IISE TRANSACTIONS
https://doi.org/10.1080/24725854.2020.1781306

Taylor & Francis
Taylor & Francis Group

A survey of optimization models and methods for cyberinfrastructure security

Q32 Forough Enayaty-Ahangar[a], Laura A. Albert[b], and Eric DuBois[b]

Q1 [a]Cornell University, Ithaca, NY, USA; [b]University of Wisconsin-Madison, Madison, WI, USA

ABSTRACT

Critical infrastructure from a cross-section of sectors has become increasingly reliant on cyber systems and cyberinfrastructure. Increasing risks to these cyber components, including cyber-physical systems, have highlighted the importance of cybersecurity in protecting critical infrastructure. The need to cost-effectively improve cyberinfrastructure security has made this topic suitable for optimization research. In this survey, we review studies in the literature that apply optimization to enhance or improve cyberinfrastructure security and were published or accepted before the end of the year 2019. We select 68 relevant peer-reviewed scholarly works among 297 studies found on Scopus and provide an overview of their application areas, mission areas, and optimization models and methods. Finally, we consider gaps in the literature and possible directions for future research.

ARTICLE HISTORY
Received 28 October 2019
Accepted 3 June 2020

KEYWORDS
Applied optimization; critical infrastructure protection; cybersecurity; security

1. Introduction

Normal societal and economic functioning depends on the efficient operation of a variety of Critical Infrastructure (CI) sectors, ranging from governmental facilities and energy to health care and communications. CI is itself substantially dependent on cyberinfrastructure, such as Information Communication Technology (ICT) networks (Smartgrid *et al*., 2010; Ravishankar *et al*., 2018). Cyberinfrastructure is composed of cyber-physical systems such as the hardware and software that enables the storing, processing, and communication of information required by all CI sectors to function. This infrastructure is vulnerable to natural disasters, physical incidents, and adversarial attacks (Ravishankar *et al*., 2018). Recent incidents such as the Equifax data breach (EPIC, 2019), cyberattacks against United States power utilities (Barnett, 2019), and the data breach of the United States Office of Personnel Management in 2015, in which over 222 000 000 federal employees' data were stolen (Koener, 2016), indicate that cybersecurity is an area of national concern across many sectors. Other companies that have suffered major data loss breaches due to cyber-attacks include Yahoo, eBay, Target, Uber, Home Depot, and Adobe (Armerding, 2018).

As systems have become more connected and reliant on cyberinfrastructure and the Internet, governments, firms, and organizations throughout the world have dramatically changed the ways they perform daily operations, administer their businesses, and communicate with each other. In addition, reports of information systems such as banks and credit companies being penetrated and compromised by hackers and ransomware attacks have made information security a matter of national security for all countries (Moore, 2010). This has led to significant and increasing attention from governments and researchers to determine how to protect cyberinfrastructure, including information systems, from adversarial attacks (Gordon *et al*., 2003; Ravishankar, 2018). These growing risks have forced firms, organizations, and governments to adapt and deploy a variety of defenses (e.g., encryption techniques, firewalls) to combat these threats (Gordon *et al*., 2003). The White House has made cybersecurity a national priority and has repeatedly emphasized the importance of cybersecurity and CI security (The White House, 2013a, 2016). By the year 2012, more than 50 countries had published some cyber strategy that explains the meaning of security to their economy and nation (Klimberg, 2012).

Threats to cyberinfrastructure come in various forms, such as industrial cyber espionage, online identity theft, and botnets (Moore, 2010). It is not possible to fully protect these systems and infrastructures by detecting and eliminating all security threats before they occur. Indeed, security threats can occur at any point in time within the systems' life-cycles and affect any part of the systems (Edwards *et al*., 2016), making these threats significantly more difficult to detect and expensive to eliminate. Due to this, a significant body of the literature has been devoted to using optimization techniques for reducing and managing risks to enhance cyberinfrastructure security. In this article, we survey the current literature on these topics.

Cyberinfrastructure relies on extensive globalized Supply Chains (SCs) consisting of systems with complex dynamic networks that assist the movement of products, information, and services. As a result, cybersecurity includes protecting these SCs. Various organizations have developed guidelines, policies, and practices to mitigate against possible threats to their SCs (Kao *et al*., 2015). The concern has also been

CONTACT Laura A. Albert laura@engr.wisc.edu

expressed by governments worldwide (Edwards *et al*., 2016), due to the national security risks posed by the existing lack of transparency in SCs. These SCs and networks are geographically diverse and interconnected. As a result, they are open to various security risks to data and information systems, as well as to the infrastructures' availability, integrity, and confidentiality (Kao *et al*., 2015). The complexity of SCs and networks makes it challenging to fully understand all of the risks they face. However, it is critical to protect these SCs to reduce the risks to cyberinfrastructure.

There have been numerous research documents published in the past two decades that focus on various aspects of cyberinfrastructure security. This survey reviews the research documents that use optimization models and methods to employ limited resources to manage vulnerabilities, reduce risks, control costs, and enhance security. This survey is organized as follows: In Section 2, we first define the terminology and concepts used throughout the article. We explain the search process we employed to identify related documents in Section 3. Studies that meet our full inclusion criteria are then classified based on their applications, mission areas, and optimization concepts in Section 4. Section 5 summarizes our findings and introduces future research directions.

2. Definitions of concepts

In this article, we survey papers that apply optimization models and methods to cyberinfrastructure security. We begin by defining each of the terms that we used to define our scope and identify related scholarly documents.

2.1. Security concepts

Security refers to protecting CI, reducing the likelihood or effects of an adverse event, or aiding in recovery efforts. In 2013, The Department of Homeland Security (2019) defines **security** as "reducing the risk to critical infrastructure by physical means or defense cyber measures to intrusions, attacks, or the effects of natural or manmade disasters." Cybersecurity is one form of security that includes all actions of prevention, protection, and restoration for computers, electronic communications systems, and other related systems to ensure availability, integrity, confidentiality (The White House, 2008). In this survey article, we use the definition of cybersecurity introduced by the Telecommunication Standardization Sector of International Telecommunication Union (2008):

> **Cybersecurity** is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.

An organization and user's assets refer to personnel, connected computing devices, infrastructure, applications, telecommunications systems, services, and stored information in cyber environments.

The Committee on National Security Systems (2015) defines an **attack** as "any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself" and a **cyber attack** as "an attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information." The difference between an "attack" and a "cyber attack" is primarily one of method. A cyber attack is made via cyberspace, whereas an attack may include other methods such as physical attacks on information systems and their SCs. We consider the broader definition of "attack" in this survey.

The usage of the term cyberinfrastructure began in the late 1990s and its definition has developed since then (Stewart *et al*., 2010). We use the National Institute of Standards and Technology's definition of cyberinfrastructure (Smartgrid *et al*., 2010):

> **Cyberinfrastructure** includes electronic information and communications systems and services and the information contained in these systems and services. Information and communications systems and services are composed of all hardware and software that process, store, and communicate information, or any combination of all of these elements. Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types. Communications include sharing and distribution of information. For example: computer systems; control systems (e.g., supervisory control and data acquisition–SCADA); networks, such as the Internet; and cyber services (e.g., managed security services) are part of cyberinfrastructure.

Cyberinfrastructure includes Cyber-Physical Systems (CPSs), which are physical systems that can be controlled or monitored by computers. CPSs integrate computation, networking, and physical systems (National Science Foundation, 2019).

CI is essential to the functioning of the modern economy and society (Eldosouky *et al*., 2015). Cyberinfrastructure is closely related to CI, since many CI assets contain cyberinfrastructure and CPSs. To this end, CI is defined as follows (The US Government, 2001):

> **Critical infrastructure (CI)** means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

CI can be divided into multiple sectors. There is no universal classification of CI sectors, with different countries having their own ways of determining the CI sectors (Eldosousky *et al*., 2015). In this survey, we use the classification defined by the United States. In 2003, the National Strategy for Homeland Security (Bush, 2003) identified 13 critical sectors of CI. This number increased to 16 in an updated version released in The White House (2013b) and The Department of Homeland Security (2019):

1. Chemical.
2. Commercial facilities.
3. Communications.
4. Critical manufacturing.

5. Dams.
6. Defense industrial base.
7. Emergency services.
8. Energy.
9. Financial services.
10. Food and agriculture.
11. Government facilities.
12. Healthcare and public health.
13. Information technology.
14. Nuclear reactors, materials and waste.
15. Transportation systems.
16. Water and wastewater systems.

CI in all of these sectors rely on CPS and computer-based systems to monitor and control their day-to-day operations (Wang, 2010). Although not all CI functions are reliant on cyberinfrastructure, any CI that is fully or partially reliant on the Internet to function is prone to adversarial cyber attacks. For example, most financial transactions are electronic; electricity generation, and water and sewage controls are adjusted to match demand over the course of the day; air traffic is monitored and controlled with electronic air traffic control systems. This means CI in all sectors may face cybersecurity risks (Oman *et al.*, 2004; Wang, 2010). As a result, all sectors are included for consideration in this survey.

2.2. Mission areas

Cyberinfrastructure security can address different goals. These goals, also known as mission areas, address a variety of defensive actions that can be categorized in different ways. We base our categorization on the national preparedness mission areas as defined by the Department of Homeland Security and Federal Emergency Management Agency, since these agencies broadly consider critical infrastructure protection (The Department of Homeland Security, 2011). The five mission areas are:

1. Prevention: Avoiding, preventing, or stopping an attack. Prevention eliminates or limits the number of successful attacks, threats, or hazards that can cause harm to a network, industry, citizens, residents, or assets. Prevention includes all actions whose intention is to eliminate or prevent attacks, minimize the number of attacks, or decrease the probability of attacks progressing through a system.
2. Protection: Adopting appropriate safeguards to ensure functionality, availability, and the delivery of critical services. Protection involves planning, warning systems, risk management, and supply chain integrity and security.
3. Mitigation: Mitigating economic consequences, including damage to property, by lessening the impact of the attack. Mitigation reduces expected amount of damage associated with an attack, rather than the likelihood of an attack.
4. Response: Taking appropriate actions after an incident to protect property, data, and the environment, and to meet basic human needs. Responding quickly limits the damage caused to a CI's network, industry, or assets after an attack by implementing corrective actions.
5. Recovery: Timely restoration of capabilities and services after an incident.
   These mission areas are closely aligned with those used by NIST (National Institute for Standards and Technology, 2018). We consider a sixth category that seeks to improve the detection of attacks as a separate mission area:
6. Detection: Identifying the occurrence of a cybersecurity event and/or attack.

We partition these mission areas into three groups based on when a defensive action is intended to occur, either before, during, or after an attack. The categories we use are defined as follows:

1. **Proactive planning**: Mission areas whose defensive actions are taken before an attack occurs. These mission areas are:
   - Prevention/Protection
   - Mitigation
2. **Real-time operational planning**: Mission areas whose required actions are taken during or immediately after an attack. These mission areas are:
   - Detection
   - Response
3. **3. Recovery planning**: Mission areas whose required actions occur after an attack. This mission area is:
   - Recovery

2.3. Optimization concepts

Optimization provides a series of tools and methods to identify a cost-effective set of actions to improve cybersecurity. Optimization helps determine efficient defensive planning to mitigate or protect against any type of attack, detection or response strategies, and cost-effective recovery planning.

Optimization involves finding an optimal solution that maximizes or minimizes an objective function in a decision-making model in which quantitative techniques or methods can be applied. Optimization identifies an optimal solution in a set of feasible solutions according to a predefined objective function that can reflect a wide range of security measures (Haidar, 2016). Optimization captures a broad set of models and methods. **Optimization models** can include linear programming, integer programming, nonlinear programming, multi-level optimization, multi-objective programming, stochastic optimization, Markov decision processes, and game theory, among others. **Optimization methods** consist of **exact** methods that are guaranteed to find an optimal solution (e.g., dynamic programming and Dijkstra's algorithm), and **non-exact** methods that identify near-optimal solutions, but do not guarantee the optimality of the solution. Many non-exact methods are highly efficient

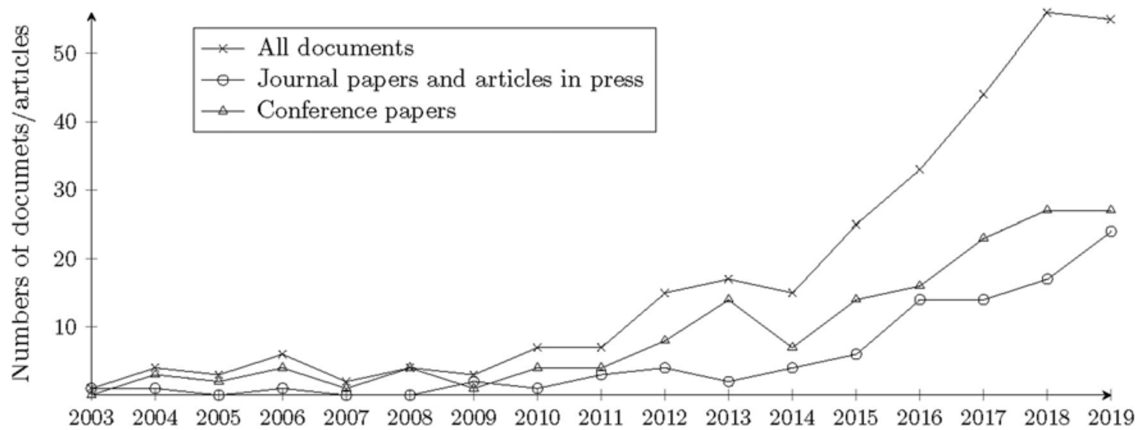

Figure 1. Numbers of documents, journal articles, and conference papers until December 31st, 2019.

in finding near-optimal solutions in a short period of time, which makes them useful in a practice for identifying near-optimal solutions to large-scale problem instances.

We divide non-exact methods into approximation, heuristic, and metaheuristic algorithms. **Approximation algorithms** return feasible solutions within polynomial time and space whose objective function values are proven to be within a certain ratio of the optimal solution value (Vazirani, 2013). **Heuristics** (e.g., greedy algorithms) and **metaheuristics** (e.g., genetic algorithm, particle swarm optimization, tabu search) are not typically guaranteed to return an optimal, close-to-optimal, or even feasible solution. For inclusion in this survey, a study must use at least one optimization model (e.g., linear programming, integer programming, or nonlinear programming) or method (e.g., dynamic programming, Benders decomposition, genetic algorithm), and focus on defensive planning for protecting cyberinfrastructure, or mitigating the risk to the CI's cyber components by timely attack detection and appropriate responses. These are discussed more in the following section.

Next, we discuss how we identified relevant documents to include in this survey.

3. Search process

Although there have been survey papers regarding the cybersecurity of CI before (e.g., Ten *et al.* (2010)), in this survey, we review papers that specifically utilize optimization within the context of cyberinfrastructure security. We searched Scopus for all English documents related to optimization in cyberinfrastructure security. After testing multiple combinations of keywords, we narrowed down our search to all English documents whose abstracts, titles, or keywords include "infrastructure"; either of "cyber" and "security", "cybersecurity", and "cyber-security"; and one of these words: "optimization", "optimisation", "optimal", "optimize", "optimise", "optimized", or "optimised". Note that in this article, we consider all the studies that were published or in press in peer-reviewed journals by the end of 2019; therefore, we excluded year 2020. Thus, our final query is:

TITLE-ABS-KEY (("**Cyber**" AND "**security**") OR "**Cybersecurity**" OR "**Cyber-Security**") AND TITLE-ABS-KEY (infrastructure) AND TITLE-ABS-KEY ("**optimal**" OR"**optimization**" OR "**optimisation**" OR "**optimize**" OR "**optimise**" OR "**optimized**" OR "**optimised**") AND (EXCLUDE (PUBYEAR, 2020)) AND (LIMIT-TO (LANGUAGE, "**English**")

3.1. Documents' information

A total of 297 articles, published or accepted between 2003 and 2019, were found on on Scopus. Among these unique documents, 94 were journal articles (89 published and five in-press) and 159 were conference papers. Figure 1 plots all documents, the number of journal articles and articles in press, as well as the number of conference papers published in each year since 2003. The values presented for "all documents" include books, book chapters, reviews, and conference reviews, which are not surveyed in this article. There has been a notable increase in the number of published documents of all types in the last decade, indicating a high interest in the topic.

Tables 1 and 2 provide information on the 297 documents found via Scopus. In both tables, the numbers in parentheses show the numbers of documents within each category. The majority of the documents (54%) are conference papers and journal articles (30%). There are also five journal articles that are in-press and waiting to be published. As mentioned earlier, neither documents that were not peer-reviewed nor review papers are included in this survey. Such documents include conference reviews, which contain only the abstracts of papers accepted in a year for a specific conference, and books. Scopus classifies authorship based on the first author's affiliation. As a result, Table 1 lists the first author's affiliation and country of employment. The University of Illinois at Urbana-Champaign; George Emil Palade University of Medicine, Pharmacy, Science and Technology of Targu Mures; New York University; and Oak Ridge National Laboratory published the most documents (see the fourth column of the table), and the United States published the most documents by far (see the last column of Table 1), followed by China, the United Kingdom, India, and France.

Table 2 presents information regarding the documents' source titles and areas. The first section of the table presents the most common source titles, including journals and conferences, where the documents were published. The second

Table 1. Documents' information - Scopus's report in April 2020.

Year (#) [a]	*Document type (#)* [a5]	*First Author (#)* [a]	*First author's affiliation (#)* [a]	*Country (#)* [a]
2019 (55)	Article (89)	Zhu, Q. (6)	University of Illinois at Urbana-Champaign (6)	United States (131)
2018 (56)	Article in Press (5)	Genge, B. (5)	George Emil Palade University of Medicine, Pharmacy, Science and Technology of Targu Mures (5)	China (22)
2017 (44)	Conference (159)	Haller, P. (4)	New York University (5)	United Kingdom (15)
2016 (33)	Conference Review (28)	Wang, L. (4)	Oak Ridge National Laboratory (5)	India (13)
2015 (25)	Book Chapter (14)	Chen, J. (3)	University of Toledo (4)	France (11)
2014 (17)	Book (3)	Myrda, P.T. (3)	Massachusetts Institute of Technology (4)	Germany (8)
2013 (15)	Review (2)	Novosel, D. (3)	Pacific Northwest National Laboratory (4)	Greece (8)
2012 (7)	Undefinded (2)	Rao, N.S.V. (3)	University of California, Berkeley (4)	Singapore (8)
2011 (7)		Sandberg, H. (3)	University of Southern California (4)	Romania (8)
2010 (3)		Tates, D. (3)	Austrian Institute of Technology (4)	South Korea (8)
2009 (3)		Udren, E.A. (3)	Others (3^{-}) [b]	Canada (7)
2008 (4)		Zheng, K. (3)[b]		Italy (7)
2007 (2)		Others (3^{-})		Australia (5)
2006 (6)				Switzerland (7)
2005 (3)				Austria (6)
2004 (4)				Iran (6)
2003 (1)				Spain (6)
				Others (5^{-}) [b]

[a] Numbers in parentheses represent the numbers of documents associated with that subcategory (e.g., there are 44 documents published in 2017).
[b] "Other" represents other subcategories with less than three or five documents.

Table 2. Most common document source titles and areas.

Studies' category	*Studies' subcategory (#)* [a]
Source title	- *Lecture Notes in Computer Science Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics* (19) - *IEEE Transactions on Smart Grid* (9) - *Advances in Intelligent Systems and Computing* (7) - *ACM International Conference Proceeding Series* (6) - *IEEE Access* (5) - *Communications in Computer and Information Science* (4) - *IEEE Control Systems* (4) - *IET Conference Publications* (4) - *International Journal of Critical Infrastructure Protection* (4) - Others (4^{-}) [b]
Source area	- Computer Science (206) - Engineering (139) - Mathematics (67) - Energy (38) - Social Sciences (30) - Decision Sciences (26) - Physics and Astronomy (12) - Business, Management and Accounting (9) - Materials Science (9) - Medicine (8) - Economics, Econometrics and Finance (5) - Earth and Planetary Sciences (4) - Chemical Engineering (3) - Environmental Science (3) - Others (3^{-}) [b]

[a] Numbers in parentheses represent the number of documents associated with that subcategory.

section of the table shows the numbers of articles by the academic area of their source. The most popular areas are computer science (206 documents), engineering (139 documents), and mathematics (67 documents). Some documents may be categorized in more than one area (e.g., both engineering and mathematics).

3.2. Selected studies

After finalizing the search, the three authors reviewed the documents for their relevance to optimization in cyberinfrastructure security. At least two of the authors agreed on the relevance of each study for it to be included in this survey. To be selected, each study had to be related to improving the cybersecurity of CI using an optimization model and/or method mentioned in Section 2. In this survey, we only consider studies whose goals are to enhance the security of cyberinfrastructure or CI from adversarial cyber attacks for defensive planning. Therefore, we do not consider papers whose goals are to optimize attacks from the attackers' perspective. However, these papers may be used to model security problems and help better understand the behavior of attackers.

The authors also found three additional journal articles that are relevant to the scope of this survey but did not appear in the Scopus search because at least one of the keywords did not show up in their abstracts, titles, or keywords. Therefore, in total, 68 studies, including 40 journal articles

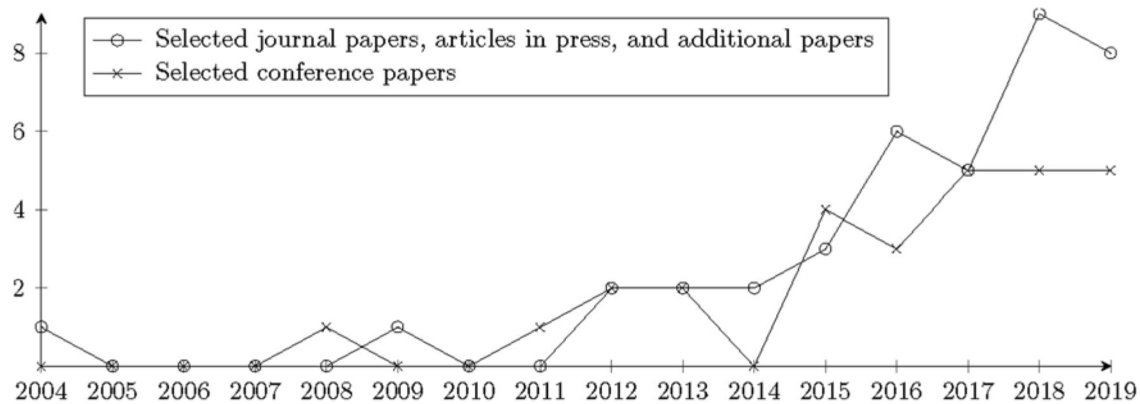

Figure 2. Numbers of the selected studies by the end of 2019.

(38 published or accepted and two additional papers) and 28 conference papers, met our inclusion criteria. These studies are discussed in the next section.

Figure 2 shows the number of selected journal articles and selected conference papers' publications by year. The figures indicate how improving cyberinfrastructure security for CI has attracted more interest in recent years, especially within the past 5 years.

4. Classifications of selected studies

In this section, we classify the selected studies based on their applications, their goals (i.e., mission areas), and the optimization techniques used. We first discuss what CI sectors are studied and what are the most and least popular sectors in the selected studies. Then, we explain what mission areas the selected studies address and the pattern they have had in the past years. Finally, we discuss what optimization techniques (i.e., models and methods) have been used in the selected studies to solve their problems.

4.1. Applications and real-world cases

In this section, the selected studies are categorized based on their real-world applications. As mentioned in Section 2.1, all CI sectors rely on cyberinfrastructure and are prone to attacks against both their cyber or cyber-physical components. These attacks may originate from a variety of sources, such as other CI sectors or trusted consumers (Puzis *et al.*, 2008). As shown in Table 3, we associate each of the selected study's application to one of the 16 different CI sectors described in Section 2.1. Table 3 shows the seven of the 16 CI sectors that have been studied in at least one of the selected studies. The other nine sectors listed in Section 2 have not been specifically addressed by the selected studies for cybersecurity. The second and third columns show the relevant studies and their specific applications in detail, respectively. The majority of studies are related to energy and Information Technology (IT), with significantly fewer studies pertaining to communications, transportation systems, and other CI sectors. This is primarily because the other CI sectors are directly or indirectly dependent on information technology and energy networks (Ravishankar *et al.*, 2018) and the reliance has made them a target of study (Amini, 2018). The other, lesser studied CI sectors provide directions for possible future study.

In recent years, power systems have been upgraded due to the integration of IT and metering infrastructures. These so-called "smart grid" features enable operators to monitor the system and take necessary actions in real-time to avoid failures (Khanna *et al.*, 2017). Modern power systems are cyber-physical systems that are subject to cyber attacks (Rass *et al.*, 2017).

For example, Vukovic *et al.* (2012) study data integrity in a power system state estimator and test the efficiency of their algorithm on IEEE 118 and 300 bus benchmark power systems. Ma *et al.* (2013) focus on protecting smart grid communication networks against cyber attacks that are intended to maximize the drop in the electricity market price and Zhang *et al.* (2013) attempt to increase the security of a smart grid by optimizing the placement of trust nodes. Kołodziej *et al.* (2014) address energy consumption in computational grids for the scheduling and execution of independent tasks in the grid environment while being under pre-specified security requirement constraints defined by their users. Kapourchali *et al.* (2016) develop a reliability model to determine how faults in the energy infrastructure can be detected while minimizing investment and customer service interruption costs.

IT is the second most popular CI sector among the selected studies. However, only some of the many studies with IT applications are directly related to IT systems. For example, Rass *et al.* (2017) use a game-theoric model to find better methods to protect against cyber intrusions on an IT system, Haller and Genge (2017) develop a methodology designed to detect system intrusion into industrial cyber-physical systems, and Miao *et al.* (2018) design detection and defense policies for cyber-physical systems against multiple types of attacks. Other studies are only indirectly related to these IT systems. For example, Young *et al.* (2016) determine how the insurance industry can provide quantitative estimates of its cyber risk while limiting its cybersecurity expenditures; and Bouet *et al.* (2015) study a virtual Deep Packet Inspection (vDPI) placement problem with a given traffic demand. They seek the best vDPI engine deployment that minimizes overall cost.

Table 3. Selected studies categorized by their applications.

Applications	*Selected studies*	*Specific applications*
	Puzis *et al.* (2008)	Intercommunication CI systems
3- Communications	El-Alfy and Al-Obeidat (2015)	Wireless mobile networks
	Genge and Haller (2016)	Modern industrial control systems communication infrastructure
	Kochedykov *et al.* (2018)	Infocommunication network and telecommunication infrastructure
6- Defense industrial base	Ravishankar *et al.* (2017)	Delay tolerant wireless network
	Salmeron *et al.* (2004)	Electric power systems
	Anwar *et al.* (2009)	Power grid: Midwestern US Electric Power System
	Vukovic *et al.* (2012)	Power system
	Zhang *et al.* (2012)	Smart grid
	Zhang *et al.* (2013)	Smart grid
	Ma *et al.* (2013)	Smart grid communication networks
	Kołodziej *et al.* (2014)	Computational grids
	Yuan *et al.* (2014)	Power grid
	Anwar *et al.* (2015)	Smart grid
	Ismail *et al.* (2015)	Electrical infrastructures
	Wang and Hou (2015)	Power systems
	Darwish *et al.* (2015)	Smart grid
8- Energy	Darwish *et al.* (2016)	Smart grid, SCADA
	Mishra *et al.* (2016)	Smart grid
	Kapourchali *et al.* (2016)	Power distribution system
	Rana *et al.* (2016)	Smart grid communication networks
	Khanna *et al.* (2017)	Smart grid
	Zeraati *et al.* (2018)	Power system and communication network
	Wei *et al.* (2018)	Power grid
	Xiang *et al.*(2018)	Power grid
	Wang *et al.* (2018)	Smart grid
	Liu *et al.* (2018)	Smart electricity meter in smart grid
	Wadhawan and Neuman [(2018)	Smart grid
	Haghnegahdar and Wang (2019)	Smart grid
	Pilz *et al.* (2019)	Smart grid
	Wang *et al.* (2019)	Power grid
	Mashima *et al.* (2019)	Smart grid
	Guan and Wang (2019)	Power grid
	Gao *et al.* (2019)	Power system
11- Government facilities	Eldosouky *et al.* (2015)	Control centers (e.g., government agency)
	Bedi *et al.* (2011)	IT and infrastructure: transmission control protocol
	He *et al.* (2012)	Cyber-physical network infrastructure
	Yuan *et al.* (2013)	Infrastructure control systems
	Patterson *et al.* (2013)	Water cillers that regulates the temperature of a super-computer
	Bouet *et al.* (2015)	Network function virtualization and IT systems
	Rao *et al.* (2016)	Cyberinfrastructure
	Young *et al.* (2016)	Smart critical infrastructure in insurance industry
	Canzani and Pickl (2016)	Information technology
	Filiol and Gallais (2016)	Information and telecommunications (the electrical power grid of the US)
13- Information technology systems	Rass *et al.* (2017)	IT cyber systems
	Haller and Genge (2017)	Industrial cyber–physical systems
	Alcaraz *et al.* (2017)	Cyber-physical control systems
	Barreto *et al.* (2017)	Firms' information technology infrastructure
	Chen *et al.* (2017)	Infrastructure networks
	Milošević *et al.* (2017)	Industrial control systems
	Ravishankar *et al.* (2018)	Critical Infrastructure
	Miao *et al.* (2018)	Cyber-physical systems
	Sokri (2018)	Information and communication technologies
	Panfili *et al.* (2018)	Cyber-physical system defense
	Li *et al.* (2019)	Industrial control systems
	Priyanga *et al.* (2019)	SCADA Systems
	Sándor *et al.* (2019)	Modern industrial control systems
	Zheng *et al.* (2019)	Information systems
	Zheng and Albert (2019)	Information technology infrastructure
	Zheng and Albert(2019)	Information technology
	Cano *et al.* (2016)	Airports
	Reilly *et al.* (2016)	Freeway traffic control systems
15- Transportation systems	Pan *et al.* (2017)	Vehicle network
	Mousavian *et al.* (2018)	Electric vehicle
	Kushal *et al.* (2018)	Shipboard power system
	Weaver and Marla (2019)	Modern shipping ports
16- Water and networks systems	Turner *et al.* (2012)	Water distribution

Table 4. Selected studies categorized by their mission areas.

Year	Selected studies	*Proactive planning*		*Real-time operational planning*		*Recovery planning*
		Prevention/Protection	*Mitigation*	*Detection*	*Response*	*Recovery*
2004	Salmeron *et al.*	X				
2008	Puzis *et al.*			X		
2009	Anwar *et al.*	X				
2011	Bedi *et al.*	X				
2012	Vukovic *et al.*		X			
	Turner *et al.*		X			
	He *et al.*		X			
	Zhang *et al.*			X		
2013	Zhang *et al.*			X		
	Ma *et al.*	X				
	Yuan *et al.*		X			
	Patterson *et al.*	X	X	X		
2014	Kołodziej *et al.*		X		X	
	Yuan *et al.*		X			
	Bouet *et al.*			X		
	El-Alfy and Al-Obeidat			X		
	Anwar *et al.*		X			
2015	Ismail *et al.*	X				
	Eldosouky *et al.*	X				
	Wang and Hou	X				
	Darwish *et al.*		X	X		
	Darwish *et al.*		X			
	Mishra *et al.*			X		
	Rao *et al.*	X				
	Cano *et al.*	X				
	Young *et al.*		X			
2016	Reilly *et al.*		X			
	Kapourchali *et al.*				X	
	Wei *et al.*	X			X	
	Canzani and Pickl	X				
	Filiol and Gallais		X			
	Genge and Haller		X			
	Rana *et al.*	X				
	Rass *et al.*			X		
	Haller and Genge			X		
	Ravishankar *et al.*			X		
	Khanna *et al.*	X				
2017	Alcaraz *et al.*					X
	Pan *et al.*			X		
	Barreto *et al.*	X		X		
	Chen *et al.*	X				X
	Milošević *et al.*	X				
	Ravishankar *et al.*				X	
	Miao *et al*				X	
	Xiang *et al.*		X			
	Mousavian *et al.*				X	
	Wang *et al.*			X		
	Zeraati *et al.*				X	
2018	Kushal *et al.*			X	X	
	Sokri	X				
	Liu *et al.*	X				
	Kochedykov *et al.*		X			
	Panfili *et al.*	X				
	Wadhawan and Neuman	X				
	Haghnegahdar and Wang			X		
	Pilz *et al.*			X		
	Priyanga *et al.*			X		
	Li *et al.*				X	X
	Sándor *et al.*		X			
2019	Zheng and Albert	X	X			
	Zheng and Albert	X				
	Zheng *et al.*	X				
	Weaver and Marla		X			
	Wang *et al.*		X			
	Mashima *et al.*	X				
	Guan and Wang		X			
	Gao *et al.*	X				

Communications is another CI sector that has been a focus of many of the selected studies. IT and communication systems are often integrated, and therefore, the differentiation between these two types of CI is nuanced and unclear. For the purposes of this survey, we assume that IT infrastructure is concerned with the movement or sharing of data between computers and communications infrastructure is concerned with the movement or sharing of information between people. As a result, the selected studies in the communications sector focus on telecommunications and wireless communications networks. For example, Puzis *et al.* (2008) study how distributing network intrusion detection systems within public communication infrastructures can protect intercommunication CI systems and Kochedykov *et al.* (2018) maximize communication in a telecommunications infrastructure by developing an optimal switching method to mitigate the effects of cyber attacks.

Only a few studies address transportation systems across any of the different modes of transportation (e.g., air, land, water). For example, Cano *et al.* (2016) analyze security allocation plans for an airport to protect against terrorists attempting to sabotage the airport's operations. Reilly *et al.* (2016), on the other hand, consider how a freeway's ramp metering control systems may be exploited by modeling the ramp metering control system's relationship to the underlying physical and cyberinfrastructures. Mousavian *et al.* (2018) propose a response approach for malware spreading from infected electric vehicles during charging. Kushal *et al.* (2018) minimize the impact of cyber attacks on shipboard power system operations.

There are only a few papers that address cybersecurity related to other CI sectors. For example, Ravishankar *et al.* (2017) optimize communications on a delay-tolerant-network primarily with applications to the military. Eldosouky *et al.* (2015) solve a resource allocation problem in which a control center (e.g., government agency) designs security protection contracts to offer to different CI owners. Finally, Turner *et al.* (2012) consider how to pressurize water networks to mitigate the effects of an attack.

One important future direction of research is to study cybersecurity aspects of CI sectors that have not been addressed as well. This is despite cyber attacks in some sectors, such as nuclear reactors (e.g., Stuxnet's cyber attack on Iran's nuclear program in Natanz (Rice and Shenoi, 2017)) or healthcare and public health (e.g., five massive data breaches reported by Anthem Inc., Excellus Health Plan, Premera Blue Cross, UCLA Health, and Medical Informatics Engineering in 2015 (Becker's Hospital Review, 2015). These attacks pose clear risks to national security, have potentially large economic consequences, and could expose large amounts of patient-sensitive data, but they have not been a primary target of study using optimization. Therefore, these areas may benefit well from future research.

4.2. Mission areas

A variety of objectives can be defined for enhancing cybersecurity of CI, since security can be improved by a variety of mechanisms based on the goal. In this subsection, the selected studies are categorized based on how and when they intend to take defensive actions against cyber attacks. We base these categories on the national preparedness mission areas as defined by the Department of Homeland Security. The Department of Homeland Security (2011) introduced in Section 2.2. Recall that the mission areas are partitioned into three groups based on when a defensive action is intended to occur (i.e., before, during, or after an adversarial cyber attack) as follows:

1. Proactive planning including prevention/protection and mitigation.
2. Real-time operational planning including detection and response.
3. Recovery planning including recovery.

Table 4 summarizes the selected studies' mission areas. Each study is assigned to at least one mission area. However, the goal of some studies is to balance investments between different mission areas (e.g., trying to prevent intrusions, detect cyber adversarial attacks, and mitigate the attackers' physical effects on computer controlled equipment) (Patterson *et al.*, 2013). Therefore, some studies are assigned to more than one mission area (e.g., Patterson *et al.* (2013) and Kushal *et al.* (2018)).

Proactive planning has been the most consistently studied among the three groups. There are many studies within this group whose sole objective is to protect CI against cyber attacks (Anwar *et al.*, 2009; Ma *et al.*, 2013; Rao *et al.*, 2016). For example, Rao *et al.* (2016) model the strategic interactions between an attacker and a defender using game-theoretic models to minimize the probability of a successful attack. Ma *et al.* (2013) model a problem in which the defender tries to protect a smart grid by protecting the energy market against adversarial attackers who seek to disrupt equilibrium market pricing. Others examine cybersecurity planning problems, where a defender selects mitigations that reduce the risk of attacks originating in IT supply chains (Zheng and Albert, 2019b; Zheng *et al.*, 2019).

Some of the selected studies assess how to proactively reduce the impact of adversarial cyber attacks through consequence mitigation (Turner *et al.*, 2012; Vukovic *et al.*, 2012; Yuan *et al.*, 2013; Yuan *et al.*, 2014) rather than reduce the probability of their success. These consequence mitigation efforts can enhance security in many CI sectors. For instance, Vukovic *et al.* (2012) try to mitigate attacks against a critical power system, whereas Turner *et al.* (2012) attempt to mitigate the effects of physical destruction caused by cyber attacks on a water network. Yuan *et al.* (2013) study how to mitigate the effects of cyber attacks on the communication channels of a control system to maintain an acceptable level of operation after an attack. Yuan *et al.* (2014) solve a budgeted problem in which defenders allocate resources to a power grid system to minimize the effect of cyber attackers who seek to maximize the load shed in the system by disconnecting transmission lines. Similarly, Zheng and Albert (2019a) explore how to select an optimal portfolio of mitigations to maximally delay attacks against critical infrastructure. Some journal articles share a similar purpose to those included in this survey, but are not directly related to the cybersecurity of CI and are not included in the tables. For example, Nandi *et al.* (2016) studies how a defender deploys security countermeasures to protect their

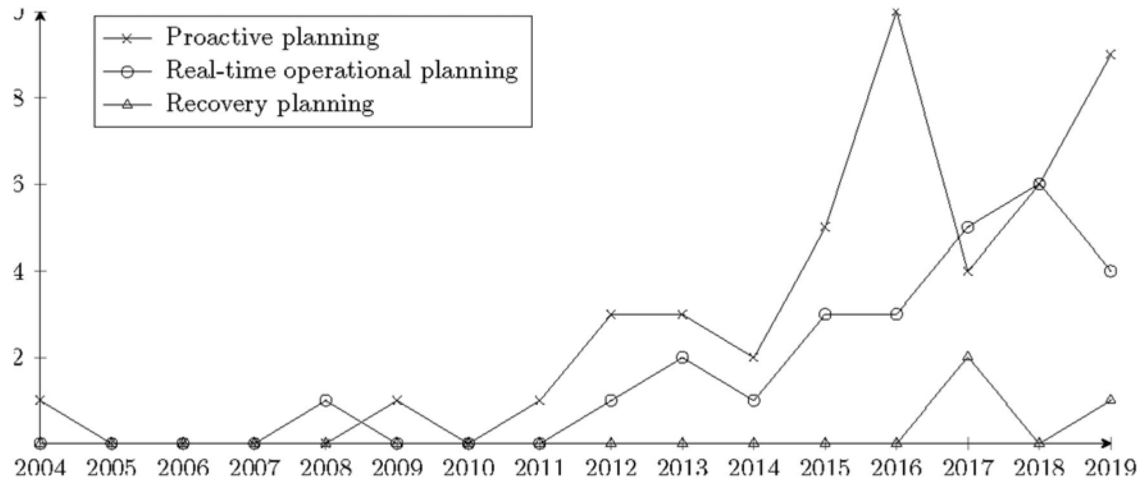

Figure 3. Number of studies published within each mission area group by year.

organization and minimize losses caused by security breaches.

The second most popular group of mission areas among the selected studies is real-time operational planing. These papers have focused on how to efficiently detect or respond to a cyber intrusion in CI. This has most commonly taken the form of improving the ability of defenders to detect attacks using optimization (Zhang *et al.*, 2013; Haller and Genge, 2017; Khanna *et al.*, 2017; Rass *et al.*, 2017; Ravishankar *et al.*, 2017). For instance, Zhang *et al.* (2013) study how an intrusion in a smart grid can be detected by placing trust nodes while Ravishankar *et al.* (2017) introduce a defense model to detect jamming attacks in a delay-tolerant wireless network. Only recently has significant attention also been given to determining how to respond when these attacks are detected (Mousavian *et al.*, 2018; Zeraati *et al.*, 2018). For instance, Zeraati *et al.* (2018) develop a bi-level optimization model to formulate a responsive defense system for a power system and communication network in the upper level problem. The lower level problem deals with how the damage that was done by attackers can be minimized through the corrective responsive actions (e.g., changing the production level of generation units or the load shed).

Among the three groups of mission areas, recovery planning has been studied the least, with only the recent publication of two papers within this area (Alcaraz *et al.*, 2017; Chen *et al.*, 2017). Planning how to effectively recover from successful attacks is important in two ways. First, recovery planning can reduce the consequences of a successful attack. This can be achieved by a variety of methods, such as increasing redundancy in data storage. Second, recovery also involves securing data and infrastructure after an attack as, well as prioritizing systems when returning cyberinfrastructure to normal operations. These latter issues are important, since there are typically large economic consequences when a system is not available for normal operations. For these reasons, recovery planning remains a worthwhile topic of future study.

As previously mentioned, some studies simultaneously consider multiple mission areas. For example, Kushal *et al.* (2018) attempt to both detect cyber intrusions and immediately minimize the damage caused by the intrusion with an effective response. Both of these mission areas consider how to react when an attack takes place and therefore, are found within the second group (i.e., real-time operational planning). On the other hand, Patterson *et al.* (2013) address mission areas concerned both with actions taken before and during attacks. Their objectives are to allocate a budget to investments that protect super-computer chillers from cyber attacks, mitigate the physical effects of successful attacks, and detect intrusions into the system.

The economics of cyber investments is another aspect considered by many other studies not selected for this survey, due to lack of relevance to cyberinfratructure. Some of these studies proactively plan investment allocations so that firms' security levels are adequate to the threat that they face. For instance, Zhuo and Solak (2014) solve a cybersecurity problem related to the stochastic investment allocation problem of determinining optimal cybersecurity investment levels to protect firms against attacks. Nagurney *et al.* (2015) plan security investments from retailers' perspective. The retailers select their supply chain security levels and investment plans to maximize their final profits. In the event of a cyber attack, their security is correlated to other retailers' security investments. They extend this idea to study the effects of cooperation and competition between firms (Nagurney and Shukla, 2017). Finally, Barreto and Cárdenas (2017) propose a Markov decision process model for an insurance market that uses incentives for defenders (i.e., asset owners) to more efficiently protect themselves against cyber attacks by proper investment management.

As depicted in Table 4, studies have primarily focused on protection, mitigation, and detection. However, within the past 10 years, papers have addressed how to quickly and effectively respond to attacks and efficiently recover CI from attacks. Figure 3 illustrates the number of studies within each group of mission areas as a function of time. Comparing to proactive planning, real-time operational planning has shown a more consistent increase in the past decade. Recovery is the newest mission area to be considered, with only two studies in 2017 (Alcaraz *et al.*, 2017;

Table 5. Selected studies categorized by the optimization model utilize.

Models	*Documents*
Game Theory	Darwish *et al.* (2016)
	Rao *et al.* (2016)
	Cano *et al.* (2016)
	Rass *et al.* (2017)
	Ravishankar *et al.* (2017)
	Ravishankar *et al.* (2018)
	Wei *et al.* (2018)
	Miao *et al.* (2018)
	Bedi *et al.* (2011)
	He *et al.* (2012)
	Yuan *et al.* (2013)
	Ismail *et al.* (2015)
	Darwish *et al.* (2015)
	Canzani and Pickl (2016)
	Pan *et al.* (2017)
	Chen *et al.* (2017)
	Sokri (2018)
	Liu *et al.* (2018)
	Panfili *et al.* (2018)
	Pilz *et al.* (2019)
	Wang *et al.* (2019)
	Guan and Wang (2019)
LP	Eldosouky *et al.* (2015)
MIP	Anwar *et al.* (2009)
	Vukovic *et al.* (2012)
	Zhang *et al.* (2013)
	Bouet *et al.* (2015)
	Mishra *et al.* (2016)
	Reilly *et al.* (2016)
	Haller and Genge (2017)
	Mousavian *et al.* (2018)
	Zhang *et al.* (2012)
	Genge and Haller (2016)
	Milošević *et al.* (2017)
	Zheng *et al.* (2019)
	Weaver and Marla (2019)
NP	Turner *et al.* (2019)
	Young *et al.* (2016)
	Wang *et al.* (2018)
	Patterson *et al.* (2013)
	Wang and Hou (2015)
	Sokri (2018)
Bi-level optimization	Khanna *et al.* (2017)
	Salmeron *et al.* (2004)
	Zeraati *et al.* (2018)
	Kushal *et al.* (2018)
	Zheng and Albert(2019a)
	Gao *et al.* (2019)
SO	Zheng and Albert (2019a)
	Zheng and Albert (2019b)
	Zheng *et al.* (2019)
Tri-level optimization	Yuan *et al.* (2014)
Semidefinite programming	Rana *et al.* (2016)
MOO	Reilly *et al.* (2016)
	Li *et al.* (2019)
	Sándor *et al.* (2019)
MDPs	Ma *et al.* (2013)
	Barreto *et al.* (2017)
	Wadhawan and Neuman (2018)
	Gao *et al.* (2019)

Chen *et al.*, 2017) and one in 2019 (Li *et al.*, 2019). It remains to be seen whether this will be a major topic of study in future years.

4.3. Optimization models and methods

Each of the selected studies uses at least one optimization model and/or method. Different models and methods may be used to identify optimal or near-optimal solutions. These models and methods, listed and described in Section 2.3, are categorized as follows:

Optimization models:

1. Linear programming
2. Mixed integer programming
3. Nonlinear programming
4. Bi-level optimization
5. Tri-level optimization
6. Stochastic programming
7. Game theory
8. Multi-objective programming
9. Markov decision processes
10. Semidefinite programming

Optimization methods:

Exact methods (e.g., dynamic programming, branch-and-bound, Dijkstra's algorithm, column generation)

Non-exact methods

1. Approximation algorithms
2. Heuristic algorithms
3. Metaheuristic algorithms (e.g., genetic algorithm, particle swarm optimization)

Tables 5 and 6 summarize the selected studies that utilize optimization models and methods, respectively. Game theory was used by a plurality of studies. Game theory makes use of mathematical models to capture the strategic interactions between two or more rational decision-makers (Myerson, 2013). Studies often seek to find Nash equilibria, which are strategies in which no single player can gain a benefit by changing to a different strategy (Osborne and Rubinstein, 1994). For example, in seeking to model the relationship between infrastructure protection and recovery, Chen *et al.* (2017) characterize the defender and attacker strategies by finding subgame perfect Nash equilibria. On the other hand, other studies may use the same concept for different purposes (Bedi *et al.*, 2011; Rao *et al.*, 2016; Chen *et al.*, 2017; Miao *et al.*, 2018; Panfili *et al.*, 2018). For instance, Panfili *et al.* (2018) use the concept to model how a defender can protect CI by minimizing the damage caused by attackers.

Mixed integer programming (MIP) is the second most popular type of optimization model utilized by the studies in this survey. MIPs are mathematical optimization programs in which a portion or all of the variables are restricted to be integer (e.g., {2,3,4}, or {0,1}) and have constraints that contain only linear relationships. For example, Zhang *et al.* (2013), extending the work done by Zhang *et al.* (2012), define a set packing MIP problem where the defender places trust nodes in a smart grid network to minimize the cost of communication routing. They use Dijkstra's algorithm to find the route with the minimum cost between two nodes and make use of this solution to develop a heuristic approach to solving the problem. Bouet

Table 6. Studies categorized by the solution methods utilized.

Methods	*Selected studies*	*Method description*
Exact methods	Anwar *et al.* (2009)	Dynamic programming knapsack problem
	Zhang *et al.* (2013)	Dijkstra's algorithm–shortest path routing
	Ma *et al.* (2013)	Dynamic programming for solving the Markov game
	Mishra *et al.* (2016)	Dynamic programming
	Khanna *et al.* (2017)	Quadrature programming
	Xiang *et al.* (2018)	Primal-dual interior point method
	Yuan *et al.* (2014)	Column-and-Constraint Generation algorithm
	Zhang *et al.* (2012)	Dijkstra's algorithm
	Filiol and Gallais (2016)	Minimum vertex cover algorithm: Dharwadker algorithm
	Barreto *et al.* (2017)	Dynamic programming
	Kochedykov *et al.* (2018)	Numerical algorithm
Non-exact methods	**Approximation Algorithms**	
	Ma *et al.* (2013)	Pruning algorithm
	Mishra *et al.* (2016)	Approximation algorithm
	Milošević *et al.* (2017)	Approximation algorithms
	Zheng *et al.* (2019)	Greedy approximation algorithms
	Heuristic	
	Bouet *et al.* (2015)	Centrality-based greedy placement algorithm and Dijkstra algorithm
	Anwar *et al.* (2015)	Heuristic: hybrid clustering algorithm based on k-means
	Mishra *et al.* (2016)	Greedy algorithm: PIVOT algorithm & Particle Swarm Optimization
	Alcaraz *et al.* (2017)	Optimal reachability-based restoration approach
	Salmeron *et al.* (2004)	Decomposition-based heuristic
	Puzis *et al.* (2008)	Simple greedy heuristic with an approximation algorithm proof
	Mashima *et al.* (2019)	Near optimal heuristic algorithm
	Zheng and Albert (2019a)	Lagrangian heuristic
	Metaheuristics	
	Kołodziej *et al.* (2014)	Six genetic-based single- and multi-population metaheuristics
	El-Alfy and Al-Obeidat (2015)	Genetic algorithm
	Khanna *et al.* (2017)	Meta-heuristic technique
	Kapourchali *et al.* (2016)	Genetic algorithm
	Xiang *et al.* (2018)	Particle swarm optimization
	Zeraati *et al.* (2018)	Genetic algorithm
	Li *et al.* (2019)	Genetic algorithm
	Haghnegahdar and Wang (2019)	Whale optimization algorithm
	Priyanga *et al.* (2019)	Binary whale optimization algorithm
	Gao *et al.* (2019)	Particle swarm optimization

et al. (2015) formulate a virtual Deep Packet Inspection placement problem as a minimum-cost multi-commodity flow MIP problem. They too take advantage of Dijkstra's algorithm in a greedy placement algorithm to solve the problem and compare the results to the MIP optimal solutions for different networks. Milošević *et al.* (2017) develop a combinatorial MIP model for industrial control system's cybersecurity. They install layers of security measures to minimize the total risk due to cyber attacks without exceeding a budgetary knapsack constraint. They develop an approximation algorithm to solve the problem in polynomial time with guaranteed approximation bounds.

Linear Programming (LP) and Nonlinear Programing (NLP) are also widely used, with NLP models being more common. In contrast with MIP models, LP and NLP problems only use continuous variables. NLPs, unlike LPs and MIPs, include at least one constraint or an objective function that is nonlinear. For example, Patterson *et al.* (2013) formulate an NLP to model finding the best security plan for super-computer chillers within a budget. In their model, the objective function and the budget constraint are both written as nonlinear functions. Young *et al.* (2016) formulate an NLP to minimize the summation of the residual risks after implementing security controls in CI in the insurance industry.

Mixed Integer Nonlinear Programming (MINLP) models combine the properties of MIPs and NLPs, using integer and continuous variables as well as at least one nonlinear constraint or objective function. Only a few studies use MINLP models (Turner *et al.*, 2012; Wanf and Holt, 2015; Sokri, 2018). Turner *et al.* (2012) models a water network problem that seeks to minimize the weighted water shortage and water truck distribution costs as a MINLP. By relaxing the existing nonlinearities in their constraints, they solve the problem as a MIP.

Some mathematical optimization problems have more than one objective function. These problems usually do not have a single feasible solution that simultaneously optimizes all of the objective functions. Therefore, a number of *Pareto* optimal solutions are determined using Multi-Objective Optimization (MOO) or Multi-Objective Programming. A solution is Pareto optimal if none of the objectives may be improved without worsening another objective. Both Reilly *et al.* (2016) and Li *et al.* (2019) model their optimization problems with MOO. Reilly *et al.* (2016) develop a MOO model and obtain Pareto solutions in order to mitigate the effects of cyber attacks on freeway traffic control systems.

Li *et al.* (2019) use MOO to model how to respond to cyber intrusions in industrial control systems. Their maximization problem has an objective vector composed of multiple minor objectives (i.e., system, state, and security benefit). They implement a genetic algorithm to identify near-optimal model solutions.

An optimization problem may be modeled with two or more embedded problems reflecting multiple decision makers. Generally, in each level, a different player seeks to maximize or minimize their own objective given the other players choices. When two levels are used, it is called bi-level optimization, and when three levels are used, it is called tri-level optimization. Several selected studies (Salmeron *et al.*, 2004; Khanna *et al.* 2017; Kushal *et al.*, 2018; Zeraati *et al.*, 2018; Zheng and Albert, 2019a) make use of bi-level optimization to model a defender/attacker game structure. For example, Salmeron *et al.* (2004) use a bi-level formulation to model an interdiction optimization problem for electric power networks vulnerable to cyber attacks. In the lower level problem, the attacker seeks to attack the power network, whereas in the upper level problem, the defender maximizes the number of disrupted attacks subject to their limited resources. They develop a decomposition-based heuristic to solve the problem. Zheng and Albert (2019a) solve an project interdiction problem in which decision makers deploy mitigations to maximally delay multiple adverserial attacks when the delay times are uncertain.

In real-world problems, not all the parameters are always known with certainty. In some applications, Stochastic Optimization (SO) is used to model decisions when there is uncertainty in some model parameters (Heyman and Sobel, 2004). Zheng *et al.* (2019) and Zheng and Albert (2019b) model a planning problem to select a portfolio of security controls given that their effectiveness may be uncertain when considering expected value and worst-case objectives, respectively.

One recent study, Yuan *et al.* (2014), models a security problem as a tri-level optimization problem. They use a defender-attacker-defender structure for their model. In the top level problem, the defender allocates defensive resources to protect transmission lines in a power grid; in the middle level problem, the attacker tries to maximize the load shed of the power systems by disconnecting transmission lines; and in the lower level problem, modeled as an LP, the defender reacts to the attacker's disruptions by minimizing the load shed.

A Markov Decision Process (MDP) is an optimization tool that is useful for modeling systems in which decisions are made sequentially when some outcomes are stochastic and the system evolves stochastically according to those decisions (Puterman, 2014). Ma *et al.* (2013) use an MDP in a smart grid problem to model interactions between providers and attackers whose goal is to maximize the drop in the market price. Barreto *et al.* (2017) also utilize an MDP to model a two-player iterative game between a defender who tries to protect and an attacker who tries to compromise a firm's infrastructure.

Rana *et al.* (2016) use a Semi-Definite Program (SDP) to improve smart grid communication by adding redundancy and stabilizing the system state. In a SDP (Vandenberghe and Boyd, 1996), a linear objective function is minimized while the problem is subject to an affine combination of symmetric matrices being positive semidefinite. Since, the constraint is convex but not linear, an SDP is more general than an LP. However, SDPs can also be solved in polynomial time.

Simulation is not an optimization method, and therefore, we do not select studies that use simulation as their solution method. However, many of the selected studies use simulation to generate scenarios (Canzani and Pickl, 2016; Darwish *et al.*, 2016; Genge and Haller, 2016), verify their model, or validate their results (Puzis *et al.*, 2008; Bedi *et al.*, 2011; Zhang *et al.*, 2012; Zhang *et al.*, 2013; Eldosouky *et al.*, 2015; Cano *et al.*, 2016; Rana *et al.*, 2016; Panfili *et al.*, 2018; Ravishankar *et al.*, 2018; Li *et al.*, 2019). These papers use different models and methods (e.g., mixed integer programming, bi-level programming, and multi-objective optimization, heuristics) to solve their proposed models. Game theory is notably more popular among the papers that also use simulation (Bedi *et al.*, 2011; Cano *et al.*, 2016; Darwish *et al.*, 2016; Ravishankar *et al.*, 2017, 2018; Panfili *et al.*, 2018; Wei *et al.*, 2018)

Table 6 reports the solution methods divided into two categories: exact methods, which exactly solve optimization problems and reach a provably optimal solution (e.g., dynamic programming) and non-exact methods, which include approximation algorithms, heuristics, and metaheuristics. These methods are described in Section 2.3. Many studies do not develop an exact solution methodology for solving larger, more realistic problem instances. This introduces a gap in the literature that may be filled by scholars with an expertise in algorithm design. On the other hand, not all of the papers presented in Table 6 use optimization models, but may only use optimization methods to solve their problems. For example, Kapourchali *et al.* (2016) use a genetic algorithm to solve a power distribution system planning problem. This also provides an opportunity for scholars to work on the modeling of such problems.

Many journal articles not presented here utilize an attack graph or attack tree methodology to study network vulnerabilities. Most of these papers (Dewri *et al.*, 2007; Sawilla and Skillicorn, 2012; Almohri *et al.*, 2016; Nandi *et al.*, 2016) are not directly related to cyberinfrastructure, and therefore, they are not included in the tables and figures. However, they are worth noting as they may easily be applied to study cyberinfrastructure security as well. For example, Dewri *et al.* (2007) model an attack tree MOO problem, in which security hardening measures are selected, subject to a budgetary constraint, to minimize the residual damage. However, their network model is general and not specifically designed for enhancing the security of CI. Nandi *et al.* (2016) formulate a bi-level MIP model to identify an optimal interdiction decision for an attack graph. Their objective minimizes the losses caused by security breaches, but does not directly consider breaches within CI. Almohri *et al.* (2016) seek to reduce the probability of successful adversarial attacks by analyzing a probabilistic attack on general complex networks. Sawilla and Skillicorn (2012) provide decision support for network administrators by developing a method to minimize the connectivity of an attack graph. They develop a greedy algorithm that closely approximates the optimal solution.

5. Conclusions and further research

CI has become increasingly vulnerable to cyber attacks due to its increasing reliance on cyberinfrastructure. This has led to widespread recognition in the past two decades by scholars with a variety of expertises of the need to utilize optimization models and methods to improve the cybersecurity of CI. We present a survey of papers that apply optimization models and methods to improve cyberinfrastructure security. In this article, we surveyed 68 peer-reviewed studies (40 journal articles and 28 conference papers) that were published or accepted by the end of year 2019 and met our full inclusion criteria. The selected studies were classified based on their applications, mission areas, and the optimization models and methods utilized.

The energy sector and IT sector attracted the most attention among the selected studies. Far less attention has been paid to other sectors such as communications or transportation. Nine sectors had no studies that met the inclusion criteria (i.e., chemical, commercial facilities, dams, emergency services, financial services, food and agriculture, healthcare and public health, and nuclear reactors, materials, and waste). Scholars have consistently studied how to prevent, mitigate and detect cyber attacks. However, only in recent years have scholars also attempted to study how to quickly and effectively respond to or recover from adversarial cyber attacks on CI. Most scholars have used game theory, mixed-integer programming, or NLP to model the problem considered, although, a variety of other optimization methods have been used. No one solution method has predominated, although dynamic programming and genetic algorithms are the most popular exact and non-exact methods, respectively.

Due to the variety and complexity of CI systems and their supporting cyberinfrastructure systems, significant work remains to be done determining how to better protect cyberinfrastructure and CI against cyber attacks. Based on the results of this survey, we believe that some of the most advantageous directions for future research include:

1. Studying CI sectors other than energy and information technology, especially as other sectors become more reliant on cyber-physical systems.
2. Determining better ways to respond to and recover from cyber attacks in a timely manner. Despite the recent attention given to these areas, they remain understudied compared with protecting, mitigating, and detecting attacks.
3. Addressing the vulnerabilities introduced by the interactions between different CI sectors.

Funding

This work was funded by the National Science Foundation Awards 1422768 and 1912166. 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 National Science Foundation.

Acknowledgments

The authors would like to thank the anonymous reviewers whose suggestions for improvement led to a substantially improved manuscript.

Notes on contributors

Dr. Forough Enayaty-Ahangar received her PhD degree in industrial engineering from the University of Arkansas in 2017. She is currently a postdoctoral associate in the Department of Population Medicine and Diagnostic Sciences at Cornell University. Her research interests lie in the field of operations research, particularly the area of integer programming and its applications in supply chains such as food chains and illegal drug networks.

Laura A. Albert, PhD, is a professor of industrial & systems engineering and a Harvey D. Spangler Faculty Scholar at the University of Wisconsin-Madison. Her research interests are in the field of operations research, with a particular focus on discrete optimization with application to homeland security, critical infrastructure protection, and emergency response. She has authored or co-authored more than 60 publications in archival journals and refereed proceedings. She is an IISE Fellow. She has been awarded many honors for her research, including the INFORMS Impact Prize, four publication awards, a National Science Foundation CAREER award, a Fulbright Award, and a Department of the Army Young Investigator Award. She is a Department Editor for *IIE Transactions* and is on or has been on six other journal Editorial Boards. She is the author of the blogs "Punk Rock Operations Research" and "Badger Bracketology."

Dr. Eric DuBois obtained his PhD in industrial and systems engineering from the University of Wisconsin-Madison. He currently works as a research analyst at CNA using operations research to inform public policy decisions.

ORCID

Forough Enayaty-Ahangar http://orcid.org/0000-0001-7081-0525

References

Alcaraz, C., Lopez, J. and Choo, K.-K. R. (2017) Resilient interconnection in cyber-physical control systems. *Computers & Security*, **71**, 2–14.

Almohri, H.M., Watson, L.T., Yao, D. and Ou, X. (2016) Security optimization of dynamic networks with probabilistic graph modeling and linear programming. *IEEE Transactions on Dependable and Secure Computing*, **13**(4), 474–487.

Amini, M. (2018) Optimal dispatch of uncertain energy resources. PhD thesis, University of Vermont, Burlington, VT.

Anwar, A., Mahmood, A.N. and Tari, Z. (2015) Identification of vulnerable node clusters against false data injection attack in an AMI based smart grid. *Information Systems*, **53**, 201–212.

Anwar, Z., Montanari, M., Gutierrez, A. and Campbell, R.H. (2009) Budget constrained optimal security hardening of control networks for critical cyber-infrastructures. *International Journal of Critical Infrastructure Protection*, **2**(1-2), 13–25.

Armerding, T. (2018) The 17 biggest data breaches of the 21st century. https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html. (accessed 20 October 2018)

Barnett, B. (2019) Security news this week: An unprecedented cyberattack hit US power utilities. https://www.wired.com/story/power-grid-cyber-attack-facebook-phone-numbers-security-news/.

Barreto, C. and Cárdenas, A.A. (2017) Optimal risk management in critical infrastructures against cyber-adversaries, in *Proceedings of the IEEE Conference on Control Technology and Applications* IEEE Press, Piscataway, NJ, pp. 2027–2032.

Barreto, C., Cardenas, A.A. and Bensoussan, A. (2017) Optimal security investments in a prevention and detection game, in *Proceedings of the Hot Topics in Science of Security: Symposium and Bootcamp*, pp. 24–34. Q3

Becker's Hospital Review (2015) 5 biggest healthcare data breaches of 2015. https://www.beckershospitalreview.com/healthcare-information-technology/5-biggest-healthcare-data-breaches-of-2015.html. Q4

Bedi, H.S., Roy, S. and Shiva, S. (2011) Game theory-based defense mechanisms against ddos attacks on tcp/tcp-friendly flows, *in Proceedings of the IEEE Conference on Computational Intelligence in Cyber Security*, IEEE Press, Piscataway, NJ, pp. 129–136.

Bouet, M., Leguay, J., Combe, T. and Conan, V. (2015) Cost-based placement of VDPI functions in NFV infrastructures. *International Journal of Network Management*, **25**(6), 490–506.

Bush, G.W. (2003) The national strategy for the physical protection of critical infrastructures and key assets. Technical report, Executive Office of the President Washington DC.

Cano, J., Pollini, A., Falciani, L. and Turhan, U. (2016) Modeling current and emerging threats in the airport domain through adversarial risk analysis. *Journal of Risk Research*, **19**(7), 894–912.

Canzani, E. and Pickl, S. (2016) Cyber epidemics: Modeling attacker-defender dynamics in critical infrastructure systems, in *Advances in Human Factors in Cybersecurity*, Springer, Heidelberg, Germany, pp. 377–389.

Chen, J., Touati, C. and Zhu, Q. (2017) A dynamic game analysis and design of infrastructure network protection and recovery: 125. *ACM SIGMETRICS Performance Evaluation Review*, **45**(2),128. Q5

Committee on National Security Systems (2015) Committee on National Security Systems Glossary - CNSSI No. 4009. https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf. Q6

Darwish, I., Igbe, O. and Saadawi, T. (2015) Experimental and theoretical modeling of DNP3 attacks in smart grids. *36th IEEE Sarnoff Symposium*, IEEE Press, Piscataway, NJ, pp. 155–160.

Darwish, I., Igbe, O. and Saadawi, T. (2016) Vulnerability assessment and experimentation of smart grid DNP3. *Journal of Cyber Security and Mobility*, **5**(1), 23–54.

Dewri, R., Poolsappasit, N., Ray, I. and Whitley, D. (2007) Optimal security hardening using multi-objective optimization on attack tree models of networks. In *Proceedings of the 14th ACM Conference on Computer and Communications Security*, pp. 204–213. Q7

Edwards, N., Kao, G., Hamlet, J., Bailon, J. and Liptak, S. (2016) Supply chain decision analytics: Application and case study for critical infrastructure security, in *Proceedings of the 11th International Conference on Cyber Warfare and Security: ICCWS2016*, p. 98. Q8

El-Alfy, E.-S. M. and Al-Obeidat, F.N. (2015) Detecting cyber-attacks on wireless mobile networks using multicriterion fuzzy classifier with genetic attribute selection. *Mobile Information Systems*, 2015.

Eldosouky, A., Saad, W., Kamhoua, C. and Kwiat, K. (2015) Contract-theoretic resource allocation for critical infrastructure protection, in *Proceedings of the Global Communications Conference*. IEEE Press, Piscataway, NJ, pp.1–6.

Q9 EPIC (2019) Equifax data breach. https://epic.org/privacy/data-breach/equifax/.

Filiol, E. and Gallais, C. (2016) Combinatorial optimization of operational (cyber) attacks against large-scale critical infrastructures: The vertex cover approach, in *Proceedings of the International Conference on Cyber Warfare and Security*, p. 128. Q10

Gao, B., Shi, L. and Ni, Y. (2019) A dynamic defense-attack game scheme with incomplete information for vulnerability analysis in a cyber-physical power infrastructure.

Genge, B. and Haller, P. (2016) A hierarchical control plane for software-defined networks-based industrial control systems, in *Proceedings of the 2016 IFIP Networking Conference*, IEEE Press, Piscataway, NJ, pp. 73–81.

Gordon, L.A., Loeb, M.P. and Lucyshyn, W. (2003) Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy*, **22**(6), 461–485.

Guan, P. and Wang, J. (2019) Optimal adaptive coordinated cyber-attacks on power grids using-greedy method, in *Proceedings of the 2019 North American Power Symposium*, IEEE Press, Piscataway, NJ, pp. 1–5.

Haghnegahdar, L. and Wang, Y. (2019) A whale optimization algorithm-trained artificial neural network for smart grid cyber intrusion detection. *Neural Computing and Applications*, 1–15. Q11

Haidar, A.D. (2016) Operations research and optimization techniques, in *Construction Program Management–Decision Making and Optimization Techniques*, Springer, Heidelberg, Germany, pp. 131–157.

Haller, P. and Genge, B. (2017) Using sensitivity analysis and cross-association for the design of intrusion detection systems in industrial cyber-physical systems. *IEEE Access*, **5**, 9336–9347.

He, F., Zhuang, J. and Rao, N S. (2012) Game-theoretic analysis of attack and defense in cyber-physical network infrastructures, in *Proceedings of the IIE Annual Conference. Proceedings*, p. 1.

Heyman, D.P. and Sobel, M.J. (2004) *Stochastic Models in Operations Research: Stochastic Optimization*, volume 2. Courier Corporation. Q12

Ismail, Z., Leneutre, J., Bateman, D. and Chen, L. (2015) A game-theoretical model for security risk management of interdependent ICT and electrical infrastructures, in *Proceedings of the 2015 IEEE 16th International Symposium on High Assurance Systems Engineering*, IEEE Press Piscataway, NJ, pp. 101–109.

Kao, G.K., Hamlet, J., Helinski, R., Shakamuri, M., Lin, H.W. and Michalski, J.T. (2015) Supply chain security decision analytics: Macro analysis. Technical report, Sandia National Laboratories (SNL-NM), Albuquerque, NM.

Kapourchali, M.H., Sepehry, M. and Aravinthan, V. (2016) Fault detector and switch placement in cyber-enabled power distribution network. *IEEE Transactions on Smart Grid*, **9**(2), 980–992.

Khanna, K., Panigrahi, B.K. and Joshi, A. (2017) Bi-level modelling of false data injection attacks on security constrained optimal power flow. *IET Generation, Transmission & Distribution*, **11**(14), 3586–3593.

Klimburg, A. (2012) *National Cyber Security Framework Manual*. NATO Cooperative Cyber Defense Center of Excellence. Q13

Kochedykov, S., Noev, A., Dushkin, A. and Gubin, I. (2018) Method of optimum channel switching in equipment of infocommunication network in conditions of cyber attacks to their telecommunication infrastructure, in *Journal of Physics: Conference Series*, volume 1015, IOP Publishing, p. 032101. Q14

Koerner, B.I. (2016) Inside the cyberattack that shocked the US government. https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/. Q15

Kołodziej, J., Khan, S.U., Wang, L., Kisiel-Dorohinicki, M., Madani, S.A., Niewiadomska-Szynkiewicz, E., Zomaya, A.Y. and Xu, C.-Z. (2014) Security, energy, and performance-aware resource allocation mechanisms for computational grids. *Future Generation Computer Systems*, **31**, 77–92.

Kushal, T.R.B., Lai, K. and Illindala, M.S. (2018) Risk-based mitigation of load curtailment cyber attack using intelligent agents in a shipboard power system. *IEEE Transactions on Smart Grid*, **10**(5), 4741–4750.

Li, X., Zhou, C., Tian, Y.-C. and Qin, Y. (2019) A dynamic decision-making approach for intrusion response in industrial control systems. *IEEE Transactions on Industrial Informatics*. Q16

Liu, S.-Z., Li, Y.-F. and Yang, Z. (2018) Modelling of cyber-attacks and defenses in local metering system. *Energy Procedia*, **145**, 421–426.

Ma, C.Y., Yau, D.K. and Rao, N. S. (2013) Scalable solutions of Markov games for smart-grid infrastructure protection. *IEEE Transactions. Smart Grid*, **4**(1), 47–55.

Mashima, D., Rajendran, R., Zhou, T., Chen, B. and Sikdar, B. (2019) On optimization of command-delaying for advanced command authentication in smart grid systems, in *Proceedings of the 2019 IEEE Innovative Smart Grid Technologies-Asia*, IEEE Press, Piscataway, NJ, pp. 1006–1011.

Miao, F., Zhu, Q., Pajic, M. and Pappas, G.J. (2018) A hybrid stochastic game for secure control of cyber-physical systems. *Automatica*, **93**, 55–63.

Milošević, J., Tanaka, T., Sandberg, H. and Johansson, K.H. (2017) Exploiting submodularity in security measure allocation for industrial control systems, in *Proceedings of the 1st ACM Workshop on the Internet of Safe Things*, pp. 64–69. Q17

Mishra, S., Dinh, T.N., Thai, M.T., Seo, J. and Shin, I. (2016) Optimal packet scan against malicious attacks in smart grids. *Theoretical Computer Science*, **609**, 606–619.

Moore, T. (2010) The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection*, **3**(3-4), 103–117.

Mousavian, S., Erol-Kantarci, M., Wu, L. and Ortmeyer, T. (2018) A risk-based optimization model for electric vehicle infrastructure response to cyber attacks. *IEEE Transactions on Smart Grid*, **9**(6), 6160–6169.

Myerson, R.B. (2013) *Game Theory*, Harvard University Press, Cambridge, MA.

Nagurney, A., Nagurney, L.S. and Shukla, S. (2015) A supply chain game theory framework for cybersecurity investments under network vulnerability, in *Computation, Cryptography, and Network Security*, Springer, Heidelberg, Germany, pp. 381–398.

Nagurney, A. and Shukla, S. (2017) Multifirm models of cybersecurity investment competition vs. cooperation and network vulnerability. *European Journal of Operational Research*, **260**(2), 588–600.

Nandi, A.K., Medal, H.R. and Vadlamani, S. (2016) Interdicting attack graphs to protect organizations from cyber attacks: A bi-level defender–attacker model. *Computers & Operations Research*, **75**, 118–131.

National Institute of Standards and Technology (2018) Framework for improving critical infrastructure cybersecurity. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

National Science Foundation (2019) Cyber-phisical systems: Enabling a smart and connected world. https://www.nsf.gov/news/special_reports/cyber-physical/.

Oman, P., Krings, A., de Leon, D.C. and Alves-Foss, J. (2004) Analyzing the security and survivability of real-time control systems, in *Information Assurance Workshop, 2004. Proceedings*, IEEE Press, Piscataway, NJ, pp. 342–349.

Osborne, M.J. and Rubinstein, A. (1994) *A Course in Game Theory*. MIT Press, Cambridge, MA.

Pan, W., Wang, M., Fu, Y. and Shi, H. (2017) Cybersecurity decision making mechanism for defense strategies in vehicle networks, in *Information Technology and Intelligent Transportation Systems*, Springer, Heidelberg, Germany, pp. 611–621.

Panfili, M., Giuseppi, A., Fiaschetti, A., Al-Jibreen, H.B., Pietrabissa, A. and Priscoli, F.D. (2018) A game-theoretical approach to cyber-security of critical infrastructures based on multi-agent reinforcement learning, in *2018 26th Mediterranean Conference on Control and Automation*, IEEE Press, Piscataway, NJ, pp. 460–465.

Patterson, I., Nutaro, J., Allgood, G., Kuruganti, T. and Fugate, D. (2013) Optimizing investments in cyber-security for critical infrastructure, in *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop*, p. 20.

Pilz, M., Naeini, F.B., Grammont, K., Smagghe, C., Davis, M., Nebel, J.-C., Al-Fagih, L. and Pfluegel, E. (2019) Security attacks on smart grid scheduling and their defences: A game-theoretic approach. *International Journal of Information Security*, 1–17.

Priyanga, S., Gauthama Raman, M., Jagtap, S.S., Aswin, N., Kirthivasan, K. and Shankar Sriram, V. (2019) An improved rough set theory based feature selection approach for intrusion detection in SCADA systems. *Journal of Intelligent & Fuzzy Systems*, **36**(5), 3993–4003.

Puterman, M.L. (2014) *Markov Decision Processes: Discrete Stochastic Dynamic Programming*. John Wiley & Sons, Hoboken, NJ.

Puzis, R., Klippel, M.D., Elovici, Y. and Dolev, S. (2008) Optimization of NIDS placement for protection of intercommunicating critical infrastructures, in *Intelligence and Security Informatics*, Springer, Heidelberg, Germany, pp. 191–203.

Rana, M.M., Li, L. and Su, S.W. (2016) Microgrid protection and control through reliable smart grid communication systems, in *Proceedings of the 14th International Conference on Control, Automation, Robotics and Vision*, IEEE Press, Piscataway, NJ, pp. 1–6.

Rao, N.S., Poole, S.W., Ma, C.Y., He, F., Zhuang, J. and Yau, D.K. (2016) Defense of cyber infrastructures against cyber-physical attacks using game-theoretic models. *Risk Analysis*, **36**(4), 694–710.

Rass, S., Alshawish, A., Abid, M.A., Schauer, S., Zhu, Q. and de Meer, H. (2017) Physical intrusion games–optimizing surveillance by simulation and game theory. *IEEE Access*, **5**, 8394–8407.

Ravishankar, M., Rao, D.V. and Kumar, C. (2017) A game theoretic approach to modelling jamming attacks in delay tolerant networks. *Defence Science Journal*, **67**(3), 282.

Ravishankar, M., Rao, D.V. and Kumar, C. (2018) A game theoretic software test-bed for cyber security analysis of critical infrastructure. *Defence Science Journal*, **68**(1)

Reilly, J., Martin, S., Payer, M. and Bayen, A.M. (2016) Creating complex congestion patterns via multi-objective optimal freeway traffic control with application to cyber-security. *Transportation Research Part B: Methodological*, **91**, 366–382.

Rice, M. and Shenoi, S. (2017) *Critical Infrastructure Protection XI: 11th IFIP WG 11.10 International Conference*, Springer.

Salmeron, J., Wood, K. and Baldick, R. (2004) Analysis of electric grid security under terrorist threat. *IEEE Transactions on Power Systems*, **19**(2), 905–912.

Sándor, H., Genge, B., Szántó, Z., Márton, L. and Haller, P. (2019) Cyber attack detection and mitigation: Software defined survivable industrial control systems. *International Journal of Critical Infrastructure Protection*, **25**, 152–168.

Sawilla, R. and Skillicorn, D. (2012) Partial cuts in attack graphs for cost effective network defence, in *Proceedings of the, 2012 IEEE Conference on Technologies for Homeland Security*, IEEE Press, Piscataway, NJ, pp. 291–297.

Smart Grid Interoperability Panel Cyber Security Working Group *et al.* (2010*) Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security*, *NIST Special Publication*, 154 NIST, Gaithersburg, MD.

Sokri, A. (2018) Optimal resource allocation in cyber-security: A game theoretic approach. *Procedia Computer Science*, **134**, 283–288.

Stewart, C.A., Simms, S., Plale, B., Link, M., Hancock, D.Y. and Fox, G.C. (2010) What is cyberinfrastructure, in *Proceedings of the 38th Annual ACM SIGUCCS Fall Conference: Navigation and Discovery*, pp. 37–44.

Telecommunication Standardization Sector of International Telecommunication Union (2008) Itu-tx. 1205. *Interfaces*, **10**(20-x):49.

Ten, C.-W., Manimaran, G. and Liu, C.-C. (2010) Cybersecurity for critical infrastructures: Attack and defense modeling. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, **40**(4), 853–865.

The Department of Homeland Security. Critical infrastructure sectors. https://www.dhs.gov/cisa/critical-infrastructure-sectors.

The Department of Homeland Security. National preparedness goal. https://www.fema.gov/pdf/prepared/npg.pdf

The U.S. Government. Critical infrastructures protection Act of 2001. https://www.law.cornell.edu/uscode/text/42/5195c#e

The White House (2008) National Security Presidential Directive/NSPD-54. Homeland Security Presidential Directive/HSPD-23. https://fas.org/irp/offdocs/nspd/nspd-54.pdf.

The White House (2013a) Executive order: Improving critical infrastructure cybersecurity. Executive order, Office of the Press Secretary, Washington, D.C.

The White House (2013b) Presidential Policy Directive – Critical Infrastructure Security and Resilience. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

The White House (2016) Commission on enhancing national cybersecurity. Report on securing and growing the digital economy, Washington, D.C.

Turner, J.P., Qiao, J., Lawley, M., Richard, J.-P. and Abraham, D.M. (2012) Mitigating shortage and distribution costs in damaged water networks. *Socio-Economic Planning Sciences*, **46**(4), 315–326.

Vandenberghe, L. and Boyd, S. (1996) Semidefinite programming. *SIAM Review*, **38**(1), 49–95.

Vazirani, V.V. (2013) *Approximation Algorithms*, Springer Science & Business Media, Heidelberg, Germany.

Vukovic, O., Sou, K.C., Dan, G. and Sandberg, H. (2012) Network-aware mitigation of data integrity attacks on power system state estimation. *IEEE Journal on Selected Areas in Communications*, **30**(6), 1108–1118.

Wadhawan, Y. and Neuman, C. (2018) Rl-bags: A tool for smart grid risk assessment, in *Proceedings of the 2018 International Conference on Smart Grid and Clean Energy Technologies*, IEEE Press, Piscataway, NJ, pp. 7 -14.

Wang, C. and Hou, Y. (2015) Reliability-based updating strategies of cyber infrastructures, in *Proceedings of the 2015 IEEE Power & Energy Society General Meeting*, IEEE Press, Piscataway, NJ, pp. 1-5.

Wang, H., Ruan, J., Wang, G., Zhou, B., Liu, Y., Fu, X. and Peng, J. (2018) Deep learning-based interval state estimation of ac smart grids against sparse cyber attacks. *IEEE Transactions on Industrial Informatics*, **14**(11), 4766–4778.

Wang, Q., Cai, X., Tai, W. and Tang, Y. (2019) A multi-stage game model for the false data injection attack against power systems, in *2018 IEEE 8th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems*, IEEE Press Piscataway, NJ, pp.1450–1455.

Wang, Y. (2010) SSCADA: securing scada infrastructure communications. *International Journal of Communication Networks and Distributed Systems*, **6**(1), 59–78.

Weaver, G.A. and Marla, L. (2019) Cyber-physical simulation and optimal mitigation for shipping port operations, in *2018 Winter Simulation Conference*, IEEE Press, Piscataway, NJ, pp. 2747–2758.

Wei, L., Sarwat, A., Saad, W. and Biswas, S. (2018) Stochastic games for power grid protection against coordinated cyber-physical attacks. Q27 *IEEE Transactions on Smart Grid*.

Xiang, Y., Wang, L. and Liu, N. (2018) A robustness-oriented power grid operation strategy considering attacks. *IEEE Transactions on Smart Grid*, **9**(5), 4248–4261.

Young, D., Lopez Jr, J., Rice, M., Ramsey, B. and McTasney, R. (2016) A framework for incorporating insurance in critical infrastructure cyber risk strategies. *International Journal of Critical Infrastructure Protection*, **14**, 43–57.

Yuan, W., Zhao, L. and Zeng, B. (2014) Optimal power grid protection through a defender–attacker–defender model. *Reliability Engineering & System Safety*, **121**, 83–89.

Yuan, Y., Zhu, Q., Sun, F., Wang, Q. and Başar, T. (2013) Resilient control of cyber-physical systems against denial-of-service attacks., in *Proceedings of the 6th International Symposium on Resilient Control Systems*, IEEE Press, Piscataway, NJ, pp. 54–59.

Zeraati, M., Aref, Z. and Latify, M.A. (2018) Vulnerability analysis of power systems under physical deliberate attacks considering geographic-cyber interdependence of the power system and communication network. *IEEE Systems Journal*, **12**(4), 3181–3190.

Zhang, Y. W. L. S. W. *et al.* (2013) Trust system design optimization in smart grid network infrastructure. *IEEE Transactions on. Smart Grid*, **4**(1), 184–195. Q28

Zhang, Y., Sun, W. and Wang, L. (2012) Location and communication routing optimization of trust nodes in smart grid network infrastructure, in *Proceedings of the Power and Energy Society General Meeting*, IEEE Press, Piscataway, NJ, pp. 1-.

Zheng, K., Albert, L., Luedtke, J. and Towle, E. (2019) A budgeted maximum multiple coverage model for cybersecurity planning and management. *IISE Transactions*, to appear. Q29

Zheng, K. and Albert, L.A. (2019a) Interdiction models for delaying adversarial attacks against critical information technology infrastructure. *Naval Research Logistics*, **66**(5), 411–429.

Zheng, K. and Albert, L.A. (2019b) A robust approach for mitigating risks in cyber supply chains. *Risk Analysis*, **39**(9), 2076–2092.

Zhuo, Y. and Solak, S. (2014) Measuring and optimizing cybersecurity investments: A quantitative portfolio approach, in *Proceedings of the IIE Annual Conference*, p.1620. Q30