RISK ASSESSMENT FOR INTEGRATED CYBER AND PHYSICAL ATTACKS ON CRITICAL INFRASTRUCTURE

Alok Baveja, Supply Chain Management, Rutgers University, 100 Rockafeller Road, Piscataway, NJ 08854, 848-445-9219, baveja@business.rutgers.edu

John Betak, Collaborative Solutions, LLC, 726-23 Tramway Vista Drive NE, Albuquerque, NM 87122, 505-238-8143, john@collaborativesolutionsllc.com

Dennis Egan, CCICADA Center, Rutgers University, 96 Frelinghuysen Road, Piscataway, NJ 08854, 848-445-4576, deegan@dimacs.rutgers.edu

Peter March, Mathematics, Rutgers University, Hill Center-Busch Campus, 110 Frelinghuysen Road, Piscataway, NJ 08854, 848-445-2390, pm630@math.rutgers,edu

Christie Nelson, CCICADA Center, Rutgers University, 96 Frelinghuysen Road, Piscataway, NJ 08854 848-445-5928, cnelson@dimacs.rutgers.edu

Fred Roberts, CCICADA Center, Rutgers University, 96 Frelinghuysen Road, Piscataway, NJ 08854, 848-445-4303, froberts@dimacs.rutgers.edu

Andrew Tucci, US Coast Guard (Ret.), Guilford, CT, 203-240-7273 andrew.e.tucci42@gmail.com

Ryan Whytlaw, CCICADA Center, Rutgers University, 96 Frelinghuysen Road, Piscataway, NJ 08854 908-309-5459, rwhytlaw@gmail.com

ABSTRACT

We address the homeland security theme that future attacks might be multimodal, with cyber and physical components, where one component is designed to increase the likelihood of success of another. Current risk assessment methodologies assess cyber or physical risks separately, potentially underestimating risk of integrated attacks, leading to non-optimal selection of security and mitigation measures. We provide sample scenarios of integrated cyber and physical attacks for critical infrastructures: the maritime transportation system, railroads, sports/entertainment venues, and power systems. We review approaches to risk assessment of integrated attacks and illustrate ways to obtain relative risk rankings by comparing integrated to non-integrated.

Keywords: Cyber-Physical Attack, Maritime Transportation System, Sports and Entertainment Venues, Railroads, Power Systems.

INTRODUCTION

There is increasing concern among security experts about terrorist or criminal attacks on critical infrastruacture that are multimodal, for example, with a cyber and a physical component. One of these attack components is intended to make the target more vulnerable and raise the possibility of a more successful second (main) attack component. This paper will discuss such integrated attacks across multiple critical infrastructure sectors, namely the maritime transportation system, railroads, sports and entertainment venues, and power systems. Commonly used risk assessment methodologies may not recognize or evaluate the risk of integrated cyber and physical attacks on critical infrastructure, which leads to underestimating risk. Such a risk miscalibration can lead to a non-optimal selection of security and mitigation measures. We will discuss the need for new tools for understanding and identifying how such attacks might occur, new methods to generate a rigorous understanding of the threats, vulnerabilities, and consequences of these attacks. Such tools will help assess risks for such complex attacks and assist in identifying countermeasures to minimize the risk of these kinds of attacks. We provide specific example scenarios of integrated cyber and physical attacks in the selected critical infrastructure sectors, develop methods to examine the threats, vulnerabilities, and consequences of integrated attacks on the maritime transportation system (MTS), sports and entertainment venues, railroads, and power systems. We also provide recommendations we hope will be useful to critical infrastructure stakeholders such as the Department of Homeland Security (DHS), the US Coast Guard (USCG), professional sports leagues, the Cybersecurity and Infrastructure Security Agency (CISA), and the Transportation Security Administration (TSA).

BACKGROUND

Experts now recognize that "conventional" warfare of the future will include attacks in both the cyber and physical domains. Indeed, publicly available military strategy from China (see Segal, 2017), The State Council Information Office of the People's Republic of China 2015), indicates that the Chinese military expects to seize information dominance at the beginning of a physical conflict through cyber-attacks.

Similarly, future terrorist or criminal attacks on critical infrastructure will likely be multimodal, with both a cyber and a physical component, where, for example, the cyber-attack is intended to increase the probability of success of a subsequent physical attack and is not an end in itself (Tucci, 2017).

Depoy et al. (2005) explored physical and cyber-attacks against critical infrastructure and introduced the concepts of cyber-enabled physical attacks and physical-enabled cyber-attacks that are in the same spirit as the ones we are considering in this work. It concurs with our viewpoint that existing risk assessment methodologies do not accurately account for such integrated attacks.

For example, hacking into security cameras at a port increases vulnerability to physical intrusion. Cyber-attacks could be used before, during, or after a physical attack to heighten vulnerability, magnify consequences, or hamper response and recovery actions. An adversary could also exploit a physical security vulnerability to install a keylogger or gain physical access to vital cyber systems to prepare for subsequent cyber or integrated attacks. While this paper will emphasize the cyber first, physical second model, there is also a need to consider other types of integrated attacks, including physical first, cyber second.

As part of a university-Coast Guard maritime cyber security initiative, a previous study involving some of the authors of this work led to the question of how the USCG, or a vessel or facility operator, could identify and evaluate potential synergies between cyber and physical vulnerabilities to result in a holistic security risk assessment, including consequence management. This work discussed a variety of scenarios of combined or integrated cyber and physical attacks and the beginning of understanding their likelihood based on the ease of attack and seriousness of potential consequences (Roberts et al., 2019).

Similar ideas were explored for sports and entertainment stadiums (Roberts, 2019). For example, the 2017 attack at the Ariana Grande concert in the Manchester Arena showed that people 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 rail transportation system (including freight, long-distance passenger, or metrorail) provides an example of how cyber technology, such as positive train control (PTC) or the European Rail Train Management System (ERTMS), has improved performance and reliability. But such novel technology can create new vulnerabilities. A recent ENISA report (ENISA, 2023) highlights the increasing global risks and attacks on rail systems, including multiple attacks in the US. To date, these attacks have largely been on IT systems, but Operational Technology system attacks are increasing in number, including those initiated by state actors. Could hacking into the ERTMS, PTC, or the signaling system lead to a locomotive stopping at an isolated location, making it easier for a coordinated physical attack to succeed? Or could it lead trains to collide head-on, as happened recently in Greece? And what if one of those trains were carrying hazardous cargo? (See Swain, 2022 for this and similar examples.)

An integrated cyber-physical risk management approach is also needed for power generation, transmission, and distribution. While many experts have analyzed cyber risks to the electric grid, physical risks are less commonly investigated. This lack of attention to physical attack is despite power systems having considerable physical vulnerabilities, as seen in December 2022 attacks in North Carolina and Washington State. It is reasonable to assume that an integrated cyber-physical attack would have magnified the negative consequences in those situations. And if it were carried out while authorities were focusing on an approaching natural event like a hurricane, with personnel and materials deployed elsewhere, things could be even worse.

While ships and ports, railroads, power systems, and sports arenas all have their unique risks, they all include cyber and physical elements that must be viewed as part of one system requiring a balanced and integrated approach in risk analysis, prevention, protection, response, and recovery. These critical sectors also interact with each other, making power system attacks and railroad attacks directly relevant to ports. For some stadiums, an attack would also affect a port (e.g., San Francisco Oracle Park, which is directly on the waterfront).

RISK ASSESSMENT FOR INTEGRATED CYBER AND PHYSICAL ATTACKS: RELEVANT WORK

Regardless of the cause, risk analysis requires considering a range of factors across a scenario timeline,

from monitoring or pre-attack surveillance to post-attack response and recovery, including the challenges of restoring faith in a compromised system. These general principles apply to all risk analysis reviews, including those for integrated cyber-physical attacks. However, as noted, commonly used risk assessment methodologies may not recognize or evaluate the risk of integrated cyber and physical attacks on critical infrastructure, which leads to underestimating risk and non-optimal selection of security and mitigation measures.

There is limited literature on risk assessment for integrated attacks where one attack is intended to make a second attack more successful, which is one major motivation for this paper. FEMA has provided guidance for risk assessment on coordinated/complex terrorist attacks (Department of Homeland Security, 2018). However, the focus is on 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." Given the generic nature of the risk assessment, these types of scenarios do not seem particularly relevant to the problem we are addressing. It only refers to goals of threat/hazard and consequence identification, along with the use of scenarios to understand hazard impacts. Event-tree literature deals with multiplying probabilities of a sequence of events along a tree branch (U.S. Bureau of Reclamation, Security, Safety, and Law Enforcement Office, 2015). The multi-hazard assessment literature (e.g., Liu, et al., 2015), Moini & Betak, 2014) studies the case of one threat resulting in another but mostly concentrates on impacts of natural events like heavy rainfall resulting in mudslides. The "combined events" risk assessment literature (e.g., Helander, 2017) concentrates on events that are essentially independent and occur at the same time, as opposed to the integrated attacks with which we are concerned.

Adams, Chisnall, Pickering & Schauer (2020) describe the EU'S SAURON Project hybrid situational awareness tool, designed to provide situational awareness of "combined" cyber-physical attacks on a port. It uses inputs from the physical and cyber domains, analyzes their interdependencies, and develops tools to show decision-makers the potential consequences, including cascading effects. Though the tool is aimed at situational awareness, not risk assessment, it will be useful in the development of scenarios and a risk model.

As noted earlier, Depoy et al. (2005) has a motivation very close to ours. That paper presents an "automated" methodology for ranking the risk of different kinds of threats, using water infrastructure as an example. It goes into great detail to describe the different assets of an infrastructure facility that might be attacked, using an engineering process model and aims to produce a relative ranking of those assets that might need additional protection. It discusses ways to identify consequences "of concern," assesses threats using different attributes an attacker might need for a successful attack, and then seeks a quantitative measure for asset vulnerability.

There is significant literature on threats to cyber-physical systems, which allow for integrated attacks due to the close relationship between cyber and physical. A number of articles in this literature have picked up the terminology cyber-enabled physical and physically-enabled cyber of Depoy et al. (2005). For example, Tsigkanos et al. (2018) provide a "speculative threat assessment" method based on modeling the evolution of topological configurations of cyber and physical systems. However, this is very specific

to particular types of models of cyber and physical systems. Nguyen et al,.(2020) and Tsigkanos, Kehrer, & Ghezzi (2016) pick up the terminology for various types of cyber-physical systems, such as the power grid, but do not consider risk assessments.

EXAMPLE SCENARIOS

A National Academy of Sciences review of DHS risk assessment methods (National Research Council, 2010) pointed out that "Effective risk analysis need not always be quantitative. In particular, the generation and analysis of scenarios is an important component of risk assessment and management in a number of fields." As a first step in risk identification, our work has compiled a database of plausible scenarios of integrated cyber and physical attacks in each of the four critical infrastructure areas of emphasis. Some examples of these types of scenarios we have developed are presented next.

MTS Scenarios

Example 1: Port Facilities

Cyber-physical systems in port facilities are designed to control gates, lights, alarm systems, traffic lights, power, and communication systems. Hacking into any of these systems could increase a facility's vulnerability to and/or magnify the consequences of a physical attack (Adams et al. 2020, Roberts et al., 2019). Turning off the lights, cameras, or alarms could make it easier for physical attackers to get in. A spoofed message could direct guards to allow access to malicious personnel and/or vehicles or to misdirect cargo. Similar techniques could create a series of false alarms, desensitizing guards to actual events, or misdirect security and emergency responders away from the actual target area. Cyber-attacks on Terminal Operating Systems or truck scheduling systems could significantly slow cargo movement and create crowds of trucks and personnel (in a predictable time and location) that could be the target of subsequent physical attacks.

Example 2: Vessel Operating Systems

Malicious actors could introduce malware into navigation, cargo, ballast, or engine management systems in a variety of ways. This could be done remotely or as part of a software/firmware update done onboard by insiders or by outsiders gaining access via social engineering and weaknesses in a vessel's physical security and credentialing procedures. Regardless of the methodology, attackers could initiate cyber actions at a time and place of their choosing, such as when the vessel navigates through narrow channels or conducts ballast, cargo, or passenger operations. Distracted and perhaps disabled by the unexplained problems, a vessel would be especially vulnerable to physical attacks, even if fail-safe systems prevented immediate, catastrophic results from the cyber actions alone.

Cyber vulnerabilities and threats to vessel operating systems are well documented. Deliberate hacking into the ECDIS (Electronic Chart Display and Information System) has been demonstrated to work (AJOT, 2017, (Bhatti & Humphreys, 2014, Zaragoza, 2014)). Blake (2017) gives an example of pirates taking control of a container vessel's navigation system. AIS (Automatic Identification System) lacks authentication and is vulnerable to manipulation impacting vessel type, position, heading, and speed (Templar Executives, 2014), Zorz, Zorz & Kucan, 2013). Examples of AIS spoofing in the Black Seaaffecting multiple ships and leading to false location information are discussed in Blake (2017). Such an attack outside a U.S. port area would stop or slow normal activity, creating backlogs that could be exploited or combined with physical attacks on port infrastructure and other supply chain elements, including rail.

Sports and Entertainment Venue Scenarios

Example 1: Hacking into Vehicles at a Stadium

People travel to stadiums by vehicles, which have demonstrated cyber vulnerabilities to vital systems. One study demonstrates how to take control of a vehicle from a laptop and control key systems, including displays, acceleration, braking, and steering (Greenberg, 2013). Terrorists could disable one or more vehicles on the roadways approaching a stadium before or after a game, possibly causing deaths or injuries and adding to the already heavy congestion. The terrorists could then attack the large congregation of people, or ambush emergency responders, using conventional weapons.

Example 2: Jumbotron and Drones

Drones could be flown into stadium areas, perhaps only causing minor direct damage but creating a sense of panic among spectators. If a terrorist also hacked into public information displays and address systems, they could direct the public towards an ambush, leading to many casualties. In 2017, a drone flew over Levi's Stadium during a football game between the San Francisco 49ers and the Seattle Seahawks, dropping a payload of leaflets. There are also other examples of drones flying over or crashing into fans at major league baseball and college football games (Laris, 2018), and a drone has even crashed into the stands at the U.S. Open Tennis tournament in New York (Talanova, 2015). Hacking into the Jumbotron seems feasible. In a rail-related incident in 2021, hackers in Iran managed to get into the displays nationwide and showed rail passengers false information, making this a plausible scenario (Swain, 2022). In a related rail scenario like the Ariana Grande example in Manchester mentioned earlier, imagine that hackers take control of the display system in a large terminal and send everyone to the same track with a message that a train is about to leave early. The stampedes alone could cause major physical damage, but if some bad actors were waiting with weapons or bombs, things could be much worse.

Railroad Scenarios

Example 1: Hackers Disable a Tunnel Pumping and Draining System

Trains go through many tunnels, including some very long ones (e.g., the one under the Hudson River into New York). These tunnels require pumping and draining controlled by cyber-physical systems, especially after storms. What if a bad actor not only used a cyber-attack to disable a pumping and draining system but also ensured that status boards indicated that the tunnel was safe? Such a scenario could lead to a train getting stuck or key systems being flooded, with the lights and AC going out, leading to serious injury to passengers (Monteagudo, 2021). Physical attacks on track sections on either side of the tunnel could further trap the train and its passengers.

Example 2: Control of Signaling Systems Causes a Direct Train Collision

Consider a situation where a bad actor takes control of a signaling or switching system for a railroad and directs two trains to travel on the same track toward each other, leading to a head-on collision as occurred recently in Greece. Such a scenario is not unrealistic. In 2022, hackers in Belarus took control of routing and switching devices to stop trains and also threatened to take down signaling and emergency control systems. Similarly, in 2022, hackers in Denmark attacked an ICT service provider for DSB (the Danish national rail company), impacting the accessibility of a key safety-critical IT system, thereby disrupting DSB operations for several hours (Bastow, 2014, ENISA, 2023, Roth, 2022), Swain, 2022)). As with the tunnel scenario, these cyber actions could create damage and confusion while placing trains in locations where follow-up physical attacks could then occur. This problem could be further exacerbated if the trains were carrying hazardous materials.

Power System Scenarios

Example 1: Deliberate Blackouts Leading to Explosions Damaging Power Systems

In 2015 Russian hackers were able to gain access to the control systems of three power distribution companies in Ukraine, cause a blackout that left over 230,000 people without power for several hours, and then use the chaos to carry out physical attacks on the power grid infrastructure that included cutting power lines and using explosives to damage power stations (Lee, Assante & Conway, 2016, E-ISAC, 2016, Council on Foreign Relations, 2017). The December 2022 physical attack on the power grid in North Carolina left thousands without power for many days. Had that attack occurred in conjunction with a cyber-attack, the outage would have likely been longer and more widespread, with greater public fear and loss of confidence. Some smaller power stations, known as “peakers,” are primarily used only when demand is very high and the grid is already stressed. Hackers could monitor routine communications among power generators to determine when extra power was needed and then conduct a physical, cyber, or integrated attack when the system was most vulnerable.

Example 2: Cyber Attacks Lead to Physical Attacks on a Pipeline

A 2021 ransomware attack on the Colonial Pipeline led to fuel shortages across five states and panic buying of fuel in many areas. Had the ransomware been accompanied by an even small physical attack, it would have required extra physical security and response measures across many miles of pumping stations and pipelines and a longer restoration time. An attacker with different motives might have used the cyber access they gained to plan carefully targeted physical attacks on the pipeline rather than request a ransom. Refineries and tank farms in port areas face similar scenarios.

DEVELOPING METHODS OF RISK ASSESSMENT

While the above scenarios may be plausible, they are merely examples and do not help agencies or critical infrastructure owners prioritize the threats and associated security investments or help develop specific mitigation strategies. Integrated cyber-physical risk modeling should consider the traditional components of Threat, Vulnerability, and Consequence in determining the risk of a given attack scenario (CISA, 2020). Conducting a traditional risk assessment of scenarios like the ones of interest to us in this work is difficult for many reasons. Given the unknowns around the adversary's capabilities and motivations, uncertainty plays into the situation and the overall impact of such an attack.

Traditionally, Risk = Threat x Vulnerability x Consequence, with Threat further defined as a combination of an adversary's capability and intent, and calculating such risk requires an accurate estimation of the factors. But there is little or no data for cyber attempts on U.S. power systems, the MTS, sporting venues, or the rail system, making Threat hard to estimate. Indeed, this is largely the realm of intelligence agencies and services. Depoy et al. (2005) provides estimates of threat that depend on different kinds of attributes of an attacker but aims just for high, medium, or low capabilities. There are many challenges in estimating Vulnerability (attack success probability). While papers such as Depoy et al. (2005) aim to provide quantitative vulnerability estimates, this requires an assessment of physical and/or cyber preventive measures or measures to mitigate against asset failure. Depoy et al. (2005) discuss the calculation of the probability of a successful cyber or physical or integrated attack with probability estimates and approach cyber-enabled physical attacks, for example, by reducing to zero the time required for physical penetration of infrastructure if a cyber-attack is successful. Our approach is different. Since the assessment of threats is qualitative, we aim, as a start, to find qualitative estimates of vulnerability, too, since statements combining qualitative and quantitative scales can be meaningless, in a precise sense of the word (Roberts, 2016). Also, Tversky & Kahneman (1974) argue that qualitative comparisons under uncertainty are less likely to lead to errors. There are many types of Consequences that can be small or extremely large. If they are large, we would need to estimate probabilities accurately, which is extremely difficult. If there are human life, economic, environmental,

and psychological consequences, combining them quantitatively into one measure may not be feasible. One approach is to analyze the combinations of asset failures that could lead to sufficiently concerning Consequences (Depoy et al., 2005), but that requires a detailed analysis of complex cyber-physical systems and understanding what failures might lead to what consequences. All of this leads us to take a different approach to risk assessments for such types of integrated attacks.

Roberts (2019) has outlined the basic structure of a potential risk assessment approach for integrated attacks. The approach does not address Threat factors directly other than acknowledging that adversaries capable of integrated attacks exist and will seek targets where the likelihood of success and maximizing damage is high. It does, however, take into account the cost of an attack to a bad actor, which, of course, is related to the Threat. Vulnerability may be viewed in the context of a specific attack mode against a specific target; for example, a truck attempting to crash through a gate or a spear phishing attack targeting a specific individual via social engineering. Perceived Vulnerability would invite attacks; decreased Vulnerability would incentivize alternative attack methods or targets. A simple risk analysis might discount specific Threats because the apparent Vulnerability or Consequences of an attack are low. A comprehensive model recognizes that an attack could be just one segment in a broader plan to increase Vulnerability or magnify the Consequences of subsequent events.

To illustrate some of our ideas, we suppose that an attacker is deciding between an integrated attack, I, using a cyber-attack, A, to enable a physical attack, B, or just using a physical attack, X, aiming at the same kind of damage. Which has higher risk, I or X? Obviously, an attacker prefers an attack with a higher probability of success, lower cost, and higher consequences. But there are tradeoffs, especially when these probabilities, costs, or consequences are relatively close to one another. Let P_I and P_X be the probabilities of I and X being successful, K_I and K_X be the costs of I and X, and C_I and C_X the consequences. We can treat P as a proxy for Vulnerability, C as one for Consequence, and K as one for Threat (though this is quite a simplified approach to Threat).

Let us consider the stadium examples to illustrate how an analysis of relative risk might be done. In the jumbotron/drone example, we first observe that hacking into the message board (attack A) seems quite feasible. Indeed, hacking into a fire alarm took place at the AFC Championship football game in 2017 (Thomas, 2017), and such alarms resulted in an automated message on the Jumbotron. Hence, the probability of A, P_A, would seem to be high. A successful attack A telling people to leave the stadium would very likely make attack B at the gates at least as successful as an attack X at the gates as people were leaving after a game. This makes the conditional probability $P_{B/A}$ of B being successful given A occurs at least as high as P_X. Of course, P_I could still be less than P_X, since $P_I = P_A \times P_{B/A}$, but since P_A is high, P_I and P_X would seem to be close. Moreover, the consequences of I would seem at least as great as those of X and possibly much higher. In addition to people getting hurt outside the stadium, many could be hurt in a stampede for the exits if an alarm message appears on the Jumbotron. While the cost of I is higher than that of X since it includes both types of attacks, the cost of A would seem to be relatively

low, and thus K_I and K_X might be similar. In summary, since C_I might be much higher than C_X and P_I and P_X and also since K_I and K_X are likely close, the risk of I might be higher than that of X.

Consider next the vehicle hacking example at a stadium roadway. Here we compare the integrated attack starting with a remote hack into a vehicle (attack A) resulting in a physical attack (B) on the resulting crowded roadway, as opposed to an attack R using a driver-initiated vehicle-driven ramming leading to the same physical attack B on people in the crowded roadway. Here, we compare two integrated attacks, I (A followed by B) and X (R followed by B). In this case, the key issue is whether the attacker is willing to risk their life in attack X. Surely, conditional probability $P_{B/A}$ is likely to be close to conditional probability $P_{B/R}$. But how do P_A and P_R compare? P_R depends on such defenses at the stadium as behavioral assessment of drivers and vehicle screening on roadway approaches. P_A might decrease as modern cars become more like computers on wheels, with appropriate regular cyber-defense updates. But since many cars remain in service for many years, it may be quite a while before P_A decreases significantly. So, we don't know how high either P_A or P_R is, we don't know whether or not P_I or P_X is higher. Surely C_I and C_X are likely to be close. If the attacker doesn't care about being killed, then perhaps K_I is less than K_X in that case. This suggests that under this assumption unless we know more about P_A and P_R, we would think that I is more of a risk than X.

CLOSING REMARKS

How can one best prevent these kinds of integrated attacks or minimize their impacts? And how can one compare the value of investing in one kind of countermeasure or another, either pre-attack or post-attack? Useful resources here are Narayanan et al. (2020) and National Academies (2017) for the power grid, National Academies (2016) for rail, and CISA (2023) for the MTS. For instance, in our first example, one should investigate questions like: Is there a specific defense against hacking into the Jumbotron at a stadium, or more generally against hacking into cyber-physical systems at the stadium, or is it more cost-effective to develop security initiatives to protect people from a physical attack? It would seem to be much more difficult to compare the benefits and costs of these two approaches quantitatively than qualitatively. A key first step is to make comparisons of relative risk, as we have done here.

Integrated cyber and physical attacks on critical infrastructure clearly present a complex risk. Our discussion has been limited to a single pair of cyber and physical events. One can imagine more complicated situations with multiple events. An attack on a cruise ship could be followed by an attack on a second cruise ship or simply the threat of such a second or third attack. There could also be cascading impacts of events. An attack on a power system that shuts down the power for a period of time could leave other systems that depend on power vulnerable, for example. The development of relevant scenarios for these kinds of situations is called for as groundwork for the development of methods of risk assessment appropriate for these complex situations. In our opinion, detailed scenario building

coupled with rigorous comparative qualitative analysis provides an innovative methodology for assessing and prioritizing risk, which can help in better allocating resources for preventing and responding to cyber and physical threats.

ACKNOWLEDGMENT

This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number 17STQAC00001-01-02.

DISCLAIMER

The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security.

REFERENCES

N.P.H. Adams, R.J. Chisnall, I.C. Pickering, S. Schauer. "How port security has to evolve to address the cyber-physical security threat: Lessons from the Sauron project," Int. J. Transp. Dev. Integr., **4**(1), 29-41. DOI: 10.2495/TDI-V4-NI-29-41, 2020.

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

M. Bastow M. "Cyber security of the railway signalling & control system," 9th IET International Conference on System Safety and Cyber Security, IET; 2014:5.2.1-. doi:10.1049/cp.2014.0986, 2014.

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

T. Blake, T. "Hackers took "full control" of container ship's navigation systems for 10 hours," ASKET Ltd, Maritime Security News and Updates, 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.

CISA. "DHS Risk Lexicon," 2010 ed., rev. 2020, https://www.cisa.gov/sites/default/files/publications/dhs-risk-lexicon-2010_0.pdf

CISA. “Marine Transportation System Resilience Assessment Guide,” 2023, https://www.cisa.gov/sites/default/files/2023-03/Marine%20Transportation%20System%20Resilence%20Assessment%20Guide.pdf.

Council on Foreign Relations. “A Cyberattack on the U.S. Power Grid,” Contingency Planning Memorandum No. 31, April 3, 2017, https://www.cfr.org/report/cyberattack-us-power-grid.

Department of Homeland Security. “Planning Considerations: Complex, Coordinated Terrorist Attacks,” July 2018, Available online at the folloiwing link: https://www.fema.gov/sites/default/files/2020-07/planning-considerations-complex-coordinated-terrorist-attacks.pdf.

J. Depoy, J. Phelan, P. Sholander, B. Smith, G.B. Varnado, G. Wyss. “Risk assessment for physical and cyber attacks on critical infrastructures,” MILCOM 2005 - 2005 IEEE Military Communications Conference, Atlantic City, NJ, USA, 2005, pp. 1961-1969 Vol. 3, doi: 10.1109/MILCOM.2005.1605959.

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

E-ISAC. “Analysis of the Cyber Attack on the Ukrainian Power Grid,” March 18, 2016. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf

ENISA. “ENISA Threat Landscape: Transport Sector,” March 2023.

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

J. Helander. “Identification and analysis of external event combinations for Hanhikivi 1 PRA,” Nuclear Engineering and Technology, 49, 380–386, 2017.

M. Laris. “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#).

R.M. Lee, M.J. Assante, T. Conway. “Analysis of the Cyber Attack on the Ukrainian Power Grid,” E-ISAC, March 18, 2016.

Z. Liu, F. Nadim, A. Garcia-Aristizabal, A. Mignan, F. Fleming, B. Quan Luna. “A three-level framework for multi-risk assessment,” Georisk: Assessment and Management of Risk for Engineered Systems and Geohazards, 9(2), 59–74, DOI: 10.1080/17499518.2015.1041989, 2015.

N. Moini, J.F. Betak. “Vulnerability Assessments of Transport Infrastructure Through Modeling of Risk Interconnectivity,” TRB 93rd Annual Meeting Compendium of Papers, Transportation Research Board, Washington, DC, 2014.

J. Monteagudo, J. “Rail and Metro Cyber Security – Where is the Industry Now?,” Cyber Startup Observatory, 2021, accessed March 12, 2023, https://cyberstartupobservatory.com/rail-cyber-security-where-is-the-industry-now/.

A. Narayanan, J.W. Welburn, B.M. Miller, S.T. Li, A. Clark-Ginsberg. “Deterring Attacks Against the Power Grid,” The RAND Corporation, Santa Monica, CA, 2020.

National Academies. "Protection of Transportation Infrastructure from Cyber Attacks: A Primer,” Washington, DC: The National Academies Press, https://doi.org/10.17226/23516, 2016.

National Academies. “Enhancing the Resilience of the Nation’s Electricity System,” Washington, DC: The National Academies Press, https://doi.org/10.17226/24836, 2017.

National Research Council. “Review of the Department of Homeland Security’s Approach to Risk Analysis,” National Academies Press, Washington, DC, 2010.

T. Nguyen, S. Wang, M. Alhazmi, M. Nazemi, A. Estebsari, P. Dehghanian. “Electric power grid resilience to cyber adversaries: State of the art,” IEEE Access, 8, 87592-87608, 2020, doi: 10.1109/ACCESS.2020.2993233.

F.S. Roberts. “Meaningful and meaningless statements using metrics for the border condition,” Proceedings of 2016 IEEE International Symposium on Technologies for Homeland Security, IEEE, 2016.

F.S. Roberts. “From football to oil rigs: Risk assessment for combined cyber and physical attacks,” Journal of Benefit Cost Analysis, 10, 251–273, 2019.

F.S. Roberts, D. Egan, C. Nelson, R. Whytlaw. “Combined cyber and physical attacks on the maritime transportation system,” NMIOTC Journal, 18, 27–37, 2019.

A. Roth. “‘Cyberpartisans’ hack Belarusian railway to disrupt Russian buildup,” The Guardian, Jan. 25, 2022, https://www.theguardian.com/world/2022/jan/25/cyberpartisans-hack-belarusian-railway-to-disrupt-russian-buildup.

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

The State Council Information Office of the People’s Republic of China. “China’s military strategy,” China Daily, 2015, http://www.chinadaily.com.cn/china/2015-05/26/content_20820628.htm.

C. Swain. (2022). “The Emerging Cyber Threat to the American Rail Industry,” Lawfare, October 20, 2022, https://www.lawfareblog.com/emerging-cyber-threat-american-rail-industry.

J. Talanova. “Drone slams into seating area at U.S. Open; teacher arrested,” CNN, September 5, 2015, https://www.cnn.com/2015/09/04/us/us-open-tennis-drone-arrest/index.html.

Templar Executives. “Cyber resilience in the maritime and energy sectors,” Templar Executives, May 1, 2014. https://www.templarexecs.com/cyberresilience/.

J. Thomas. “ Gillette Stadium evacuated for fire alarm prior to Steelers vs. Patriots,” SBNation, January 22, 2017, http://www.sbnation.com/2017/1/22/14350196/boston-mansets-off-fire-alarms-at-steelers-hotel-before-championship-game-vs-patriots.

C. Tsigkanos, T. Kehrer, C. Ghezzi. “Architecting dynamic cyber-physical spaces,” Computing, 98, 1011–1040, DOI 10.1007/s00607-016-0509-6, 2016.

C. Tsigkanos, L. Pasquale, G. Ghezzi, B. Nuseibeh. “On the interplay between cyber and physical spaces for adaptive security,” IEEE Transactions on Dependable and Secure Computing, 15, 466-480, 2018.

A. Tucci. “Cyber risk management: Preparing for new operational risks,” Port Technology International Journal, 74, 90–92, 2017.

A. Tversky, D. Kahneman. “Judgment under uncertainty: Heuristics and biases,” Science, 185, 1124–1131, 1974.

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

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

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