Communications of the Association for Information Systems

Volume 47 Article 36

12-31-2020

Cyber-physical Systems (CPS) Security: State of the Art and Research Opportunities for Information Systems Academics

Chetan Kumar
California State University, San Marcos, ckumar@csusm.edu

Sean Marston
Western Kentucky University

Ravi Sen
Texas A&M University

Follow this and additional works at: https://aisel.aisnet.org/cais

Recommended Citation
Kumar, C., Marston, S., & Sen, R. (2020). Cyber-physical Systems (CPS) Security: State of the Art and Research Opportunities for Information Systems Academics. Communications of the Association for Information Systems, 47, pp-pp. https://doi.org/10.17705/1CAIS.04731

This material is brought to you by the AIS Journals at AIS Electronic Library (AISeL). It has been accepted for inclusion in Communications of the Association for Information Systems by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Communications of the Association for Information Systems

Commentary DOI: 10.17705/1CAIS.04731 ISSN: 1529-3181

Cyber-physical Systems (CPS) Security: State of the Art and Research Opportunities for Information Systems Academics

Chetan Kumar
Department of Management Information Systems, College of Business Administration,
California State University San Marcos
ckumar@csusm.edu

Sean Marston
Department of Information Systems,
Gordon Ford College of Business,
Western Kentucky University

Ravi Sen
Department of Information and Operations Management,
Texas A&M University

Abstract:

Attacks on cyber-physical systems (CPS) continue to grow in frequency. However, cybersecurity academics and practitioners have so far focused primarily on computer systems and networks rather than CPS. Given the alarming frequency with which cybercriminals attack CPS and the unique cyber-physical relationship in CPS, we propose that CPS security needs go beyond what purely computer and network security requires. Thus, we require more focused research on cybersecurity based on the cyber-physical relationship between various CPS components. In this paper, we stock of the current state of CPS security and identify research opportunities for information systems (IS) academics.

Keywords: CPS, Cyber Physical Systems, Cybersecurity, Cyberattack.

This manuscript underwent editorial review. It was received 12/04/2019 and was with the authors for five months for two revisions. Devinder Thapa served as Associate Editor.

1 Introduction

A nation's critical infrastructure (CI) refers to "fundamental systems and services that are critical to [its] security, economic prosperity, and social well-being" (Rinaldi, Peerenboom, & Kelly, 2001). The U.S. Department of Homeland Security (2020) defines CI in a similar way as "the physical and cyber systems and assets that are so vital to the United States that their incapacity or destruction would have a debilitating impact on its physical or economic security or public health or safety". Based on this definition, the U.S. Government has identified sixteen CI sectors: chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, materials, and waste, transportation, water and wastewater systems (Cybersecurity and Infrastructure Security Agency, 2020). The communications and information technology (IT) sectors collectively comprise critical information infrastructure (CII). The IT sector produces and provides hardware, software, and information technology systems and services, while the communications sector provides the infrastructure that IT products and services need to communicate and exchange data (e.g., the Internet) (Cybersecurity and Infrastructure Security Agency, n.d.). Correspondingly, one might ask where cyber-physical systems (CPS) fit into this framework.

A cyber-physical system (CPS) comprises computers that communicate with sensors and actuators embedded in physical systems in a highly integrated and tightly coupled system (Potteiger et al., 2017). Thus, a CPS integrates information technology (IT) systems with the physical componets from other CI sectors (e.g., manufacturing, dams, emergency services, healthcare, etc.) and relies on CII for communication and coordination. Researchers and practitioners often refer to CPS that focus on manufacturing and production as cyber-physical production systems (CPPS) or industrial control systems (ICS). When a CPS uses the Internet to exchange data, optimize processes, and monitor devices, one refers to it as the Internet of things (IoT). The system's computational part (the cyber tier) comprises information technology, software, hardware, and data, while the physical components (or the physical tier) includes devices, machines, and manufacturing plants that various CI sectors use. Specially designed sensors integrate these two tiers (see Figure 1).

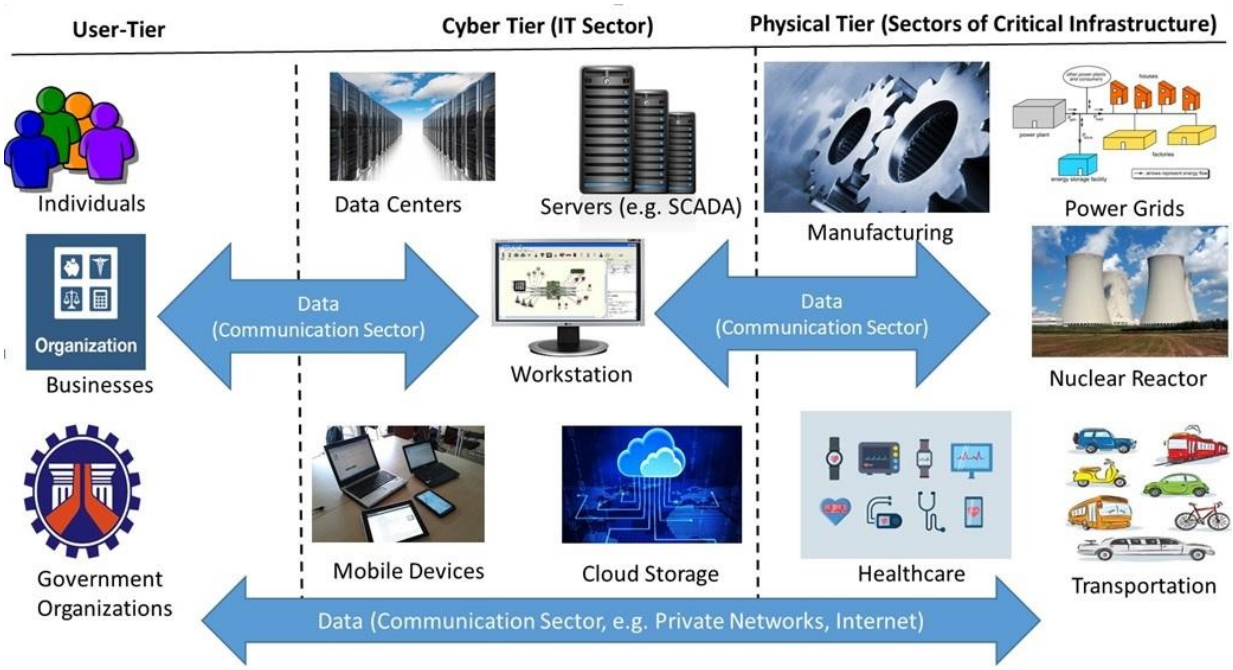

Figure 1. Cyber-physical Systems (CPS)

CPS have seen increasing use in areas such as healthcare, emergency management, traffic flow control, and electric power generation and delivery. CPS examples include the IoT, ICS, smart cities, smart power distribution grids, or, for that matter, "smart" anything (e.g., cars, buildings, homes, manufacturing, hospitals, appliances, etc.).

CPS security represents an important topic because various critical infrastructure (CI) sectors use CPS, and their failure can impact physical and economic security and public health. Furthermore, the fact that various CI components depend on one another means that a failure in one CI component can cause a cascading effect that impacts one or more other CI components. For example, in 1998, a Galaxy 4 telecommunication sattelite failed, which not only lead to service disruption for more most pagers in use (over 90%) but also impacted banking services, ATM transactions, credit card purchases, and communication with doctors and emergency medical service providers (Rosenbush, 1998). Therefore, we need to protect CPS from cyberattacks. Furthermore, we have seen an increase in the number, magnitude, sophistication, and scope of attacks on CPS in the last decade. Examples include:

- In 2010, a worm named Stuxnet hit the Iranian nuclear facilities at Natanz. Exploiting four "zero-day vulnerabilities" (i.e., vulnerabilities that the public did not yet know about, which meant no patch for them existed). The worms targeted parts of the systems that various organizations such as Siemens, Microsoft, and FararoPaya manufactured and/or developed. These systems powered the centrifuges used for Uranium enrichment. Stuxnet altered the current electrical frequency to the centrifuge drivers, which resulted in damage to the centrifuges. By some estimates, the Stuxnet attack delayed the Iranian nuclear program for two to five years (Langner, 2011).
- A cyberattack in 2012/2013 disrupted the Internet network in Iran by attacking the country's infrastructure and communications companies. The attack affected not only Internet communication but also nuclear, oil, and information networks (Aryan, Aryan, & Halderman, 2013).
- Iranian specialists in electronic warfare brought down an American RQ-170 Sentinel drone by cutting off its communications links in order to understand their stealth and intelligence capabilities (O'Hanlon, Psiaki, Bhatti, Shepard, & Humphreys, 2013).
- A cyberattack on Istanbul Ataturk Airport's passport control system managed to shut the system down, which delayed flights and caused passengers to wait in line for hours at the airport (Urban, 2017; Livanis, 2016).
- A source from the Ministry of Energy in Turkey claimed that critical cyberattacks caused widespread electricity cuts in Istanbul (Schauer, 2018).
- In December, 2015, attackers remotely accessed the control centers of three Ukrainian electricity-distribution companies. Taking control of the facilities' supervisory control and data acquisition (SCADA) systems, the attackers opened breakers at some 30 distribution substations in the capital city Kiev and western Ivano-Frankivsk region and caused more than 200,000 consumers to lose power (E-ISAC, 2016; Greenberg, 2017).
- Distributed denial-of-service (DDoS) attack launched via Internet of Things (IoT) devices (Sanger & Perlroth, 2016).
- The WannaCry ransomware attack in 2017 infected thousands of computers worldwide and invalidated critical services such as hospitals and manufacturing plants and caused an estimated loss of US$4 Billion (Fruhlinger, 2018).

However, while the increasing frequency with which attackers attack CPS represents an important concern, we should also recognize that security that focuses predominantly on cyber-physical systems' cyber tier or physical tier (see Figure 1) cannot sufficiently protect these systems. For instance, IS academics and practitioners focus on protecting computer systems' and networks' confidentiality, integrity, and availability (CIA) (Avi˘zienis, Laprie, Randell, & Landwehr, 2004). In doing so, they focus primarily on protecting data. However, such a focus cannot sufficiently protect CPS for two primary reasons:

- **Availability**: unlike traditional information technology (IT) systems, CPS interact strongly with the physical infrastructure and devices, which makers their availability one of the most important security objectives. In most computer systems (networked or not), one needs to protect the confidentiality and integrity of the data that resides on those systems, sometimes at the expense of availability (e.g., by strict access-control mechanisms). Business needs (e.g., account balance in banks should accurately reflect the true numbers), laws and regulations (e.g., protecting patient data to comply with the Health Insurance Portability and Accountability Act (HIPAA)), or both tend to drive an organization to prioritize confidentiality and integrity over availability. However, CPS need to remain available at all times. For instance, smart power grids need to provide power to a city's residents without interruption. Thus, CPS become

vulnerable to various threats from cyberattackers and cyber-physical attackers (e.g., DoS attacks). While well established controls to minimize the risk that cyberattacks pose to computer systems exist, the connection with the physical tier creates a unique unique challenge to actors responsible for securing CPS because the attack surface extends beyond computer and networks to the sensors present on the physical tier (e.g., Colbert, 2017).

- **Safety and reliability**: when dealing with traditional critical infrastructure systems, organizations expend great effort on addressing their safety and reliability. They develop appropriate techniques to detect faults, isolate their causes, and recover components in the physical tier. The additional cyber elements in CPS introduce specific vulnerabilities that traditional fault tolerance and reliable computing practices do not directly address (e.g., Colbert, 2017). Introducing highly integrated CPS into critical infrastructures and emerging systems can lead to situations where cyberattacks against the cyber tier in the CPS could adversely affect widespread public safety (e.g., Cardenas, Amin, & Sastry, 2008), which means one needs to pay special attention to addressing safety and reliability when adding cyber elements to CPS.

In additon to increased emphasis on operational objectives, securing CPS also differs from securing traditional IS/IT systems due to several reasons:

- **Interdependent cyber and physical components**: while the growing interdependency between cyber and physical entities has led to improved system performance, it has also led to new avenues for attackers to target a large number of entities by exploiting those interdependencies (Potteiger et al., 2017). Since the system's physical and cyber components are tightly coupled, we need to address not only the seurity of the cyber tier and the physical tier but also the infrastructure, devices, and processes needed to integreate these two tiers. Colbert (2017) has argued that, as CPS owners continue to install remote network control devices and incorporate an increasing number of insecure IoR devices in their industrial processes, the underlying security of their interdependent operations becomes increasingly vulnerable.
- **Defense perspective**: most existing research has focused on cybersecurity issues from the perspective of a single or centralized defender. However, multiple self-interested stakeholders rather than single entities usually manage large-scale CPS. For example, different independent system operators (ISO) manage different portions of a single smart power grid. As a result, their cybersecurity efforts remain independent. Lack of coorination among these independent efforts can result in vulnerabilities that attackers can exploit (Hota, Clements, Bagchi, & Sundaram, 2018). Therefore, our approach to CPS security should move from individual stakeholders trying to protect their own turf to an approach that requires a coordinated and joint effort from every participant in a CPS.
- **Incident response**: analyzing a cyberattack provides data, information, and knowledge that one can apply to prevent future similar attacks. With CPS, the interconnection between the cyber tier and the physical tier makes it harder to analyze cyberattacks. Furthermore, the independent ISO that participate in a CPS might not cooperate and share information about cyberattacks that occur, which could further hinder them from understanding the attacks. As a result, of the ISO may find it difficult to mitigate threats in the future (Potteiger et al., 2017).
- **Incident impact**: researchers have conducted much work on cyberattacks on cyber systems and physical attacks on physical systems. However, while one may use such research to assess traditional attacks on a CPS's cyber and physical tiers, one may not be able to use it to evaluate and assess the impact that an attack has on an entire CPS. Cyberattacks on CPS tend to be complex and challenging because they use the cyber physical relationship in CPS as part of the attack. The unique relationship between a CPS's cyber and physical parts makes assessing the impact that attacks have on CPS difficult because their complexity make traditional assessments fall apart. A prominent cyber-physical attack example includes the BlackEnergy attack on the Ukrainian power grid that brought it offline (Pattanayak & Kirkland, 2018). This attack included a DoS attack on telephone lines, hijacked virtual private networks (VPN), disabled control over the power supply, malware, and spear phishing. This highly coordinated and sophisticated attack compromised multiple aspects of the power grid, which makes it difficult for traditional approaches to estimate its overall impact.

To illustrate the cybersecurity objectives and system needs that we discuss above, we use a well-known CPS (i.e., embedded medical devices) as an example. We show a generic setup of such a CPS in Figure 2. Organizations in the CI sector healthcare have increasingly adopted this particular CPS. The system's physical tier comprises the embedded medical device (EMD), and cyber tier comprises mobile devices and applications, computers, data storage servers, and relevant software. Sensors on the embedded medical devices facilitate integration between the EMD (i.e., physical tier) and the computing devices (i.e., cyber tier). Either a private network or the Internet (in which case also qualifies as the IoT) facilitates communication between the system's various components. As Figure 2 shows, the embedded device (e.g., gastric stimulators, insulin pumps, deep brain neurostimulators, pacemakers, etc.) comprises the relevant sensors, hardware, and software to monitor and treat specific medical problems. The sensors transmit readings to relevant computer and mobile devices (e.g., devices that patients, healthcare providers, doctors, hospitals, researchers, and so on own). One can collect and store the data that such devices generate in the cloud or dedicated data centers.

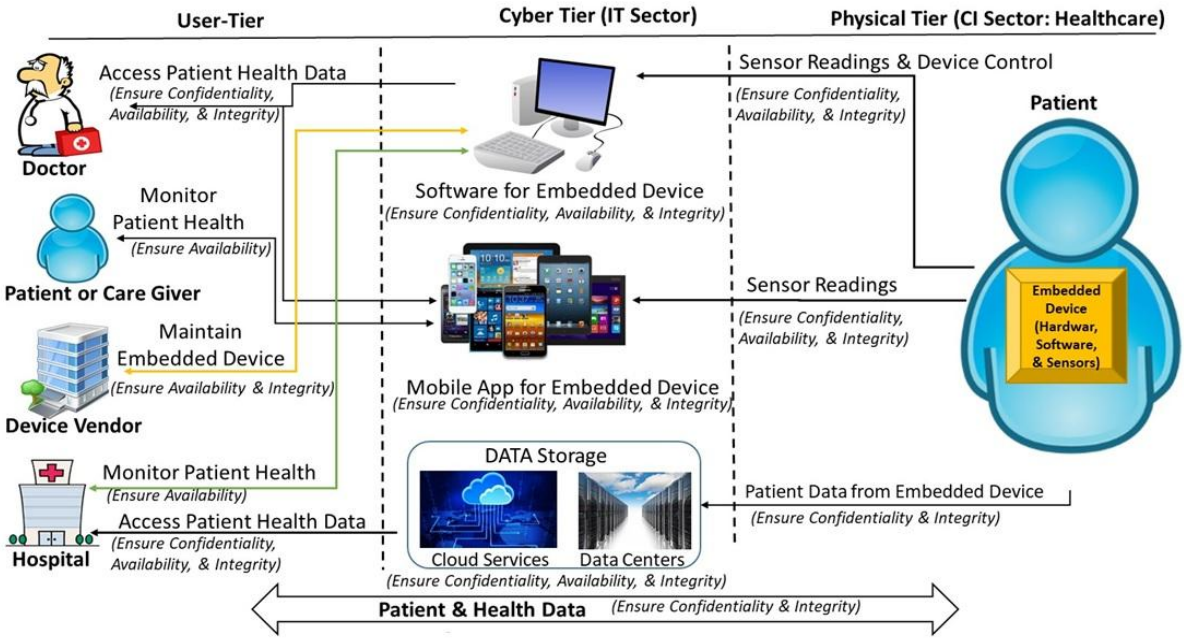

Figure 2. A Generic Setup of Embedded Medical Devices

Current cybersecurity resources focus mostly on protecting the system's cyber tier (i.e., computers, databases, cloud storage, and mobile devices) (Fu & Blum, 2013). However, we also need to ensure that the health data from sensors should be available to the controlling devices that the relevant actors (e.g., doctors and patients) use all the time (i.e., availability has paramount importance). Any disruption could adversely impact patients' health. The fact that we cannot embed redundant devices in patients to ensure continuous availability in case a cyberattack compromises the primary device. In addition, one needs to ensure the integrity of the health data that moves from the embedded medical device to the control devices (e.g., cell phones, computers, etc.) to maintain devices' reliability and patients' safety. To fully defend this CPS, all the stakeholders need to coordinate and communicate to ensure that they are on the same page when it comes to securing it. Patients, doctors, hospitals, device manufacturers, network service providers, and cloud vendors should all share the responsibility of protecting patients' health data and ensuring its availability to relevant entities and individuals in a timely manner. While easily said, various technical, behavioral, economic, and legal factors make such a task challenging (e.g., Sen, 2018). If attackers conduct a cyberattack on this CPS, the corresponding incident response will not be as straightforward compared to a cyberattack only on its cyber tier. The interconnection between the embedded device sensors, doctors' and patient's devices, hospital networks, and the data storage vendors,makes analyzing any attack on this system and responding to it in a timely manner more challenging. For example, suppose that malware has affected a patient's mobile phone that hosts the application that one needs to analyze the data from an embedded device. The malware then launches a DoS attack on the embedded device. Lack of cybersecurity awareness or relevant controls (e.g., anti-

malware application) on the patient's device might delay one's efforts to detect the malware, and, in the mean time, critical patrient data will not be availbale to the healthcare provider. An approach in which patients and the healthcare providers independently focus on protecting their part of a CPS and the embedded device vendor focuses on protecting its product will fail to detect and contain this attack in a timely manner. During this interim period, the patient's health could be endangered. More importantly, the integrity of the device itself could be compromised. Finally, unlike cyberattacks on an information system that one organization owns, a cyberattack on this CPS can have a wide-ranging impact. For example, it could result in adverse impact on patients' health; legal proceedings against the device manufacturer, hospital, and doctors; reduced research efforts on embedded devices; longer delays in approvals for embedded devices for heathcare; higher charges to store data that generate embedded devices (due to higher risk); and an increase in insurance premiums for actors who use embedded devices. In short, security needs for CPS go beyond what pure computer systems require.

In Section 2, we assess our current knowledge about: 1) designing CPS, 2) security risks to CPS, 3) preventing cyberattacks on CPS, 4) detecting such attacks when they happen, and 5) responding to these cyberattacks.

2 Cyber-physical Systems' Design

CPS designs and relevant technologies represent a key area in CPS cybersecurity that has attracted researchers' attention. For example, manufacturing and military CPS have traditionally lacked an emphasis on cybersecurity. Several existing and ongoing studies in engineering focus on complex CPS and address issues such as control, data analytics, autonomy, and information management. Potteiger et al. (2017) proposed a model-based software development framework integrated with a hardware-in-the-loop (HIL) testbed for rapidly deploying CPS attack experiments. They illustrated the framework they developed with a case study on a railway transportation system. The framework allows one to emulate cyberattacks and obtain platform-specific performance measurements that one cannot easily obtain in a traditional simulation environment. One can use the resulting data to improve CPS security during the design process. Additionally, we need to accelerate research on issues such as privacy, safety, security, and verification in CPS.

The Ptolemy Project at the University of California at Berkeley's Electrical Engineering and Computer Sciences (EECS) department identifies and defines the following CPS security objectives that pertain to their design:

- **Resilience**: A CPS's resilience refers to its ability to continue operating satisfactorily when unexpected inputs, subsystem failures, or environmental conditions or inputs outside the specified operating range stress it. Techniques the promote resilience include fault tolerance, fault detection, and adaptation.
- **Privacy**: with CPS, privacy refers to protecting data on individuals to and from sensors and ensuring other humans or machines cannot access operational data without authorization.
- **Cyberattack prevention**: like all networked computing systems, vulnerabilities in the cyber tier can affect CPS. Even closed networks (e.g., Iran Nuclear Facilities) have risks due to the possibility that one accidentally introduces malicious code (e.g., Stuxnet), back doors, DoS attacks, trojans, and other malware.
- **Intrusion detection**: with CPS, one needs to consider intrusion into both the cyber and physical tiers. Therefore, one needs to invest in all the relevant technical controls (e.g., intrusion-detection systems), administrative controls (e.g., separation of duty), and physical controls (e.g., motion detection and tracking) to minimize the risk that attackers will intrude on their cyber and physical tier components.

3 Estimating Cybersecurity Risk to Cyber-physical Systems

In this section, we present the current approaches to estimating CPS security risks. After searching for current studies in this area, we found that researchers have conducted significant work to understand and estimate CPS security risks. Most studies have focused on a particular CPS application. For example, Pretorius and van Niekerk (2015) provided a risk-assessment approach for industrial control systems (ICS) in South Africa to identify the gaps that cyberattacks could exploit. In another study, DeSmit, Elhabashy, Wells, and Camelio (2016) examined a CPS in the manufacturing domain and proposed a

method to assess security risks and vulnerabilities in the system. The method posits that one should first map how the system's cyber, physical, and human elements intersect. After one has completed the intersection mapping and identified vulnerable points, one should use decision tree mapping to analyze CPS vulnerabilities on low, medium, and high levels.

Studies that provide more widely applicable methods include one that Huang, Zhou, Tian, Yang, and Qin (2018a) conducted. They proposed a risk-assessment framework using a Bayesian network to assess cyberattacks on CPS. Radanliev et al. (2018) assessed the risk to CPS using an integrated cyber risk-assessment approach that accounts for both economic and physical risks and illustrated this approach in the IoT context. Elsewhere, Ismail, Leneutre, Bateman, and Chen (2018) proposed a quantitative model based on game theory analysis to assess the risks associated with the interdependency between the cyber and physical components in a power grid. In scenarios where one can use the Stackelberg game to model the interaction between defenders and attackers, they found that defenders can benefit more if they include attackers' reaction in their defense strategy in their analysis, which bounds attacks' potential impact in cases with rational attackers. They also found that, depending on the features of the system that one wants to protect, defenders might need to disclose some information about the system's architecture publicly. In doing so, defenders can ensure that they can correctly assess rational attackers' behavior that the computed payoffs matches the real payoffs of players' actions and, thus, optimize how they deploy valuable defense resources.

Due to CPS' integrated nature, cyberattacks on one CPS part often spread to other connected parts. To assess the risk that such a spread will occur, Konig and Gouglidid (2018) demonstrated how one can use data that vulnerability scanners gather to simulate the infection that arises from a cyberattack and use it to assess the likelihood that it will transmit through interconnected networks. Hota et al. (2018) used two complementary game-theoretic models to study networked systems' security. Their model comprised multiple self-interested defenders that each manage a set of assets that nodes in a directed graph represent. Attacks spread through the network via the interconnecting links in the graph. In the first class of game, each defender minimizes its expected loss subject to budget constraints on the defense investments, while, in the second class of games, each defender minimizes its cost of defense investment subject to the upper bounds that a successful attack will likely affect its asset (or its risk tolerance). Under suitable assumptions about how effectively defense investments will reduce attack probabilities, the authors found that a (generalized) Nash equilibrium exists in both settings and showed that each defender can compute its optimal defense allocation for a given allocation by other defenders by solving a convex optimization problem.

4 Prevent Cyberattacks against CPS

In this section, we examine the controls, policies, guidelines, standards, and regulations that focus on preventing or minimizing the risk of cyberattacks against CPS and whether they work as intended. With the way things stand at present, the US needs to work harder towards improving the overall relationships between public and private cyber agencies to better protect CPS in its critical infrastructure sectors (Weed, 2017). Horowitz (2018) has also discussed the need for the U.S. Government to implement the right policies to help adequately protect CPS. Their recommendations include: 1) selecting, certifying, and training CPS operators; 2) ensuring coordination among governments and private entities to create polices to curate data; and 3) creating market incentives to address potential attacks prior to actual incidents (Horowitz, 2018). The National Institute of Standards and Technology (NIST) has published guidelines for security best practices for general IT in its Special Publication 800-53. Furthermore, to address control systems' security, an integral component in any CPS, the NIST has also published a guide to industrial control system security (Stouffer, Falco, & Kent, 2006). On one hand, these guidelines, if followed, minimize the cybersecurity risks to CPS. On the other hand, law agencies cannot legally enforce them (except for U.S. federal agencies), which means relevant stakeholders often ignore them. Securing CPS constitutes an active research area. Rashid, Wan, Quiros, Canedo, and Al Faruque (2017) presented a model-based secure-by-design approach for modeling and simulating a CPS's cybersecurity aspects. They illustrated this approach by modeling several classes of cyberattacks that may affect a CPS's normal operations and evaluated the impact that these attacks had on the system via simulation. This modeling approach can reduce the engineering effort in developing a CPS, increase its quality, and increase its resilience when exposed to cyberattacks. Ensuring a CPS's resilience requires cross-discipline analysis and involves many challenges, such as how to address evolving cybersecurity threats. To comprehensively understand a CPS's resilience, refer to the book that Flammini (2019) edited. This

work describes emerging paradigms and techniques from two main viewpoints: 1) a CPS's exposure to new threats and 2) a CPS's potential to counteract them. It offers the latest approaches to evaluating, ensuring, and improving resilience in both the development and assessment stages.

Huang, Chen, and Zhu (2018b) applied Markov games to capture the adversarial interactions between attacks on and efforts to defend interdependent critical infrastructures (ICIs). The results state that fewer attacks happen when the system has defenders because attackers tend to avoid attacking nodes equipped with safeguard procedures. The security strategy for the infrastructure defender suggests that: 1) defenders' policy can successfully thwart attacks; 2) as more nodes equip protections, the attack number decreases; and 3) attackers avoid attacking nodes with healthy neighboring nodes because they have a better chance to survive and receive protection. In another study, Kamhoua et al. (2018) used game theory to provide a quantitative approach to perform a cost-benefit analysis on cloud services while considering other cloud users' actions and their different potential losses from a security breach. They found that an increase in the probability that a successful attack would compromise a cloud service may force other cloud participants to protect their own application/service and, thus, increase overall cloud security. They also found an intricate relationship between the total expenses required to invest in security and in a higher-profile user's payoff.

Schauer (2018) presented a novel risk-management approach for highly connected network infrastructures such as the ones that utility providers operate. This approach extends the steps that the international risk-management standard ISO 31000 specifies by including activities that specifically address utility providers' particular requirements. The proposed process, called hybrid risk management for utility networks (HyRiM), builds on a game theory framework to help utility provides improve their mitigation actions and identify an optimal risk-management strategy. It can estimate the worst-case damage and determine the corresponding optimal mitigation strategy for a given set of potential risks. Other researchers have practically applied the approach with water utility networks (Gouglidis, Konig, Green, Rossengger, & Hutchison, 2018), utility networks (Konig, Gouglidis, Green, & Solar, 2018), critical infrastructures (Alshawish, Abid, & de Meer, 2018), and a medium-sized electrical cooperative that managed a town's electricity distribution (Zambrano, Caceres, & Martinez, 2018).

5 Detect Cyberattacks against CPS

While organizations should take all necessary steps to minimize the risk of cyberattacks, they remain vulnerable. Therefore, organizations require controls, policies, and procedures in place to detect cyberattacks. In this section, we summarize some recent work in the area.

Intrusion-detection systems (IDS) have traditionally relied on two broad approaches to detecting cyberattacks: signature matching and anomaly detection. In brief, signature-matching techniques involve looking for unique signatures in network traffic to identity the related cyberattacks, and anomaly detection involves statistical approaches to identify "anomalies" in how computers and network behave that could represent cyberattack symptoms. Existing work on detecting intrusions into CPS has primarily built on these two techniques. Colbert (2017) examined IDS in industrial control systems (ICS) using a two-control process technique that built on traditional IDS based on anomaly detection. This proposed method requires one to monitor 1) an ICS's network component and 2 its critical processes. ICS operators and network engineers identify key measures for both the network and the critical processes and define threshold values for these measures. As in case of anomaly-detection techniques, IDS generates an alarm or alert if these measures breach these thresholds values. In another study, Mo, Chabukswar, and Sinopoli (2013) developed a model that used knowledge about systems dynamics to detect attacks on CPS. They showed that using a noisy control-authentication signal improves overall attack detection but at the expense of control performance. Pal, Adepu, and Goh (2017) applied an a priori algorithm to extract process constraints on ICS network traffic to establish the relationship among different process variables. They successfully identified process constraints on single variables (if X occurs, then Y will likely occur) and applied the technique to a water-treatment plant. Using the algorithm, they identified approximately 11,500 association rules for the 51 sensors in the plant's CPS.

Once stakeholders detect a cyberattack on a CPS, they must have an incident-response procedure in place to minimize its adverse impacts. In Section 6, we summarize and analyze current knowledge in this area.

6 Responding to Cyberattacks against CPS

Response to any cyberattack on a CPS has three aspects: 1) operational response, 2) policy response, and 3) legal response. In this section, we look at the recent developments along these dimensions and gauge the current knowledge in each area.

6.1 Operational Response

The operational response to cyberattacks on CPS resembles the operational response to traditional cyberattacks. One needs to gather as much information as possible while minimizing the attack's adverse impacts. For example, Rohr (2018) offered a list of actions to follow and mistakes to avoid so that the victim organization can collect data on the attack (for later analysis) and stop it before it does "too" much damage. In fact, after a simple online search for the keywords "responding to cyberattacks", we found several papers from cybersecurity consultants, practicing IT administrators, database experts, and legal experts on this topic. They recommend actions such as having a response team (e.g., a computer emergency response team) to handle the incident response to cyberattacks, conducting regular "drills" on responding to cyberattacks, training employees so that everyone knows their role in detecting and responding to the attacks, understanding the legal implications of their response, and coordinating and communicating with other stakeholders in the CPS (e.g., employees, customers, trade partners, etc.), relevant law enforcement, and regulatory agencies. A lack of effective coordination and communication between various stakeholders in the CPS represents the main challenge to an effective operational response to cyberattack on CPS. Indeed, Weed (2017) emphasized that U.S. public and private sectors need to cooperate in securing systems critical to U.S. infrastructure.

6.2 Policy Response

After any cyberattack on a CPS, the relevant stakeholders should analyze the missing controls that contributed to the attack. This analysis should lead to policy changes with the intent to prevent similar incidents in the future. For instance, Pattanayak and Kirkland (2018) reviewed cybersecurity challenges with respect to ICS in the Unites States and, in particular, focused on the federal stance from 2009 to 2018 on growing and supporting cybersecurity. They investigated attacks on critical infrastructure in Ukraine that used the BlackEnergy and CrashOverride malware tools in order to learn lessons that would help mitigate future attacks that relied on these tools. Others working in the area have found that a lack of key policy initiatives that deal with the communication and coordination among the various stakeholders in the CPS often contribute to the cyberattacks (e.g., Weed, 2017). Weed's (2017) recommendations for detecting and responding to cyberattacks on CPS include linking the different federal agencies involved in defending critical national infrastructure, creating international cybersecurity information-sharing channels, and having public and private sector agencies participate in national cybersecurity exercises. Furthermore, he suggested creating and improving automated tools for detecting cyberattacks. Towards this end, Laddaga et al. (2019) created a tool called Deriving Cyber-security Requirements Yielding Protected Physical System (DCRYPPS) to automate the cybersecurity requirements that a CPS requires.

6.3 Legal Response

Cyberattack victims can rely on several laws and regulations when they clearly identify threat agents and when such agents reside in the same jurisdiction as the victim CPS. However, when one cannot clearly identify threat agents or they reside in locations beyond the jurisdiction of the country in which the compromised CPS resides, few, if any, regulations can help victim CPS respond with legal action against the threat agent(s).

In particular, the US lacks a single, comprehensive federal law that regulates cybersecurity. Instead, the U.S. Government has approached cybersecurity by regulating only certain sectors and types of sensitive information (e.g., health and financial). Furthermore, a patchwork of state laws adds to the complex cybersecurity legal landscape. Finally, most federal and state laws primarily focus on securing personally identifiable information (PII). Therefore, these laws do not necessarily apply to all data-breach incidents. For example, the laws would not cover a data breach that targeted a power utility grid (and, thus, interrupted the power supply) but that did not compromise PII data. Interestingly, the Electronic Communications Privacy Act (ECPA), which protects certain wire, oral, and electronic communications from unauthorized interception, access, use, and disclosure, could apply to protect digital signals travelling

between a CPS's sensors and computer systems. However, we know about no incident in which someone used this law to charge the threat agent that attacked a CPS.

Many advanced economies such as Canada, Israel, and Japan have pivoted toward creating privacy regimes that are compatible with the General Data Protection Regulation (GDPR) in the European Union. Once again, we know about no laws in these countries that specifically address cyberattacks against CPS. According to Nicholas (2018), a key challenge in criminalizing cyber threats to CPS from threat agents who do not operate from inside the victim's country's jurisdiction concerns "the fact that the world lacks a common space for finding out the facts about cyberattacks, for learning from such incidents, for interpreting laws, and for agreeing on who did what to whom" (Nicholas, 2018).

On the positive side, we must point out that debates continue in and between nations on the best way to address such cyberattacks on CPS. Recently, the US (Waxman, 2017), the North Atlantic Treaty Organization (Gaud, 2017), and the EU (Muncaster, 2017) have deliberated over whether they should categorize some cyberattacks as constituting acts of war, armed attacks, or uses of force (under international law). In fact, the Pentagon has a general framework to identify and respond to a cyberattack that meets the threshold of an armed attack under international law. The U.S. Department of State even outlined principles that govern cyber warfare in 2012 (Koh, 2012). A key challenge that the US and other nations face in trying to come up with an actionable law on CPS security concerns the confusion among policymakers in defining the legal thresholds to classify cyberattacks on CPS as "acts of war". Nations require a clear and widely accepted threshold before they can invoke existing international regulations. For example, a nation can invoke Articles 2(4) and 51 of the U.N. Charter if they can classify a cyberattack against a CPS as "use of force" and/or an "armed attack" respectively. In the September, 2016, U.S. Senate Armed Services Committee's cybersecurity hearing, the Pentagon proposed that a cyberattack that meets the threshold of an "act of war" would include a "significant loss of life, injury, destruction of critical infrastructure, or serious economic impact (Adams & Reiss, 2017). However, other countries do not necessarily share this stance. Furthermore, while the U.S. Government has proactively made public statements about international law's applicability to cyberspace operations and sought to hold other states and non-state actors accountable for their cyber operations, it has done little publicly to advance the dialogue about what specific types of cyberattacks violate international law (Adams & Reiss, 2017).

As for future, since the fifth United Nations Group of Governmental Experts on Information Security's (UN-GGE) failure (Korzak, 2017) to produce a consensus report after two decades and five sessions with governmental groups of experts (Tanglen & Yammine, 2018), the following three major initiatives to mitigate the risks to cybersecurity have emerged:

1) The United Nations (UN) approved two groups to develop international rules and norms to improve cybersecurity across borders: 1) the U.S.-led Group of Governmental Experts (GGE) that comprises 25 experts that represent 25 states (including the five permanent members of the United Nation's Security Council) and 2) the Open-ended Working Group (OEWG) that Russia and China lead and that all U.N. member states may join. The main challenge that U.N.-sponsored initiatives face concerns arriving at a consensus. The fact that similar past initiatives have failed creates no hope that these current groups will succeed.
2) Major tech corporations in cooperation with some nation states, think tanks, and civil society organizations have voluntarily formed groups such as the Paris Call, the Cybersecurity Tech Accord, the Charter of Trust (Bruer & Webel, 2018), and the Global Commission on the Stability of Cyberspace (GCSC). The initiatives focus on improving cybersecurity through international cooperation between all relevant stakeholders. However, they recommend non-binding guidelines for cybersecurity. Furthermore, in the absence of major international powers such as the US, the UK, Russia, and China, these groups may find it challenging to convince countries to adopt them. At best, these guidelines will have only limited and indirect impact on cybersecurity (Efroni, 2019).
3) Some nation states have decided to identify and name the threat agents behind cross-border cyberattacks on computer networks and CPS and to lawfully retaliate against these threat agents via diplomatic or economic sanctions (Efroni, 2019). For example, in May, 2019, the US indicted a Chinese national and unnamed conspirator for hacking and stealing data from nearly 80 million customers of the healthcare company Anthem in 2015 (Volz, 2019), which researchers previously linked to Chinese state-sponsored actors (Threatconnect Research Team, 2015). However, the question remains as to whether this strategy works as a deterrent. Carlin (2016), who oversaw the early efforts to charge foreign hackers as assistant attorney

general for national security from 2014 to 2016, has written about charging foreign hackers more broadly as part of a package of tools that the U.S. Government can use to disrupt and deter state-sponsored hacking. Hinck and Maurer (2019) have supported his efforts in stating that that this approach: 1) could lead to the arrest of those accused and may deter individual hackers from working with particular states and 2) could communicate important details about hacking operations to the public and result in lessons learned. In contrast, Goldsmith and Williams (2018) have argued that charging Chinese hackers for stealing U.S. trade secrets has failed to deter such activity. Furthermore, this approach could affect broader alliance relationships among countries (Smeets, 2019). To bring about these charges, countries need to proactively monitor threat traffic globally (Nakasone, 2019). In doing so, they will need to access traffic outside their own and their adversaries' networks, such as routers in Nairobi, servers in Denmark, or operating infrastructure in any other country around the world. As a result, these activities could lead to friction with friendly nations (Nakasone, 2019).

In short, the national and international legal communities need to start a serious discussion on the laws and regulations that target cyberattacks on CPS to resolve interpretation issues.

7 Conclusion and Opportunities

CPS have an integral role in our lives. These systems have seen increasing use in areas such as agriculture, aeronautics, building design, civil infrastructure, energy management, environmental quality control, healthcare and personalized medicine, manufacturing, emergency response, and transportation. The impact that cyberattacks have on CPS can go beyond data and identity theft or stolen credit cards. These attacks can disrupt normal societal functions such as power supply and distribution, transportation, and communications. Therefore, we need to minimize the risk that these cyberattacks pose. In this paper, we summarize state-of-the-art cybersecurity research that pertains to CPS as a way to better understand the subject. We summarize the security objectives and relevant controls for a CPS's cyber tier and the physical tier in Figure 3. The common area between the two tiers represents the integration between the two tiers and their dependence on each other via the data they share.

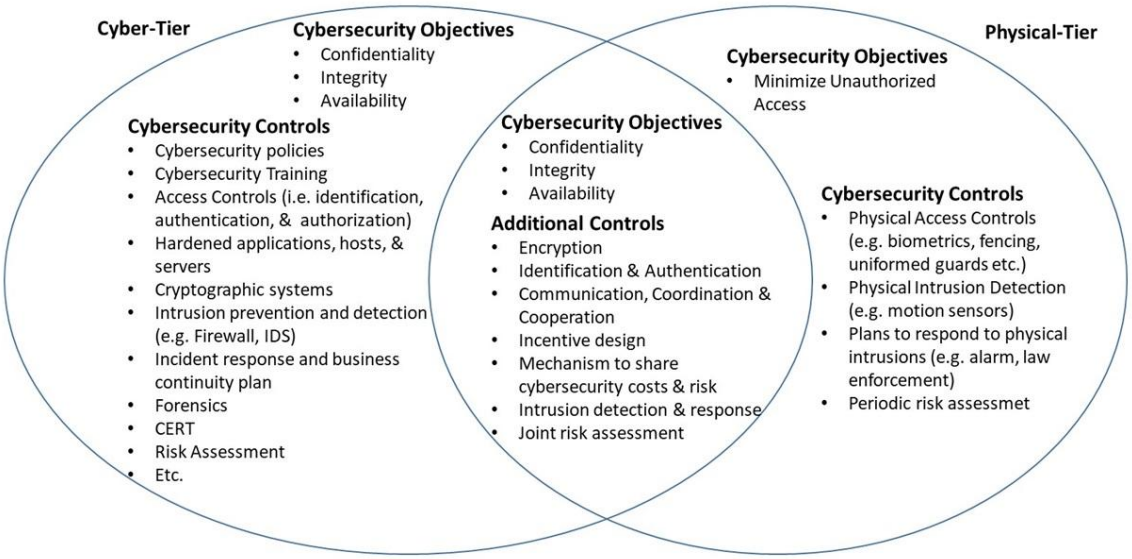

Figure 3. Cybersecurity Objectives & Relevant Controls

A large body of research that focuses on CPSs' cyber and physical tiers already exists. In addition, much research has provided methods for conducting CPS security risk assessments. Cybersecurity practitioners who have proposed standards, guidelines, and procedures to minimize cybersecurity risks to CPS have primarily conducted studies on preventing cyberattacks on CPS. However, information systems (IS) academics have a huge research opportunity in this area. For instance, they can 1) investigate the effectiveness of these standards, guidelines, and procedures in the CPS security context; 2) identify what factors influence stakeholders to adopt these standards, guidelines, and procedures; and 3) quantify the benefits that stakeholders gain from adopting these standards, guidelines, and procedures. Similarly, IS

researchers also have an opportunity to conduct work on detecting cyberattacks on CPS and, in particular, on detecting cyberattacks on the data that travels between the physical and the cyber tiers. The link between the two tiers can provide opportunities to threat agents to launch cyberattacks attacks such as DoS attacks (e.g., Su & Ye, 2018) and man-in-the-middle attacks (e.g., Lesi, Jovanow, & Pajic, 2018). Some interesting studies have proposed controls and procedures for detecting attacks on both a CPS's cyber and the physical tiers. However, these studies have focused on specific CPS, which limits their application to those particular CPS. Given that various sectors have increasingly used CPS, researchers have a good opportunity to design and develop intrusion-detection controls and procedures for these different CPS. Finally, when it comes to responding to cyberattacks on CPS, we have much relevant research in the area of operational and policy responses to such attacks. However, we lack research on legal responses to cyberattacks on CPS, especially in situations where nation states perform an attack and/or the threat agents reside in areas beyond the jurisdiction of the country in which the compromised CPS exists.

As far as research methodology goes, current research on CPS security has predominantly relied on simulations, testbeds, and modeling. For instance, Wadhawan, Neuman, and Al Majali (2018) used the outputs from multiple cyberattacks on various systems in a smart grid as inputs into the Network and PowerWorld Simulator to analyze how cyberattacks potentially destabilize underlying power systems. Adepu, Kandasamy, and Mathur (2018) presented the Electrical Power and Intelligent Control (EPIC) testbed, a small-scale industrial grade smart grid testbed that mimics real-world full-size power systems. They analyzed a power supply-interruption attack and a physical-damage attack using the EPIC testbed to discuss methods that one can use to mitigate these attacks on real-world systems. Zhou, Gou, Huang, and Yang (2018) reviewed the current state of methods and testbeds that researchers have used to examine CPSs' fragility, robustness, and security and found that they have extensively relied on these methodologies. More recently, several studies have used game theory in their research. Readers can refer to Alpcan and Basar (2010), Laszka, Felegyhazi, and Buttyan (2014), and Tambe (2011) for comprehensive discussions on the literature on applying game theory to model decentralized decision making among multiple stakeholders (as in CPS). We can classify most existing work that has used game theory into two distinct paradigms. In the first paradigm, referred to as interdependent security games (Laszka et al., 2014, Kunreuther & Heal, 2003), researchers have treated each node in the network as an independent decision maker responsible for protecting itself. Jiang, Anantharam, and Walrand (2011), who investigated inefficiency equilibria in interdependent security, Schwartz, Shetty, and Warland (2013), who studied the effectiveness of cyber insurance, and Hota and Sundaram (2016), who researched the impacts of behavioral decision making in interdependent scenarios, have used this approach. In the second paradigm, researchers have typically considered two players, an attacker and a defender, who compete over attacking and defending multiple targets. Game-theoretic models in this second framework that cybersecurity researchers have used include Stackelberg security games (e.g., Tambe, 2011), Colonel Blotto games (e.g., Roberson, 2006), and network interdiction games (e.g., Israeli & Wood, 2002). Researchers have applied these models when conducting work on protecting physical assets (e.g., Tambe, 2011), analyzing military conflicts (e.g., Roberson, 2006), and securing CPS (e.g., Durkota, Lisy, Bosansky, & Kiekintveld, 2015; Gupta, Schwartz, Langbort, Sastry, & Basar, 2014). Finally, some studies have investigated multi-defender security games with the assumption that defenders have a discrete strategy space (e.g., Letchford & Vorobeychik, 2013; Lou, Smith, & Vorobeychik, 2017), while others have relaxed this assumption (e.g., Hota et al., 2018).

We also need to consider that CPSs' continuing evolution leads to new challenges that we need to address to secure CPS. These challenges require continuing research in the risk, prevention, and detection areas. We identify several areas that provide exciting research opportunities to IS academics:

- **Designing CPS**: designing CPS involves various separate components in the cyber and physical tiers that are integrated together. Designers have primarily treated these components as independent entities and focused on individual systems' security with little concern for the cyber-physical relations between them. Future research on designing CPS needs to address integrated systems' security needs from the design process's beginnings. These studies should identify and test cybersecurity controls for not only the components in the cyber tier and the physical tier but also the secure interaction and integration between the two tiers. Designing a CPS to ensure its overall security from the ground up has potential to reduce risk, increase prevention, and help stakeholders detect attacks on the system.
- **Privacy**: a key cybersecurity objective with CPS (see Figure 3) involves ensuring the confidentiality and integrity of the data that flows between the system's cyber and physical

tiers. To do so, one could implement access control techniques between sensors in the physical tier and the computing devices in the cyber tier, which would reduce the risk that someone could access the data that travels between the two tiers without authorization (e.g., Rasmussen, Castelluccia, Benjamin, & Capkun, 2009). Another solution could involve using cryptographic systems to identify, authenticate, and authorize the components that reside in the physical and cyber tiers. However, one would face many challenges in implementing such solutions, such as power supply constraints, limited computation resources, the need to reduce how often devices require upgrades or replacements, and the prohibitively high cost. While some researchers have suggested ways to design sensors that avoid concerns about the power that cybersecurity controls require (e.g., Halprin et al., 2008; Beck, Masny, Geiselmann, & Bretthauer, 2011, Hosseini-Khayat, 2011), we require more work in this area.

- **Incentive design**: any CPS has several independent stakeholders in both the cyber and the physical tiers (e.g., software vendors, sensor manufactures, network service provided, facilities owner, etc.). In order to secure CPS, these stakeholders need to communicate, coordinate, and cooperate with one another. Furthermore, unlike cyberattacks on a single organization or platform, attacks on CPS require a coordinated response from all involved stakeholders. To ensure stakeholders respond in this way (without any legal regulations), incentives would need to exist to make cooperation and coordination the optimal strategy. The solution should optimally balance reward and risk sharing to encourage cooperation among the CPS holders. Accordingly, researchers have ample opportunities to conduct work in areas such as incentive design, game theory, negotiations, incident response, business continuity planning, and cybersecurity risk assessment of integrated but independent entities.
- **Coordination and communication between CPS stakeholders**: practitioners and academics have identified the lack of or poor communication and coordination between various CPS stakeholders (i.e., network infrastructure providers, sensor manufacturers, hardware and software vendors, etc.) as a key factor that has an adverse impact on their ability to prevent cyberattacks on CPS and responding to them when they happen. IS academics can investigate current approaches to coordination and communication between CPS stakeholders and propose better ones where applicable. Accordingly, researchers who conduct work related to emergency response systems have many opportunities in this area since they deal with similar challenges already.
- **Joint CPS risk assessments**: at present, various stakeholders assess the risk that attacks will have on only their part of a CPS. In the example that we present in Figure 2, healthcare providers (e.g., hospitals) will assess their computers and networks, the organizations that manufacture embedded medical devices will do the same for their devices, and the organizations that manufacture computing devices (e.g., computers, mobile devices) and software producers will try to harden their products. IS academics can investigate the factors that lead to this independent and uncoordinated approach to securing a CPS, provide a more comprehensive and coordinated approach to assessing the cybersecurity risk to all its parts, and identify tangible benefits that one approach has over others.

Researchers have come a long way in understanding CPS security objectives. However, they still need to conduct much more work to meet these objectives, especially as CPS continue to advance and evolve. Accordingly, IS academics have an opportunity to contribute towards more secure CPS design, effective cybersecurity controls, effective strategies for cooperation among CPS stakeholders, and better public policies to incentivize this cooperation. We outline many challenges in this paper, which makes this area an exciting one for IS researchers to make their unique contributions.

References

Adams, M. J., & Reiss, M (2017). How should international law treat cyberattacks like WannaCcry? *Lawfare*. Retrieved from https://www.lawfareblog.com/how-should-international-law-treat-cyberattacks-wannacry

Adepu, S., Kandasamy, N. K., & Mathur, A. (2018). EPIC: An electric power testbed for research and training in cyber physical systems security. In S. K. Katsikas, F. Cuppens, N. Cuppens, C. Lambrinoudakis, A. Anton, S. Gritzalis, J. Mylopoulos, & C. Kalloniatis (Eds.), *Computer security* (LNCS vol. 11387, pp. 37-52). Berlin: Springer.

Alpcan, T., & Basar, T. (2010). *Network security: A decision and game-theoretic approach*. Cambridge, UK: Cambridge University Press.

Alshawish, A., Abid, M. A., & de Meer, H. (2018). Game-theoretic optimization for physical surveillance of critical infrastructures: A case study. In S. Rass & S. Schauer (Eds.), *Game theory for security and risk management* (pp. 353-389). Berlin: Springer.

Aryan, S., Aryan, H., & Halderman, J. A. (2013). *Internet censorship in Iran: A first look.* Retrieved from https://www.usenix.org/system/files/conference/foci13/foci13-aryan.pdf

Avižienis, A., Laprie, J. C., Randell, B., Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing*, *1*(1), 11-33.

Beck, C., Masny, D., Geiselmann, W., & Bretthauer, G. (2011). Block cipher based security for severely resource-constrained implantable medical devices. In *Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies.*

Bruer, H., & Webel, S. (2018). Time for action: Building a consensus for cybersecurity. *Siemens*. Retrieved from https://new.siemens.com/global/en/company/stories/research-technologies/cybersecurity/cybersecurity-charter-of-trust.html

Cardenas, A., Amin, S., & Sastry, S. (2008). Secure control: Towards survivable cyber-physical systems. In *Proceedings of the 28th International Conference on Distributed Computing Systems Workshop.*

Carlin, J. P. (2016). Detect, disrupt, deter: A whole-of-government approach to national security cyber threats. *Harvard National Security Journal*, *7*, 391-436.

Colbert, E. (2017). Security of cyber-physical systems. *Journal of Cyber Security and Information Systems*, *5*(1).

Cybersecurity and Infrastructure Security Agency. (2020). *Critical infrastructure sectors*. Retrieved from www.cisa.gov/critical-infrastructure-sectors

Cybersecurity and Infrastructure Security Agency. (n.d.). Information technology sector. Retrieved from www.cisa.gov/information-technology-sector

DeSmit, Z., Elhabashy, A. E., Wells, L. J., & Camelio, J. A. (2016). Cyber-physical vulnerability assessment in manufacturing systems. *Procedia Manufacturing*, *5*, 1060-1074.

Durkota, K., Lisy, V., Bosansky, B., & Kiekintveld, C. (2015). Approximate solutions for attack graph games with imperfect information. In *Proceedings of the International Conference on Decision and Game Theory for Security*.

Efroni, D. (2019). Entering the third decade of cyber threats: Toward greater clarity in cyberspace. *Lawfare*. Retrieved from https://www.lawfareblog.com/entering-third-decade-cyber-threats-toward-greater-clarity-cyberspace

E-ISAC. (2016). *Analysis of the cyber attack on the Ukrainian power grid.* Retrieved from https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

Flammini, F. (Ed.). (2019). *Resilience of cyber-physical systems: From risk modelling to threat counteraction.* Berlin: Springer.

Fruhlinger, J. (2018). What is WannaCry ransomware, how does it infect, and who was responsible? *CSO*. Retrieved from https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html

Fu, K., & Blum, J. (2013). Controlling for cybersecurity risks of medical device software. *Communications of ACM*, *56*(10), 35-37.

Gaud, N. (2017). NATO tags the latest cyber attack as an "act of war". *Cybersecurity Insiders.* Retrieved from https://www.cybersecurity-insiders.com/nato-tags-the-latest-cyber-attack-as-an-act-of-war/

Goldsmith, J., & Williams R. D. (2018). The failure of the United States' Chinese-hacking indictment Strategy. *Lawfare*. Retrieved from https://www.lawfareblog.com/failure-united-states-chinese-hacking-indictment-strategy

Gouglidis, A., Konig, S., Green, B., Rossengger, K., & Hutchison, D. (2018). Protecting water utility networks from advanced persistent threats: A case study. In S. Rass & S. Schauer (Eds.), *Game theory for security and risk management* (pp. 313-333). Berlin: Springer.

Greenberg, A. (2017). Crash overdrive: The malware that took down a power grid. *Wired.* Retrieved from http://bit.ly/2raojOf

Gupta, M., Schwartz, G., Langbort, C., Sastry, S. S., & Basar, T. (2014). A three-stage Colonel Blotto game with applications to cyberphysical security. In *Proceedings of the American Control Conference.*

Halperin, D., Heydt-Benjamin, T. S., Ransford, B., Clark, S. S., Defend, B., Morgan, W., Fu, K., Kohno, T., & Maisel, M. (2008). Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In *Proceedings of the IEEE Symposium on Security and Privacy*.

Hinck, G., & Maurer, T. (2019). What's the point of charging foreign state-linked hackers? *Lawfare*. Retrieved from https://www.lawfareblog.com/whats-point-charging-foreign-state-linked-hackers

Horowitz, B. M. (2018). *Policy issues regarding implementations of cyber attack resilience solutions for cyber physical systems.* Retrieved from https://www.aaai.org/ocs/index.php/SSS/SSS18/paper/download/17488/15484

Hosseini-Khayat, S. (2011). A lightweight security protocol for ultra-low power asic implementation for wireless implantable medical devices. In *Proceedings of the 5th International Symposium on Medical Information & Communication Technology.*

Hota, A. R., Clements, A. A., Bagchi, S., & Sundaram, S. (2018). A game-theoretic framework for securing interdependent assets in networks. In S. Rass & S. Schauer (Eds.), *Game theory for security and risk management* (pp. 157-184). Berlin: Springer.

Hota, A. R., & Sundaram, S. (2016). Interdependent security games on networks under behavioral probability weighting. *IEEE Transactions on Control of Network Systems*, *5*(1), 262-273.

Huang, K., Zhou, C., Tian, Y. C., Yang, S., & Qin, Y. (2018a). Assessing the physical impact of cyberattacks on industrial cyber-physical systems. *IEEE Transactions on Industrial Electronics*, *65*(10), 8153-8162.

Huang, L., Chen, J., & Zhu, Q. (2018b). Factored Markov game theory for secure interdependent infrastructure networks. In S. Rass & S. Schauer (Eds.), *Game theory for security and risk management* (pp. 99-126). Berlin: Springer.

Ismail, Z., Leneutre, J., Bateman, D., & Chen, L. (2018). Managing security risks interdependencies between ICT and electric infrastructure: A game theoretical analysis. In S. Rass & S. Schauer (Eds.), *Game theory for security and risk management* (pp. 223-250). Berlin: Springer.

Israeli, E., & Wood, R. K. (2002). Shortest-path network interdiction. *Networks*, *40*(2), 97-111.

Jiang, in L., Anantharam, V., & Walrand, J. (2011). How bad are selfish investments in network security? *IEEE/ACM Transactions on Networking*, *19*(2), 549-560.

Kamhoua, C. A., Kwiat, L., Kwiat, K. A., Park, J. S., Zhao, M., & Rodriguez, M. (2018). Security and interdependency in a public cloud: A game-theoretic approach. In S. Rass & S. Schauer (Eds.), *Game theory for security and risk management* (pp. 253-284). Berlin: Springer.

Koh, H. (2012). Harold Koh on international law in cyberspace. *OpinioJuris.* Retrieved from http://opiniojuris.org/2012/09/19/harold-koh-on-international-law-in-cyberspace/

Konig, S., & Gouglidis, A. (2018). Random damages in interconnected networks. In S. Rass & S. Schauer (Eds.), *Game theory for security and risk management* (pp. 185-201). Berlin: Springer.

Konig, S., Gouglidis, A., Green, B., & Solar, A. (2018). Assessing the impact of malware attacks in utility networks. In S. Rass & S. Schauer (Eds.), *Game theory for security and risk management* (pp. 335-351). Berlin: Springer.

Korzak, E. (2017). UN GGE on Cybersecurity: The end of an era? *The Diplomat.* Retrieved from https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/

Kunreuther, H., & Heal, G. (2003). Interdependent security. *Journal of Risk and Uncertainty*, *26*(2-3), 231-249.

Laddaga, R., Robertson, P., Shrobe, H., Cerys, D., Manghwani, P., & Meijer, P. (2019). *Deriving cyber-security requirements for cyber physical systems.* Retrieved from https://arxiv.org/abs/1901.01867

Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy, 9*(3), 49-51.

Laszka, A., Felegyhazi, M., & Buttyan, L. (2014). A survey of interdependent information security games. *ACM Computing Surveys, 47*(2), 1-38.

Lesi, V., Jovanow, I., & Pajic, M. (2018). *Integrating security in resource-constrained cyber-physical systems.* Retrieved from https://arxiv.org/pdf/1811.03538.pdf

Letchford, J., & Vorobeychik, Y. (2013). Optimal interdiction attack plans. In *Proceedings of the International Conference on Autonomous Agents and Multi-agent Systems.*

Livanis, E. (2016). Financial aspects of cyber risks and taxonomy for the efficient handling of these risks. In *Proceedings of the 14th International Scientific Conference on Economic and Social Development.*

Lou, J., Smith, A. M., & Vorobeychik, Y. (2017). Multidefender security games. *IEEE Intelligent Systems*, *32*(1), 50-60.

Mo, Y., Chabukswar, R., & Sinopoli, B. (2013). Detecting integrity attacks on SCADA systems. *IEEE Transactions on Control Systems Technology*, *22*(4), 1396-1407.

Muncaster, P. (2017). EU to declare cyber-attacks “act of war”. *Infosecurity.* Retrieved from https://www.infosecurity-magazine.com/news/eu-to-declare-cyber-attacks-act-of/

Nakasone, P. (2019). Defending forward: An interview with Paul M. Nakasone. *Joint Force Quarterly, 92(1), 4-9.*

Nicholas, P. (2018). Filling the gaps in international law is essential to making cyberspace a safer place. *Microsoft*. Retrieved from https://www.microsoft.com/en-us/cybersecurity/blog-hub/filling-the-gaps-in-international-law-is-essential-to-making-cyberspace-a-safer-place

O’Hanlon, B. W., Psiaki, M. L., Bhatti, J. A., Shepard, D. P., & Humphreys, T. E. (2013). Real-time GPS spoofing detection via correlation of encrypted signals. *Navigation*, *60*(4), 267-278.

Pal, K., Adepu, S., & Goh, J. (2017). Effectiveness of association rules mining for invariants generation in cyber-physical systems. In *Proceedings of the 18th International Symposium on High Assurance Systems Engineering.*

Pattanayak, A., & Kirkland, M. (2018). Current cyber security challenges in ICS. In *Proceedings of the International Conference on Industrial Internet*.

Potteiger, B., Emfinger, W., Neema, H., Koutosukos, X., Tang, C. Y., & Stouffer, K. (2017). Evaluating the effects of cyber-attacks on cyber physical systems using a hardware-in-the-loop simulation testbed. In *Proceedings of the International Symposium on Resilient Communications Systems.*

Pretorius, B., & van Niekerk, B. (2015). Cybersecurity and governance for ICS/SCADA in South Africa. In *Proceedings of the 10th International Conference on Cyberwarfare and Security*.

Radanliev, P., De Roure, D. C., Nicolescu, R., Huth, M., Montalvo, R. M., Cannady, S., & Burnap, P. (2018). Future developments in cyber risk assessment for the internet of things. *Computers in Industry*, *102*, 14-22.

Rasmussen, K. B., Castelluccia, C., Benjamin, T., & Capkun, S. (2009). Proximity based access control for implantable medical devices. In *Proceedings of the 16th ACM Conference on Computer and Communications Security*.

Rashid, N., Wan, J., Quiros, G., Canedo, A., & Al Faruque, M. A. (2017). Modeling and simulation of cyberattacks for resilient cyber-physical systems. In *Proceedings of the 13th IEEE Conference on Automation Science and Engineering.*

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, *21*(6), 11-25.

Roberson, B. (2006). The Colonel Blotto game. *Economic Theory*, *29*(1), 1-24.

Rohr, A. (2019). Incident response: How to deal with a cyberattack. In A. Miljus, M. Perkowski, & A. Perlman (Eds.), *Navigating the digital age* (pp. 255-260). Santa Clara, CA: Palo Alto Networks.

Rosenbush, S. (1998). Satellite's death puts millions out of touch. *USA Today*.

Sanger, D. E., & Perlroth, N. (2016). A new era of internet attacks powered by everyday devices. *The New York Times*. Retrieved from https://www.nytimes.com/2016/10/23/us/politics/a-new-era-of-internet-attacks-powered-by-everyday-devices.html

Schauer, S. (2018). A risk management approach for highly interconnected networks. In S. Rass & S. Schauer (Eds.), *Game theory for security and risk management* (pp. 285-311). Berlin: Springer.

Schwartz, G., Shetty, N., & Warland, J. (2013). Why cyber-insurance contracts fail to reflect cyber-risks. In *Proceedings of the 51st Annual Allerton Conference on Communication, Control, and Computing.*

Sen R. (2018). Challenges to cybersecurity: Current state of affairs. *Communications of Association for Information Systems*, 43, 22-44.

Smeets, M. (2019). Cyber command's strategy risks friction with allies. Lawfare. Retrieved from https://www.lawfareblog.com/cyber-commands-strategy-risks-friction-allies

Stouffer, K., Falco, J., & Kent, K. (2006). *Guide to supervisory control and data acquisition (SCADA) and industrial control systems security*. Gaithersburg, MD: National Institute of Standards and Technology.

Su, L., & Ye, D. (2018). A cooperative detection and compensation mechanism against denial-of-service attack for cyber-physical systems. *Information Sciences*, *444*, 122-134

Tambe, M. (2011). *Security and game theory: Algorithms, deployed systems, lessons learned*. Cambridge, UK: Cambridge University Press.

Tanglen, L. J., & Yammine, R. E. (2018). The collapse of UN talks on the application of international law in cyberspace: Why it matters to U.S. businesses. *K&L Gates.* Retrieved from http://www.klgates.com/the-collapse-of-un-talks-on-the-application-of-international-law-in-cyberspace-why-it-matters-to-us-businesses-05-24-2018/

Threatconnect Research Team. (2015). *The Anthem hack: All roads lead to China.* Retrieved from https://threatconnect.com/blog/the-anthem-hack-all-roads-lead-to-china/

Urban, J. A. (2017). Not your granddaddy's aviation industry: The need to implement cybersecurity standards and best practices within the international aviation industry. *Albany Law Journal of Science & Technology, 27*(1), 62-93.

U.S. Department of Homeland Security. (2020). *Critical infrastructure security*. Retrieved from https://www.dhs.gov/topic/critical-infrastructure-security

Volz, D. (2019). Chinese national indicted on hacking charges related to Anthem breach. *The Wall Street Journal*. Retrieved from https://www.wsj.com/articles/chinese-national-indicted-on-hacking-charges-related-to-anthem-breach-11557433541

Wadhawan, Y., Neuman, C., & Al Majali, A. (2018). A systematic approach for analyzing multiple cyber-physical attacks on the smart grid. In *Proceedings of the International Science Index, Computer and Information Engineering International Conference on Cyber Security of Cyber Physical Systems.*

Waxman, M. C. (2017). *Cyber strategy & policy: International law dimensions*. Retrieved from https://www.armed-services.senate.gov/imo/media/doc/Waxman_03-02-17.pdf

Weed, S. A. (2017). *US policy response to cyber attack on SCADA systems supporting critical national Infrastructure*. Maxwell Air Force Base, AL: Air University Press.

Zambrano, A., Caceres, S., & Martinez, A. I. (2018). Smart SECPLAN: A process implementation tool for hybrid risk management. In S. Rass & S. Schauer (Eds.), *Game theory for security and risk management* (pp. 391-418). Berlin: Springer.

Zhou, X., Gou, X., Huang, T., & Yang, S. (2018). Review on testing of cyber physical systems: Methods and testbeds. *IEEE Access*, *6*, 52179-52194.

About the Authors

Chetan Kumar is an Associate Professor of Information Systems at California State University San Marcos. He received his PhD from Purdue University. His research interests include cybersecurity, big data, cloud computing, electronic commerce, web analytics, healthcare analytics, and green IT. He research has been published in journals such as *Decision Support Systems*, *Electronic Commerce* R*esearch and Applications, Journal of Information Systems and Technology Management*, and others. He has presented his research at conferences such as the Institute for Operations Research and Management Sciences (INFORMS) Annual Meeting, Workshop on E-Business (WeB), Workshop on Information Systems and Economics (WISE), and International Conference on Information Systems (ICIS) Doctoral Consortium.

Sean Marston is an associate professor in the Department of Information Systems at the Gordon Ford College of Business at Western Kentucky University. He received his PhD in Information Systems and Operations Management at the Warrington College of Business at the University of Florida. His research includes the analysis of digital distribution of information, the economic analysis of information systems policies, and cloud computing security policy. His work has been published in *Journal of Management Information Systems*, *International Journal of Electronic Commerce*, *Decision Support Systems*, and *Decision Sciences*.

Ravi Sen is an Associate Professor at Mays Business School, Texas A&M. He received his Ph.D. in 2003 from the University of Illinois at Urbana-Champaign. His research interests include cybersecurity, open source software, and economics of electronic commerce. He has published in the *Journal of Management Information Systems*, *Decision Sciences*, *International Journal of Electronic Commerce, Communications of the AIS*, *Electronic Markets*, and *Journal of Electronic Commerce Research*.

Copyright © 2020 by the Association for Information Systems. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and full citation on the first page. Copyright for components of this work owned by others than the Association for Information Systems must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers, or to redistribute to lists requires prior specific permission and/or fee. Request permission to publish from: AIS Administrative Office, P.O. Box 2712 Atlanta, GA, 30301-2712 Attn: Reprints or via e-mail from publications@aisnet.org.