (Secs. 5 & 6).

2. Some Example of Cyber Attacks on Stadiums

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 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.\(^8\)

A cyber attack disrupted the opening ceremony at the Pyeongchang 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.\(^9\)

The Southeast Asian Games are a multi-sport event for nations in Southeast Asia. A hacker disrupted 30 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.)\(^10\)

---

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 Sec. 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 you 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 semi-autonomous, taking decisions away from the driver, and thereby frequently aiding in preventing accidents. But could a criminal or terrorist take control of your 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.\textsuperscript{11} They were able to remotely control the smart steering, braking, displays, acceleration, engine, horn, lights, etc.

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 him- or herself driving the car into the crowd? We return to this question in Sec. 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 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.\textsuperscript{12} In 2015, a drone smashed into the seating area at the US Open Tennis tournament in the US National Tennis Center in Flushing Meadows, NY. Luckily, there were no injuries.\textsuperscript{13}

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.\textsuperscript{14}

Current restrictions (by the FAA and FCC) on drone detection, drone defense, etc. make the only feasible use of drone detection for a stadium the identification of nuisance drones, e.g., those used by hobbyists. NFL 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.

\textsuperscript{11} See Greenberg, 2013, for more information.
\textsuperscript{12} See Laris, 2018.
\textsuperscript{13} See Talanova, 2015.
\textsuperscript{14} See Laris, 2018.
Is this joint attack feasible? Professor Todd Humphreys of UT Austin has demonstrated how global positioning system (GPS) signals of an unmanned aerial vehicle can be commandeered by an outside source\(^{15}\). 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 Sec. 5.3.

3. The Maritime Transportation System

3.1 Some Examples of Cyber Attacks on the Maritime Transportation System

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.\(^{16}\)

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.\(^{17}\)

Combined cyber attacks on cargo handling systems at the Port of Antwerp and elsewhere are described in Sec. 3.2.6.

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 Sec. 3.2.3 and on the Electronic Chart Display and Information System (ECDIS) of vessels in Sec. 3.2.4.

3.2 Some Example Scenarios\(^{18}\)

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

---

\(^{15}\) Cockrell School of Engineering, 2012.

\(^{16}\) See Osborne, 2018.

\(^{17}\) See Mongelluzzo, 2018.

\(^{18}\) Most of the example scenarios given in this section were first developed in the papers DiRenzo, et al (2015) and Roberts, et al (2018). The author thanks his colleagues Joe DiRenzo, Dana Goward, Dennis Egan, Christie Nelson, and Ryan Whytlaw for their ideas.
traffic lights, the emergency communication system, etc. 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 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. 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 Sec. 6.1.

### 3.2.2 Lines of Trucks at Ports

Anyone who has visited a port knows that there are long lines of trucks waiting to deliver cargo. The scheduling of trucks picking up or delivering containers at a port is controlled by a cyber system. Could a cyber attack on the scheduling system cause large traffic jams in the area? Could a physical attack somewhere in the port (say with an explosive device) then follow, with the traffic jams making it harder for emergency vehicles to get through? Will this type of joint attack be any more effective than a 2-part physical attack to the same end, with an explosive device in the middle of the truck lineup to damage some of the trucks and create the traffic jam, followed by an explosive device set off somewhere in the port?

### 3.2.3 Blocking the Entryway to a Port through Attack on the Automatic Identification System of a Vessel

Per International Maritime Organization agreement, Automatic Identification System (AIS) transceivers are required on all passenger ships and commercial (non-fishing) 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. An attacker could exploit weaknesses in AIS and falsify a vessel’s identity or type, or its position, heading, and speed. 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

---

19 See Tucci, 2017.
21 Mullin, 2014.
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.\(^\text{22}\)

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.\(^\text{23}\)

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\(^\text{24}\)) 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.\(^\text{25}\) 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.\(^\text{26}\) Then the perpetrator could take over the vessel and run it hard aground.

### 3.2.4 Hacking into a Ship’s Navigation System

Modern vessels depend critically on the Electronic Chart Display and Information System (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 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.\(^\text{27}\)

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.\(^\text{28}\)

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

---

\(^{22}\) DiRenzo, et al., 2015.

\(^{23}\) See Blake, 2017.

\(^{24}\) Mackenzie, 2013.

\(^{25}\) See references in the introduction to Sec. 3.


\(^{27}\) See Baraniuk, 2017.

\(^{28}\) See AJOT, 2017.
system of the vessel was completely hacked.” The pirates intended to steer the vessel to an area where they could board and take over.29

In 2012, a UT 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”30.

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.

3.2.5 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 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.

3.2.6 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).31

29 See Blake, 2017.
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.\textsuperscript{32}

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.\textsuperscript{33} 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 Sec. 6.6.

3.2.7 Debarking in a Cruise Ship Terminal

In present practice, passengers debark from a returning cruise ship in groups to avoid crowding and long lines at customs. A cruise ship scenario analogous to the Ariana Grande concert scenario discussed in Sec. 2.2.1 would seek to change this. Here, an attacker would hack into a cruise ship terminal’s fire alarm system, aiming to get all passengers to debark at once – leading to the vulnerabilities about exiting from a cruise ship terminal analogous to those upon exiting a stadium. The issues involved in doing a risk assessment of this scenario are similar to those in the stadium example, except that there is already a long history of placing staff to help direct exiting patrons in this case and not so much in the stadium case.

3.2.8 Fire Alarm on a Cruise Ship at Sea

The cruise ship industry is a multi-billion dollar industry. Passengers on a modern cruise ship want all the services they are used to onshore: email, Internet access to shop or plan their offshore activities, entertainment systems, not to mention air conditioning, heat, etc. The cruise ship industry is well aware of the risks of a cyber attack on a ship’s operating system carried out through one of the passenger systems, and so has emphasized firewalls between the two types of systems. However, there are other ways in which a cruise ship could be targeted.

We talked in the previous section about hacking into a fire alarm at a cruise ship terminal. What if an attacker could hack into the fire alarm on a cruise ship at sea? In such a case, passengers would muster at boat stations. This could make them vulnerable to a physical attack at those stations – a cyber attack as the predecessor to a physical one. But here again we ask, would an attacker actually work to accomplish this? Wouldn’t it be easier to pull off a physical attack at some part of the

\textsuperscript{32} See CyberKeel, 2014.
\textsuperscript{33} See Hand, 2016 and Baraniuk, 2017.
vessel where passengers gather, e.g., a dining room, without going to the trouble of hacking into a fire alarm system?

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. FEMA has provided guidance on complex, coordinated terrorist attacks, with a section on risk assessment. 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. 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. 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.

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. 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

36 See e.g., Liu, et al, 2015.
37 See e.g., Helander, 2017.
38 Some relevant references on this topic are Caplan (2006), Davis and Cragin (2009), Kydd and Walter (2006), Nalbandov (2013), and Rosoff and John (2009).
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 $C_J$ 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 for
consequence, and K in a very simplified way for threat.) Of course, parameters such as $P_J$, $K_J$, $C_J$,
etc. 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 a
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 eight cases:

<table>
<thead>
<tr>
<th>Case #</th>
<th>Probability of Success</th>
<th>Cost</th>
<th>Consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$P_J &gt; P_T$</td>
<td>$K_J &lt; K_T$</td>
<td>$C_J &gt; C_T$</td>
</tr>
<tr>
<td>2</td>
<td>$P_J &gt; P_T$</td>
<td>$K_J &lt; K_T$</td>
<td>$C_J &lt; C_T$</td>
</tr>
<tr>
<td>3</td>
<td>$P_J &gt; P_T$</td>
<td>$K_J &gt; K_T$</td>
<td>$C_J &gt; C_T$</td>
</tr>
<tr>
<td>4</td>
<td>$P_J &gt; P_T$</td>
<td>$K_J &gt; K_T$</td>
<td>$C_J &lt; C_T$</td>
</tr>
<tr>
<td>5</td>
<td>$P_J &lt; P_T$</td>
<td>$K_J &lt; K_T$</td>
<td>$C_J &gt; C_T$</td>
</tr>
<tr>
<td>6</td>
<td>$P_J &lt; P_T$</td>
<td>$K_J &lt; K_T$</td>
<td>$C_J &lt; C_T$</td>
</tr>
<tr>
<td>7</td>
<td>$P_J &lt; P_T$</td>
<td>$K_J &gt; K_T$</td>
<td>$C_J &gt; C_T$</td>
</tr>
<tr>
<td>8</td>
<td>$P_J &lt; P_T$</td>
<td>$K_J &gt; K_T$</td>
<td>$C_J &lt; C_T$</td>
</tr>
</tbody>
</table>
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, e.g., 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 of 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 report Roberts, et al. (2018).
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 Sec. 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 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 $C_J \geq C_T$, and 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 non-combined attack, though 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 Maritime Transportation System

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, etc. 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 – though 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 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. 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, light, 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 Lines of Trucks in Ports

In this example, we are considering a joint cyber-physical attack, hacking into the truck scheduling system (A) followed by a physical attack B in the port, one that emergency vehicles couldn’t respond to due to resulting traffic jams. We are comparing this to a two-part physical attack T where the first part X involves an explosive device to create the traffic jams and the second part is attack B. Now \( P_T = P_X \times P_{B/X}. \) It seems quite likely that after the first explosion aimed to create the traffic jam by damaging trucks on line, authorities would become more vigilant, making the likelihood \( P_{B/X} \) smaller than \( P_{B/A}. \) We don’t know whether or not \( P_A > P_X. \) If it is, then \( P_J > P_T. \) If it isn’t, the judgment of whether or not \( P_J > P_T \) is hard to make using simply qualitative considerations. Since costs of J and T may be close and similarly consequences, it seems that the probability of success of J vs T will determine the risk. We judge J to be more of a risk than T if we judge \( P_A > P_X, \) but are not sure if J is more of a risk than T if we judge \( P_A < P_X. \)
6.3 Blocking the Entryway to a Port through Attack on the Automatic Identification System of a Vessel

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. 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 Automatic Identification System (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.

6.4 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, 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 Sec. 3.2.4, 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 or 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 riskier 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.

6.5 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. 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. 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 \( P_{X/A} \) 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.

6.6 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 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 which could lead to it eventually

\[40\] See AJOT, 2017.
\[41\] Maritime Executive, 2017.
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, \( P_{B/A} \) 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 above, but as noted earlier, in this case, the adversary could 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. 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 \( T \).

### 6.7 Debarking in a Cruise Ship Terminal

Here we consider a cruise ship scenario where an attacker hacks into a cruise ship terminal’s fire alarm system, aiming to get all passengers to debark at once – leading to a successful attack on debarking passengers. The feasibility of the cyber attack might depend upon whether the alarm system were online. Port fire alarm systems are designed to operate over a network and push a signal out to a monitoring agency and hacking into this system might be quite a bit harder than physically setting off the fire alarm. Thus, a two-pronged physical attack \( T \) that starts with a physical attack \( X \) on the alarm system and ends with a physical attack \( B \) on the debarking passengers has a higher probability of success than the joint attack starting with a cyber attack \( A \) on the alarm system and ending with a physical attack \( B \). That is because \( P_{B/A} \) is about the same as \( P_{B/X} \), but \( P_A < P_X \) and so \( P_J < P_T \). It is hard to tell if \( K_J \) is less than \( K_T \) or vice versa. However, \( C_J \) would seem to be similar to \( C_T \). Because there are people trained to direct passengers where to go in case of a fire alarm, this could minimize the possibility of serious consequences of either \( J \) or \( T \). In short, with small consequences, probably neither \( J \) nor \( T \) are of very high risk, and because \( P_J < P_T \), \( J \) presents a smaller risk than \( T \).

### 6.8 Fire Alarm on a Cruise Ship

Here we move from an attacker hacking into the fire alarm in a cruise terminal to hacking into the fire alarm on the cruise ship while at sea. In this joint attack \( J \), when passengers would muster at boat stations, the attacker performs a physical attack \( B \) on a large group of them. We compare \( J \) to a physical attack on passengers in the dining room, without a predecessor fire alarm. Here we have to compare the probability of success of physically attacking passengers at boat stations, under the potential chaos of a fire alarm, with the probability of success of physically attacking them while they dine, \( T \). Perhaps \( P_{B/A} > P_T \), because of the location of the passengers out on the deck and because of the potential chaos and distraction caused to security personnel. If \( P_A \) is large enough, then perhaps \( P_J > P_T \). The costs \( K_A \) and \( K_T \) are perhaps not that different, so \(|K_J - K_T| < k \). The number of casualties might be smaller with \( J \) because there would be a smaller group at an individual boat station, but even though \( C_J \) is smaller than \( C_T \), it is still high enough that \(|C_J - C_T| < c \). By our reasoning above, 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 more
likely than T. Thus, as long as we think that $P_A$ is sufficiently high, we conclude that $P_J > P_T$, and so we think that J has a higher risk than T.

It should be noted that just hacking into the fire alarm system without the physical attack could be another scenario. An attacker could do this multiple times, totally disrupting a cruise. Or the attacker could simply do it once and announce that they had done it, threatening to do so the next time with serious physical consequences. There would likely be major loss of business for the cruise line (or all cruise lines) in the future. There would then be no risk of loss of life for the attackers, and so could possibly be a preferred alternative for them, making this new scenario higher risk than the joint scenario.

Suppose for example that E is the attack of hacking into the fire alarm system, announcing it was done, and threatening to do so the next time with physical consequences. Since $P_E = P_A$, we have $P_E > P_J$. It is likely that $P_E$ will also be higher than $P_T$. Clearly $K_E < K_J$, $K_E < K_T$. It is very possible that the economic costs of E could be quite close to those either J or T if loss of life is minimal, i.e., $|C_E - C_J|$ and $|C_E - C_T|$ are small. Thus, because $P_E > P_J$ and $K_E < K_J$, E seems to be of higher risk than J, at least if we don’t think the passenger loss of life from J would be very high. For similar reasons, E seems to be of higher risk than J. This also follows since J is seen as higher risk than T. There are some subtleties here. How much the adversary values the life of its own people might also enter into the analysis, since if it doesn’t place high value on their lives, then it is possible that $K_E$ and $K_J$ (as well as $K_E$ and $K_T$) are close, and so in the case where the adversary believes there is a good chance for large loss of life for passengers, we would rate J (and perhaps T) as higher risk than E.

Defending against the two scenarios E and J would start in the same way, with defense against a hack into the fire alarm system. Moreover, given a fire alarm, it would be wise to at least consider the possibility of the joint attack, because for the attackers who don’t put such a high value on their own lives, the joint attack would very possibly be preferred. It could likely lead to a much higher consequence than just the fire alarm attack because of passenger casualties.

7. Closing Remarks

Combined cyber and physical attacks, whether on a large sports and entertainment venue, the maritime transportation system, 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.
References


