www.itcon.org - Journal of Information Technology in Construction - ISSN 1874-4753

CONSTRUCTION CYBERSECURITY AND CRITICAL INFRASTRUCTURE PROTECTION: NEW HORIZONS FOR CONSTRUCTION 4.0

SUBMITTED: November 2020
REVISED: December 2021
PUBLISHED: June 2022
EDITOR: Robert Amor
DOI: 10.36680/j.itcon.2022.028

Borja García de Soto
Division of Engineering, New York University Abu Dhabi, United Arab Emirates
garcia.de.soto@nyu.edu

Alexandru Georgescu
National Institute for Research and Development in Informatics, Romania
alexandru.georgescu@ici.ro

Bharadwaj Mantha
Division of Engineering, New York University Abu Dhabi, United Arab Emirates
bmantha@nyu.edu

Žiga Turk
Faculty of Civil and Geodetic Engineering, University of Ljubljana, Slovenia
ziga.turk@fgg.uni-lj.si

Abel Maciel
The Bartlett School of Architecture, University College London, UK
a.maciel@ucl.ac.uk

Muammer Semih Sonkor
Division of Engineering, New York University Abu Dhabi, United Arab Emirates
semih.sonkor@nyu.edu

SUMMARY: *One of the key concepts of Construction 4.0 is cyber-physical systems. The construction industry is increasingly creating valuable digital assets, but it is also gradually using digital technology to plan, design, build, monitor, and control the physical ones. This makes construction sites and operations vulnerable to cyber-attacks. While the damage to digital assets can have financial implications, attacks on digitally-controlled physical assets may impact people's well-being and, in worst-case scenarios, result in casualties. The problem is amplified by the emerging cyber-physical nature of the systems, where the human checks may be left out. The construction industry could draw inspiration from the work done in critical infrastructures (CI). Construction is the prelude of any socio-technical asset tagged as a CI. While most assets may not be critical in the CI sense, they are essential to a business' operations and the people directly or indirectly associated with them. This study presents a literature review on the previous CI protection (CIP) efforts and construction cybersecurity studies to show their synergy. Recommendations based on well-established CIP processes to make construction more cyber-secure are provided. It is expected that this study will create awareness about cybersecurity practices within the construction industry. Ongoing work includes understanding where construction stands and developing a framework to address cybersecurity throughout the different project phases.*

KEYWORDS: *Construction 4.0, Digitalization, Critical Infrastructure, Cyber Security, Cyber-physical Systems, EPCIP.*

REFERENCE: *Borja García de Soto, Alexandru Georgescu, Bharadwaj Mantha, Žiga Turk, Abel Maciel, Muammer Semih Sonkor (2022). Construction cybersecurity and critical infrastructure protection: new horizons for Construction 4.0. Journal of Information Technology in Construction (ITcon), Vol. 27, pg. 571-594, DOI: 10.36680/j.itcon.2022.028*

1. INTRODUCTION AND MOTIVATION

Construction is increasingly digital. Designs and plans are created using digital tools and stored in digital repositories such as Common Data Environments (CDEs) and exchanged over the Internet. The products of the information-intensive phases of construction are increasingly valuable. They contain intellectual property (IP) that, in some cases, is more valuable outside of the project context in which they were created. They also contain information that can be reused, not to mention commercial and trade secrets. With this trend, construction is catching up with the other industries that have already recognized the value of their digital assets.

Recently, digitalization has been moving beyond the information processes. Construction 4.0 is an umbrella concept for the current efforts to digitalize construction, and its key concept is cyber-physical systems (CPSs) (Klinc and Turk, 2019). Essentially, these are systems where material assets are monitored and controlled using digital technology with little or no human intervention (Alguliyev et al., 2018). For example, ground motion in an earthquake area is monitored, and the structural systems and counterweights in the building respond to the ground acceleration. In water treatment plants, water quality is monitored, and automatically chlorine disinfectant is added to the system. In some construction sites, a robotic excavator does its job with no humans present (Bock and Linner, 2016). While such systems were limited in the past, they are becoming ubiquitous (e.g., (Kanan et al., 2018)), are connected to the Internet (e.g., (Tang et al., 2019)), and are autonomous (e.g., (Mantha et al., 2020)). As such, they are much more vulnerable to cyber-attacks. While cyber-attacks on purely digital assets can lead to damage in the digital world and have an economic impact, they may also lead to physical property damage and even loss of human life (Boyes, 2015) due to the predominantly material nature of construction and its essential role in vital infrastructure.

1.1 Significance and relevance of the construction sector

The construction industry is an essential driver of a country's economy and accounts for a considerable amount of its GDP (World Economic Forum, 2016). According to the Global Construction 2030 report, the volume of construction output will grow to $19.2 trillion worldwide by 2035 (compared to $12 trillion in 2019) (de Best, 2021), with China, India, and the US accounting for a significant part of that growth, and will account for about 14.7% of the global GDP (GCP, 2015).

Although these projections will be affected by the impacts caused by the SARS-CoV-2 pandemic, the contributions of the Architecture, Engineering, Construction, and Operations (AECO) industry to a country's economy will continue to be essential and hover at about 10% of the GDP for developed nations. However, it should be pointed out that most of the remaining 90% of the GDP is either created in buildings or using other built environment assets. Any disruption of those assets would likely have an economic impact that would be orders of magnitude greater than the value of the assets.

Although it is expected that new technologies will have a profound change in the industry, the implications and potential benefits of Construction 4.0 are still difficult to assess. Moreover, its repercussions on the different stakeholders, critical components of the supply chain, and the different phases of the lifecycle of construction projects are not yet fully understood. Of particular concern is the general lack of awareness and understanding of cybersecurity implications when switching to a connected and digital environment. To address that, this paper lays out key cybersecurity elements to enable the full potential of Construction 4.0 and defines research areas needed to pave the roadmap for the future of the construction industry and the successful development of a secured and trusted Construction 4.0. This study also advances a proposal for integrating Construction 4.0 concerns in the Critical Infrastructure Protection framework as one potential avenue for addressing the identified security gaps.

1.2 Why is construction different?

In some aspects, the challenges construction companies are encountering are not significantly different from those faced by other industries that have already adopted new technologies and are at a more advanced level of digitalization. However, some cyber risks are specific to the construction industry due to the peculiarities of the different phases of construction projects. Electronic tendering is becoming the standard during the bidding process, as digital procurement platforms save time and money. However, highly confidential or proprietary information such as project specifications, pricing, profit and loss data, employee information, and banking records could be exposed (Boyes, 2015). During the planning and design phases, an attack on the Building Information Model

(BIM) could compromise essential project information, including personal data. It could also prevent access to the model or corrupt project information, leading to issues in subsequent phases (e.g., construction, O&M). During the construction phase, smart and automated sites are replacing the conventional ones with the help of new technology (Melenbrink et al., 2020). They might include sensors equipped on the construction equipment or materials, a network of cameras to monitor construction progress in real-time, wearable technology to minimize safety hazards, or robotic systems (connected to sensors to capture information that is fed to a control system) to assist workers or conduct construction activities autonomously (Bock and Linner, 2016). Hijacked heavy autonomous construction equipment could endanger lives (Andersson et al., 2019; Sonkor and García de Soto, 2021a, Sonkor et al., 2022), the project, and the surrounding area, while also having tertiary impacts on markets and wider critical infrastructure systems (e.g., damage or delays to the project can impact energy security or other sectors, depending on the nature of the project). During the O&M phase, new technology allows the possibility to move from rigid building management systems (BMSs) to more flexible ones using sensors that interconnect different elements through the Internet of Things (IoT) (Jia et al., 2019). BMSs are particularly vulnerable and can compromise the performance of the building or infrastructure being managed and the safety of humans inside the building.

The previously mentioned risks are particularly unique to construction compared to the other industries, such as healthcare, electronics, and aerospace, for several reasons. The dynamic and continuously changing construction site environments that require active human-machine collaboration increases the criticality of safety and cybersecurity (Sonkor and García de Soto, 2021c). The construction workforce includes people from different socio-economic classes, education levels, cultural backgrounds, and geographic locations, which leads to variability in cybersecurity knowledge, awareness, and understanding. Interoperability issues arise due to the complex nature of the projects where different multidisciplinary teams collaborate across various platforms. Due to the interdependencies and involvement of multiple sub-contracted parties, information exchange, which in many cases includes confidential and sensitive data, occurs even outside the company's network (e.g., using personal computers), which increases the cyber threat surface (Shemov et al., 2020). Moreover, 95% of construction supply chains are small and medium-sized enterprises (SMEs) (Adzroe and Ingirige, 2017) with limited resources devoted to IT. While most general contractors and large subcontractors have cyber-security policies, many smaller subcontractors that participate in projects do not (García de Soto, 2019); nevertheless, they may have access to the information assets of other partners. Last but not least, organizational fluidity caused by the changing landscape of entities assembled for one particular project constitutes a challenge for providing robust cybersecurity. Complex projects result in assemblies of different entities, each with their own level of cybersecurity preparedness, subject to different jurisdictions, and with different norms and practices. Therefore, each project has the potential to create a unique consortium, faced with ever-renewing challenges of coordination on cybersecurity and homogenization on security practices and standards.

Due to the risks and challenges outlined above, construction companies are significantly vulnerable to cyberattacks (Doss and Saul Ewing Arnstein & Lehr LLP, 2019; Mantha et al., 2020, 2021; Mantha and García de Soto, 2019; Pärn and Edwards, 2019; Pärn and García de Soto, 2020; Richey and Sawyer, 2015) and should be proactive in implementing strategies and educating employees to secure data. However, the reality is that awareness and investment in high-level security in the industry are still very low, making this industry susceptible and particularly attractive to hackers (Ghadiminia et al., 2021; Mohamed Shibly and García de Soto, 2020). Therefore, an essential element for the successful transition into the digitalization of the industry is the consideration of cybersecurity.

Some blockchain solutions have been described and proposed to address construction-specific challenges (Sonkor and García de Soto, 2021b; Ye et al., 2018), whereby a building activity is 'blockchained' at the source, complementing BIM journaling mechanisms. These new methods aim to mitigate the cyber-physical disconnect of accountability in the decision-making processes at the preconstruction, construction, and operation phases, adding resilience to the traceability of actors and digital assets in BIM processes. Lamb (2018) surveyed some of these implications, and more recently, working prototypes of blockchain-based Smart Contracts for BIM have been developed and demonstrated to show how contractual RFIs (Request for Information) can be linked directly to BIM object geometry as BIM models are developed (Maciel, 2019a, 2019b, 2020).

1.3 Critical Infrastructure Protection (CIP)

At the basis of the functioning of any society lies a foundation of interdependent and complex systems composed of both technical and organizational components called infrastructures, which operate together as part of a system of systems. These infrastructures are composed of roads, railways, pipelines, power plants, markets, public administration, laboratories, and research facilities. Some of these infrastructures are so important to the functioning of a society that they may be termed critical in that their disruption or destruction would cause significant casualties, loss of life, material losses, and loss of trust and prestige.

In the United States (US), critical infrastructures (CIs) are *"those physical and cyber-based systems essential to the minimum operations of the economy and government"* (PDD-63, 1998) and comprise infrastructures, critical assets, and key resources (Department of Homeland Security, 2003). The European Union (EU) defines CI as an *"asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions"* (Council Directive, 2008). CIs are characterized by (inter)dependencies of various types (geographic, physical, technical, informational, social, and political) (Gheorghe and Schlapfer, 2006) and by their tendency to generate complex systems with emergent and ambiguous behaviors that generate potentially dangerous phenomena such as cascading disruptions and unanticipated threats (Bouchon, 2006). The United Nations Security Council (United Nations Security Council, 2017) highlighted this – *"as a result of increasing interdependency among critical infrastructure sectors, some critical infrastructure is potentially susceptible to a growing number and a wider variety of threats and vulnerabilities that raise new security concerns"*.

US President Bill Clinton issued the Presidential Decision Directive 63 (PDD-63) in 1998 to set up a national CIP program that targets to eliminate any potential vulnerabilities to cyber and physical attacks against CIs (PDD-63, 1998). The program got more attention after the September 11 attacks in 2001, which triggered the US and European awareness of the risks of escalating disruptions in interconnected CI systems. CIP offers a comprehensive framework for understanding interdependencies in complex systems and allocating scarce security resources to prevent disruptive events, mitigate their effects, and resume normal functioning as quickly as possible, thereby ensuring resilience in society (Georgescu et al., 2019). The United Nations acknowledges that CIP is a "relatively new acquisition to the global public policy discourse" and that *"a number of countries have chosen to adopt broad and integrated strategies that take into account the need to enhance CI resilience against all hazards, whether man-made or natural"* (The United Nations, 2018).

Given the continuing improvement of CIP processes, this study advances the importance of national and collective action to mitigate the evolving security situation caused by the Construction 4.0 paradigm. Like the Industry 4.0 paradigm, Construction 4.0 is transforming this vital sector through digitalization, automation, and other cyber-mediated processes in all aspects, from design to construction and operation and maintenance (O&M) (García de Soto et al., 2019; Klinc and Turk, 2019; Mantha et al., 2021). The national CIP frameworks, and formalized collective ones, such as the European Programme for Critical Infrastructure Protection (EPCIP), are useful tools for addressing the impact of systemic changes in the construction sector caused by the shift towards digitalization and automation. This position was forged during the 1st Workshop on Cybersecurity Implications of Construction 4.0 that took place in February 2020 at New York University Abu Dhabi (NYUAD). To that end, the possible inclusion of Construction 4.0 considerations in the current CIP practices is described with minimum friction. In addition, suggestions are provided regarding possible future courses of action to ameliorate the increasingly vulnerable cyber-security environment across all the life cycle phases of a construction project, including design, construction, O&M, and end of life.

The rest of this paper is structured as follows. Section 2 presents the details of the research methodology followed in this study. Section 3 provides an overview of the reviewed literature on the past CIP and construction cybersecurity efforts. Section 4 shows the overlap between CIP and the construction sector. Section 5 summarizes how the authors define the classic CIP model. Section 6 proposes a model for CIP that considers construction sites as CIs. Section 7 discusses the findings from this research and provides a future outlook. Finally, the conclusions of the paper are summarized in Section 8.

2. RESEARCH METHODOLOGY

This section explains the methodology employed in the following sections of this paper. The research methodology is divided into three main sections: (1) *Literature review process*, (2) *The classic CIP model*, and (3) *Proposing a CIP model that includes construction sites*. The first two sections are the predecessors of the third section, and they target justifying the need for the proposed model. The first section (i.e., the literature review process) goes over each step of the literature review prior to having the final set of publications to review and the relevant considerations in each step. The second section (i.e., the classic CIP model) presents a generic summary of the current practices of CIP regulations and processes and their limitations. The last section (i.e., proposing a CIP model that includes construction sites) briefly introduces the proposed CIP model, which is explained in detail in Section 6. The overview of the methodology is demonstrated step by step in a process flow diagram in FIG. 1 to provide a reproducible approach. The step numbers do not necessarily indicate an order (e.g., Steps 1-6 and Steps 7-8 are parallel sets of activities); their intrinsic purpose is to help refer to each step clearly in the following subsections.

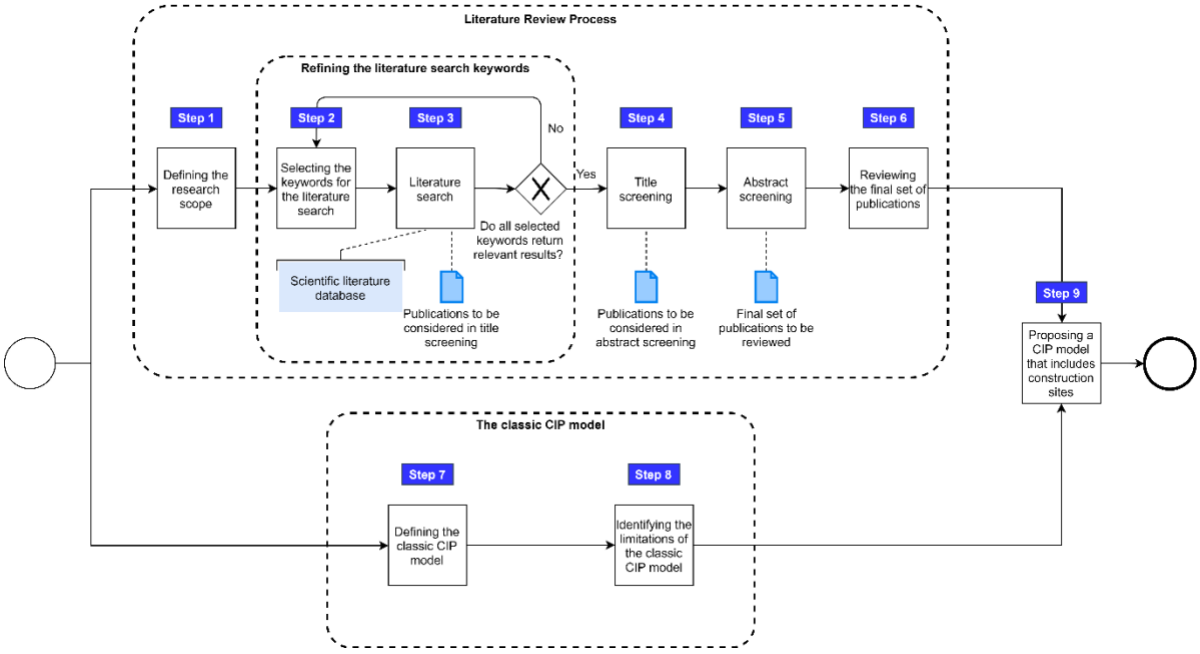

FIG. 1: Process flow diagram of the research methodology

2.1 Literature Review Process

Merriam and Simpson (2000, p. 10) define literature review as "to develop a conceptual framework or to explore a topical area for study". In this study, the authors aim for the latter by conducting an exploratory type of review. Exploratory reviews provide a broad overview of the topic rather than a detailed one that covers all available relevant literature (Frederiksen and Phelps, 2018). Since the purpose of the literature review section in this paper was to outline the previous efforts on the two main topics of the study (i.e., *CIP* and *construction cybersecurity)* and show the synergy between them, an exploratory review was a suitable option. The prominent publications from each topic were selected following the steps presented below, and their highlights and common aspects were provided in the Overview of the Reviewed Literature section.

2.1.1 Step 1: Defining the research scope

One of the initial and critical steps of the literature review process is defining the scope of the review (Randolph, 2009). It helps narrow down the possible results of the literature search to a more focused area and thus prevents dealing with a vast amount of information available. This step is necessary to distinguish the relevant from the irrelevant and efficiently manage the time and effort spent on the review (Chen et al., 2018). Determining the period to focus on is also required while conducting the search to ensure the reviewed studies are not obsolete. It is particularly crucial for technology-related topics.

The research scope of this study is twofold: reviewing the previous efforts on (1) CIP and (2) construction cybersecurity. The necessity of connecting these two topics and how to make this connection are discussed in Section 6; however, before presenting such a discussion, an overview of both and background knowledge are required. For this reason, the Overview of the Reviewed Literature section provides an overview of these topics. Moreover, the literature search was limited to a five-year publication period, which starts in 2016 and ends in September 2021.

2.1.2 Step 2: Selecting the keywords for the literature search

Steps 2 and 3 are iterative processes that refine the literature search keywords. In Step 2, a set of keywords have been determined and used for the literature search in Step 3. According to the results returned from the search in each iteration, the keyword combinations to be used were edited, and this iteration was repeated until reaching a list of keywords that only returned relevant results. TABLE 1 shows the final set of keyword combinations used in the literature search and the ones considered but decided not to be included. Boolean operators such as OR and AND were used to combine keywords in searches. From the third column to the fifth column (from the left-hand side), the first set of keywords is given, and they are connected with the OR operator. The sixth and seventh columns consist of the second set of keywords, which are also connected with the OR operator. The first and second sets of keywords are connected with the AND operator, which is why AND is shown in the upper row. For example, Search 1 indicates the following: ("Building information model*" OR "Built environment" OR "Construction industry") AND (Cybersecurity OR "Cyber security").

TABLE 1 is divided into two sections to show all considered keyword combinations to be used in the literature search on the two main topics of the study. In the upper section, three included and three not included keyword combinations related to *construction and cybersecurity* are shown. Search 1 and 2 combine two sets of keyword combinations: keywords related to (1) construction (i.e., *building information model*, built environment, construction industry*) and (2) cybersecurity (i.e., *cybersecurity, cyber security, information security*). For the keyword combination, *building information model*, an asterisk (*) was used as a wildcard to cover other possible alternatives such as *building information modelling* and *building information modeling*, as Beatty (2016) suggested. Search 3 combines the previously mentioned construction-related keywords with the blockchain-related keywords (i.e., *blockchain* and *distributed ledger*) since the primary benefits of utilizing blockchain technology (e.g., immutability and transparency) are related to cybersecurity. The remaining three keyword combinations in the *construction and cybersecurity* section were not included in the literature search since they did not return any significant results to be considered in the review.

In the lower section of TABLE 1, keyword combinations related to *CIP* are shown. Only Search 4, which combines the keyword *critical infrastructure protection* with *cybersecurity* (or *cyber security*), was included in the literature search. Even though the focus of the CIP-related articles is mostly cybersecurity, the keyword *cybersecurity* (or *cyber security*) was still included to exclude irrelevant results and focus only on cybersecurity aspects. The remaining keyword combinations were not included as they did not return useful results for the study.

2.1.3 Step 3: Literature search

As mentioned in the previous subsection and demonstrated in FIG. 1, Step 3 is a part of an iterative process that aims to refine the search keywords. In every iteration, the keyword combinations determined in Step 2 were used for the literature search in Step 3. Scopus database was used for the literature search since it covers more than 82 million documents, over 234 thousand books, and over 7,000 publishers (Elsevier, 2021). The *Article title, Abstract, Keywords* option was selected while searching documents on Scopus. The publication date range was limited from 2016 to the search date (i.e., September 2021), as explained in Step 1. Only the publications written in English were considered. Scopus defines *secondary documents* as documents that are not indexed in their database but included in the references sections of indexed documents. They were also considered as a part of the literature search results. The total number of publications returned from the searches presented in TABLE 1 was 366, as shown in TABLE 2.

2.1.4 Step 4: Title screening

Title screening is the first step of the overall screening process that narrows down the publications from the literature search. In this step, only the titles of each document were reviewed to eliminate any irrelevant publications. Initially, duplications between different searches were removed. Next, the publications with titles

that do not directly relate to the search categories were eliminated. For example, in the Search 3 (i.e., construction and blockchain) results, there were a significant number of articles considering the financial contributions of blockchain utilization, such as security of payment and automated payment. Such articles were removed during the title screening step as they did not fit the purpose of this research. Search 4 in the *CIP* category returned many publications focusing on cybersecurity training. These publications were also removed in this step as they are not directly relevant to the scope of this article. This step eliminated 122 publications and left 244 publications for the next step, as shown in TABLE 2.

TABLE 1: Final set of keyword combinations for the literature search

Category	**Search No.**	**Search Keyword**			**AND**	
			OR	**OR**		**OR**
Construction and Cybersecurity	Search 1	"Building information model*"	"Built environment"	"Construction industry"	Cybersecurity	"Cyber security"
	Search 2	"Building information model*"	"Built environment"	"Construction industry"	"Information security"	
	Search 3	"Building information model*"	"Built environment"	"Construction industry"	Blockchain	"Distributed ledger"
	Not Included	"Building information model*"	"Built environment"	"Construction industry"	"Threat model*"	
	Not Included	AECO			Cybersecurity	"Cyber security"
	Not Included	"Building construction"			Cybersecurity	"Cyber security"
CIP	Search 4	"Critical infrastructure protection"			Cybersecurity	"Cyber security"
	Not Included	"Critical infrastructure protection"			Construction	Execution
	Not Included	"Critical infrastructure protection"			"Planning phase"	"Planning stage"
	Not Included	"Critical infrastructure protection"			"Design phase"	"Design stage"
	Not Included	"Critical infrastructure protection"			"Operation and Maintenance"	"O&M"

2.1.5 Step 5: Abstract screening

After reducing the number of publications to a more manageable number in the title screening step, the next step was to further screen them by reading their abstracts. This step employed a more rigorous review than the previous step and targeted to obtain the final list of publications to be reviewed in detail. For Search 1 and 2, since the number of publications was relatively small, the screening was conducted only based on relevance without considering any other aspect. Abstracts of each publication were read to determine relevance, and the publications that did not fit the scope of this research were removed from consideration. As Search 3 and 4 initially returned larger numbers of publications than the other searches (as shown in TABLE 2), additional considerations were employed while screening them. When there are too many sources to be reviewed, Knopf (2006) suggests focusing on particular authors and studies that are frequently cited and considered to be the leading authorities and focusing on the most recent studies. The latter was already considered during Step 1 (i.e., defining the research scope) by limiting the publication date to the last five years. Following the former suggestion, the publications were sorted by their citation counts before starting the abstract screening. Among the publications with a common research focus, those with higher citation counts were selected and screened for relevance. For example, Search 3 returned multiple publications that specifically focus on the potential of blockchain in the construction sector. Among them, Turk and Klinc (2017) had the highest citation count and was selected due to its influence on this subject. For Search 4 results, a similar approach to Search 3 was used not to miss the prominent research while screening the publications. In addition, the studies focusing on the protection of specific types of critical infrastructures (e.g., water treatment plants, electric power grid) were eliminated in this step since reviewing the publications that

discuss the general aspects of CIP was more helpful for this study's purpose. After the abstract screening, 49 publications remained for the detailed literature review, as shown in TABLE 2. A list of these publications can be seen in TABLE 3 in Appendix A.

TABLE 2: Number of publications before and after the screening steps

Category	Search No.	No. of Publications After the Literature Search	No. of Publications After the Title Screening	No. of Publications After the Abstract Screening
Construction and Cybersecurity	Search 1	28	15	28
	Search 2	11	9	
	Search 3	198	131	
CIP	Search 4	129	89	21
Total No. of Publications:		**366**	**244**	**49**

2.1.6 Step 6: Reviewing the final set of publications

After the title and abstract screening, the final set of publications shown in TABLE 3 in Appendix A remained to be reviewed in detail in Step 6. In this step, the 49 publications were scrutinized to find common aspects and differences among them. While reviewing, the main aspects of each publication were listed to summarize the studies and group them using these aspects. Grouping the studies helped organize the overview presented in Section 3. This step is crucial to show the connection between the two main topics of the study (i.e., *CIP* and *construction cybersecurity*) and support the proposal made in Step 9.

2.2 The classic CIP model

This set of activities is the predecessor of Step 9, which proposes a novel CIP model that includes construction sites. Steps 7 and 8 were included in this part of the process flow (as shown in FIG. 1), and they were performed in parallel to the previously explained literature review process. The details of these steps are explained below.

2.2.1 Step 7: Defining the classic CIP model

This step presents a generic overview of the current common practices of identifying a system as critical and setting regulations for the identified CI. The set of common practices is demonstrated with the classic CIP, which is based on the authors' experiences. The classic CIP model is explained in three levels: strategy level, decision-making level, and operational level. The actors involved (e.g., CI owner, authorities) and their roles are briefly provided at each level.

2.2.2 Step 8: Identifying the limitations of the classic CIP model

In this step, the limitations of the current common practices of CIP were listed to support the need for a novel approach. The potential adversaries that might occur by not including the earlier stages (e.g., design, planning, construction) of CI within the CIP efforts were provided. The limitations presented in this step justify the reasons for integrating construction in the classic CIP model.

2.3 Step 9: Proposing a CIP model that includes construction sites

This is the final step of this research, where the authors propose the inclusion of a new aspect in the current practices of CIP. This new aspect includes all the phases of the CI life cycle before the handover and O&M, including the construction works. The roles and responsibilities of different parties in the proposed CIP model are explained and demonstrated with a process flow (See FIG. 3). Additional steps appended to the proposed model are grouped into two levels, namely the *decision making level* and *operational level.* The functions and benefits of these two additional levels are provided in this step.

3. OVERVIEW OF THE REVIEWED LITERATURE

This section presents an overview of the reviewed literature, mentioning the common aspects and research focuses of the 49 publications listed in TABLE 3 in Appendix A. This overview aims to support the proposed CIP model in Section 6.

3.1 Construction and Cybersecurity

After a long history of under-digitalization, the construction industry is making a shift towards digitalization and automation due to rapidly growing information and communication technologies (ICT) (Doss and Saul Ewing Arnstein & Lehr LLP, 2019; Jones, 2016; Mantha and García de Soto, 2019) such as 3D printing, blockchain, robotics, machine learning, drones, big data, IoT, artificial intelligence, predictive analytics, augmented reality, and real-time graphic engines, to name a few. This is referred to as Construction 4.0, which is the construction industry's surrogate of Industry 4.0. The aim thus is to have connected CPSs at every stage of a construction project's life cycle (Alsaadoun, 2019; Mantha and García de Soto, 2019), starting from the bidding phase to the end of life. If achieved, this will have the capability to transform the design, planning, construction, and O&M of the civil infrastructure systems and positively impact the overall project time, cost, and resources used (Mantha and García de Soto, 2019). For example, the adoption of digital twin technology assists in creating a digitally built environment, which can integrate the currently fragmented sector by having a digital replica through which all project participants can collaborate (Alshammari et al., 2021). This Industry 4.0 concept has been mostly driven by BIM and CDE technologies in construction. This also promotes transparency among the different phases of the lifecycle of construction projects. However, as the industry becomes more connected and digitized, the importance of cybersecurity becomes significant (Doss and Saul Ewing Arnstein & Lehr LLP, 2019; Gambill and Giszczak, 2017; Jones, 2016; Mantha et al., 2021; Mantha and García de Soto, 2019; Pärn and Edwards, 2019) and should be considered by all of the stakeholders and project participants.

The digitalization inherent in the Construction 4.0 phenomenon has led to a transformation in the security environment of the AECO sector, which has become more challenging and more dynamic (Mantha et al., 2021; Mantha and García de Soto, 2019). The challenges associated with Construction 4.0 and cybersecurity have been described throughout this article. However, in general, the AECO sector has become exposed to the security dynamics of the cyber environment, with specific risks, vulnerabilities, and threats. There is a rich literature in the broad cybersecurity field; however, it has to be noted that the AECO sector has rarely been distinguished from other domains as an object of study to highlight the specifics of cybersecurity threats in the sector. The threat environment of Construction 4.0 is complex, and the relative opacity of the sector heightens its vulnerability to external threats and fragility to internal weaknesses from a cybersecurity perspective. With this in mind, the security and threat environment of the AECO sector concerning the general cybersecurity issues and suggested solutions from the reviewed literature are presented below.

3.1.1 Occupational Phase

Different studies on construction cybersecurity focused on different phases of built environments. Several of the reviewed publications focused on the cybersecurity threats and risks of smart buildings and thus the O&M phase of construction projects. This phase has received greater attention from scholars due to the advances in smart building technologies and the increasing use of IoT for facilities management. Pärn and Edwards (2019), Gračanin et al. (2018), Stamatescu et al. (2020), Ghadiminia et al. (2021), Raveendran and Tabet Aoul (2021), and Urquhart et al. (2019) stressed the importance of robust cybersecurity in the smart built environments due to the potential physical impacts on the safety and well-being of the inhabitants, and they all mentioned the lack of attention to cybersecurity in the AECO industry. Pärn and Edwards (2019) mainly focused on CI asset management and listed the potential malicious actors, their motivations, and the different techniques used. The malicious actors mentioned in their paper are grouped as hacktivists, patriot hackers, cyber-criminals, malware authors, cyber-terrorists, cyber-militias, and script kiddies based on their motivations. As a potential solution and risk mitigation measure, blockchain technology was proposed due to the secure approach that it provides for data storage and exchange. Grundy (2017) went over the cybersecurity vulnerabilities of CPSs utilized in the BMSs and discussed several possible solutions, such as blockchain and cybersecurity frameworks. Gračanin et al. (2018) pointed out the need for a real-time monitoring system to track potential risks and warn the inhabitants when needed. They proposed a biologically inspired smart built environment modeling approach that jointly employs the robotics' three laws and swarm intelligence. Stamatescu et al. (2020) and Ghadiminia et al. (2021) provided an overview of cybersecurity challenges faced during the O&M phase of built environments and underlined the criticality of the human factor. Raveendran and Tabet Aoul (2021) investigated the risks and threats of smart buildings and cities from a broader perspective and reviewed the relevant literature. They identified five main risk themes that include *the consternation from cyber-security threats*. Last but not least, Urquhart et al. (2019) scrutinized the challenges of adaptive architecture from several different lenses, including the physical and information security risks and the

management of personal data. They emphasized the importance of designing buildings that are resilient to cyber-attacks and breaches.

3.1.2 Pre-occupational Phases

Among the reviewed literature, some publications focused on the cybersecurity aspects of the pre-occupational phases (e.g., design, construction, commissioning) of construction projects. Mantha et al. (2021) mentioned that the data collected by commissioning agents during the commissioning phase could be tampered with at the sensor (i.e., by compromising the sensor) or at the display (by compromising the dashboard) or when the sensor data is in transit. A malicious owner, or a rogue contractor, could do this to obtain the certification faster and without fixing the violations. Alternatively, an employee in either entity could do this to damage their reputation. To address this issue and detect faulty or rogue sensors or deter a rogue insider, Mantha et al. (2021) suggested a randomized sensor check-pointing approach as a countermeasure. For this, they developed an autonomous multi-sensor fusing mobile robotic data collectors to use during the onsite data collection and verification process. Mohamed Shibly and García de Soto (2020) and Mantha and García de Soto (2019) focused on the elevated cybersecurity risks due to the increasingly connected and digital nature of construction sites. Mohamed Shibly and García de Soto (2020) proposed a threat modeling approach based on QuantitativeTMM for the construction phase. To demonstrate the implementation steps and practicality of the proposed model, a 3D concrete printer was considered. Mantha and García de Soto (2019) developed a generic cybersecurity risk identification framework and conducted scenario analysis using design-bid-build and integrated project delivery construction networks. Zheng et al. (2019a) underlined the paucity of studies on potential information security issues related to BIM. They proposed a context-aware access control model for BIM systems that utilize cloud servers to store and exchange data. They targeted to provide enhanced confidentiality and a reduced risk of data leakage. Finally, Cuinas (2020) suggested adding new layers in the building information model to include the electromagnetic behavior of the construction elements to demonstrate the isolation level of the building with regards to wireless communication and estimate the protection of the building against cyber-attacks.

3.1.3 Blockchain and Distributed Ledger Technologies in Construction

After the successful financial implementations of blockchain, such as cryptocurrencies, industry and academia started investigating various use cases in different fields. Construction is one of these fields, and Turk and Klinc (2017) are among the first to identify the value of blockchain in relation to the different phases of construction projects and, in particular, to address some of the confidentiality issues raised by BIM CDEs. Further analysis of distributed ledger technologies (DLT)—the umbrella term for peer-to-peer value transaction systems that comprises blockchain as well— and blockchain applications in the sector has been published by numerous reports in the industry and articles by academic scholars, reinforcing this trend.

Blockchain technology has the potential to provide a hacker-safe ecosystem for the transfer of digital assets (Turk and Klinc, 2017). Li et al. (2019) conducted a systematic literature review to identify the state-of-the-art of DLT applications in the construction industry. Moreover, they proposed a socio-technical framework for the DLT implementation in the industry. This framework includes two conceptual models, namely *DLT Four-Dimensional Model* and *DLT Actors Model*, which are explained in detail in their paper. Yang et al. (2020) analyzed and compared the feasibility of two different types of blockchain systems— public and private. They evaluated the pros and cons of each system in two case studies. Zheng et al. (2019b) proposed a new system named bcBIM, which integrates BIM and blockchain to enhance cybersecurity aspects such as integrity, traceability, and authenticity. Hunhevicz and Hall (2020) developed a framework that helps match different DLT design options with the specific requirements of different scenarios in the construction industry. In Nawari and Ravindran's (2019) paper, the potential of blockchain in providing quick recoveries for post-disaster areas was studied. They proposed a framework that jointly uses BIM and blockchain to accelerate the permit processes in post-disaster situations. Xue and Lu (2020) emphasized the information redundancy problem of previous blockchain implementations in the construction industry and proposed an approach to minimize this redundancy in the BIM-blockchain integration.

Blockchain can also be used to share sensitive digital information of an asset in a CDE environment, limiting unauthorized redistribution of data and, therefore, making collaborative workflows more secure. The asset data (e.g., a BIM object) can be validated by or converted into a block representing a digital transaction, and there can be stakeholder interaction within a federated project in the CDE environment as they receive a track record of the

individual transaction created by the nodes sharing the block (Pärn and Edwards, 2019). Erri Pradeep et al. (2021) focused on the potential cybersecurity improvements in data exchange systems in construction networks that blockchain can provide. These aspects include but are not limited to data privacy, data integrity, and data longevity. Another research to provide secure information exchange in construction was conducted by Lee et al. (2021). In their study, the integrated use of digital twin and blockchain was proposed for traceable data communication and demonstrated in a case study using a prefabricated brick.

More recently, blockchain applications such as smart contracts are thought to be the key technology for improving collaboration and management of construction teams and enhancing traceability during projects, reducing cash flow issues often experienced by all tiers of contractors and suppliers (Maciel, 2020). For example, the study by Ciotta et al. (2021) proposes the use of smart contracts and blockchain in construction projects where the information exchange takes place in various CDEs. They aim to increase the transparency and reliability of the decisions made during the projects and reduce human error in data transmittals. They presented their idea on a prototype and compared it with the traditional approach. Another use case of blockchain, quality information management, was studied by Sheng et al. (2020). They developed a framework that utilizes blockchain and smart contracts to provide secure quality information management and reduce the possibility of disputes between stakeholders by involving them in the consensus mechanism. To verify the feasibility of the proposal, a prototype named Construction Quality Integration System was built.

3.2 Critical Infrastructure Protection (CIP)

Cybersecurity threats constitute a significant challenge for critical national infrastructures, similar to all other environments where interconnected devices and systems are becoming the norm (Ani et al., 2019; Bobowska et al., 2018; Carr, 2016; Karabacak et al., 2016b, 2016a; Tatar et al., 2016; Watanabe, 2019). The potential adverse effects of these threats are exacerbated considering the criticality of CIs to keep any society functioning (García de Soto et al., 2020; Harašta, 2018; Tatar et al., 2019; Watanabe, 2019). Therefore, providing robust cybersecurity for CIs is a vital part of the national security agendas of most countries (Karabacak et al., 2016a; Tatar et al., 2016). The initial acts of CIP by the US government and the following actions taken by the European Union were briefly mentioned in Section 1. This section provides an overview of the prominent academic research analyzed as a part of the literature review.

Regulation is one of the most common tools for governments to manage cyber-risks against CIs (Slayton and Clark-Ginsberg, 2018). Therefore, several studies among the reviewed publications focused on the regulatory aspects of CIP. Slayton and Clark-Ginsberg (2018) mentioned the concerns about *regulatory capture* where the regulations are to the advantage of particular private organizations instead of the public welfare. They analyzed the source of expertise and the inclusion of experts from various disciplines while making governmental decisions related to CIP. Karabacak et al. (2016b) analyzed different regulatory approaches for the CIs in Turkey to identify the most suitable ones. Nweke and Wolthusen (2020) discussed the effect of privacy and data protection laws and regulations in motivating or deterring companies from sharing cyber threat information, which is suggested as an effective tool for enhancing a country's overall cybersecurity level. Clark-Ginsberg and Slayton (2019) investigated the interaction between the CIP regulations and CIs themselves. They concluded that cybersecurity regulations do not necessarily reduce all forms of cyber-risks and worsen them in some cases. Butrimas (2020) stressed the necessity of taking international actions (e.g., European Council's Convention on Cybercrime) instead of the national ones to be better protected from state-resourced attackers (i.e., state actors). Wilner's (2017) work focused on the practicality of linking deterrence theory to cybersecurity regulations and CIP and identified its potential limitations. White et al. (2016) analyzed the current cybersecurity practices applied by critical sectors such as Electricity, Water, and Aviation to find the emerging threats against them.

Public-private partnership (PPP) is seen as a key factor in mitigating the threats against CIs (Carr, 2016; Watanabe, 2019). Carr (2016) investigated how governments and private entities see their roles in improving the national cybersecurity level and discovered that there is a disjunction between what each side expects from the other. Watanabe (2019) emphasized the importance of having a strong PPP in keeping CIs secure. They presented the lessons learned and challenges from Japan's ten-year PPP for CIP, which can serve as a good example for other countries. Warren and Leitch (2018) presented the strengths and weaknesses of the Australian National Cybersecurity Strategy, developed in 2016. Weiss and Biermann (2021) claimed that governments' choices of assigning responsibilities to private entities should depend on the characteristics of challenges and nationwide

institutional settings. Aoyama et al. (2017) and Kim et al. (2019) focused on the role of cybersecurity exercises in enhancing various organizations' preparedness for cyber threats. While Aoyama et al. (2017) examined different types of exercises to suggest the most suitable options for different preparedness levels, Kim et al. (2019) developed a cybersecurity exercise platform that simulates real industrial control systems (ICS) conditions. Bucovetchi et al. (2019) developed a Netlogo model that utilizes agent-based modeling to emphasize the dependency of the critical air transport infrastructure on critical space infrastructures. One of the scenarios tested included the propagation of disruptions caused by cyber-attacks on satellite systems. Finally, Toliupa et al. (2019) proposed a quantitative assessment that measures the level of protection for CIs.

4. OVERLAP BETWEEN CIP AND CONSTRUCTION

A CI is a system that may also consist of a built asset, in addition to the specific equipment, human resources, organization or digital command, control, and coordination systems (such as for administrative purposes) that enable it to perform its critical functions, such as the production of critical goods or services. Most CI, as identified in the taxonomy of CIP-practicing states, will contain the built environment. Critical Infrastructure Protection also concerns itself with the lifecycle aspects of the systems and the underlying critical assets, whether built, manufactured, or coded (Gheorghe et al., 2018). In practice, however, due to the identification and designation model discussed in Section 6, the existing CIP frameworks focus on the O&M phase and, in certain instances, on the decommissioning phase as well (e.g., nuclear power plants, offshore oil rigs) where hazards may occur as a result of the process.

For the most part, we find that CIP does not dedicate sufficient attention to the earlier phases and only in particular situations where existing regulations warrant it (e.g., nuclear facilities). In the recent past, there has been an increased focus on resilience by design as a principle of CI (Gheorghe et al., 2018), where the future infrastructure needs to be designed and built with the idea of a) minimizing vulnerabilities; b) mitigating damage from the materialization of an adverse event; c) ensuring graceful decline in infrastructure operation; d) ensuring reduced couplings between CI components and subsystems or between the particular CI and others, thereby slowing down the propagation of dysfunctions in chained critical infrastructures; e) having failsafes, redundancies, flexibility and adaptability in operation; f) promoting the rapid resumption of normal levels of activity or an acceptable percentage of normal functioning; g) preventing the "fortuitous alignment of breaking points", which leads to cascading disruptions in a CI system-of-systems and the enhancement of the scope, duration and severity of a crisis event, among others (Pescaroli and Alexander, 2016).

Nonetheless, most of the CIP efforts still do not consider all the different life cycle phases of a construction project as a whole, just the O&M phase, which involves operation, retrofitting, and decommissioning. One exception is the heavily regulated sector of nuclear power plants, where there is already a focus on the security consequences of all the phases of the plant's life cycle – from site selection to design, construction, O&M, upgrading, and decommissioning to the sourcing of fuel and the disposal of waste (Mureșan et al., 2018). This study argues that the changes in the security environment generated by the Construction 4.0 paradigm warrant a similar approach to the protection of other types of infrastructure in general and, most importantly, the CI across all the phases of its life cycle.

5. DEFINING THE CLASSIC CIP MODEL

This section defines what the authors consider *the classic CIP model* based on their experience. FIG. 2 shows a generic overview of the classic CIP model. It consists of three levels, namely, strategy level, decision-making level, and operational level. The overarching objective is to identify a system as critical and formulate security plans and other related compliance measures. This model, and its three levels, refers to the organization and regulation of the protection of the critical infrastructure, not to the organization and regulation of the activity of the critical infrastructure, usually consisting of the production of critical goods and services. While the two may overlap, it is no less true that CIP activities may take place also when the CI in question is partly or totally nonoperational due to maintenance, upgrades, or a pre-occurring disruption event.

5.1 Strategic level

At this level, a national CIP authority (usually under the Ministry of Interior or, in the US, the Department of Homeland Security) receives input from several organizations such as the Executive (e.g., dedicated organizations

under the President or Prime Minister), the legislature (e.g., regulations), partner countries, and supranational authorities. With the help of this input, CIP activities are coordinated, information is exchanged, and incidents are reported.

5.2 Decision-making level

This level deals with a competent authority designated for a particular sector (e.g., finance, agriculture, energy, communications, etc.) to lead a process to identify and designate new CI in accordance with the set methodologies. At the end of this process, it will be decided if an asset will be designated a CI or not and which will be the competent regulatory authority.

5.3 Operational level

Finally, the owner or operator of the CI (which can also be a tandem of owner entity and facility management entity) is responsible for its functioning and, after having its asset or system designated as a CI, must comply with various regulations (national, international, supranational transposed in national legislation like in the EU). Usually, regulations include obligations such as performing regular security and risk assessments, reporting incidents to their competent authority, formulating and updating an Operator Security Plan, or investing in resolving security issues.

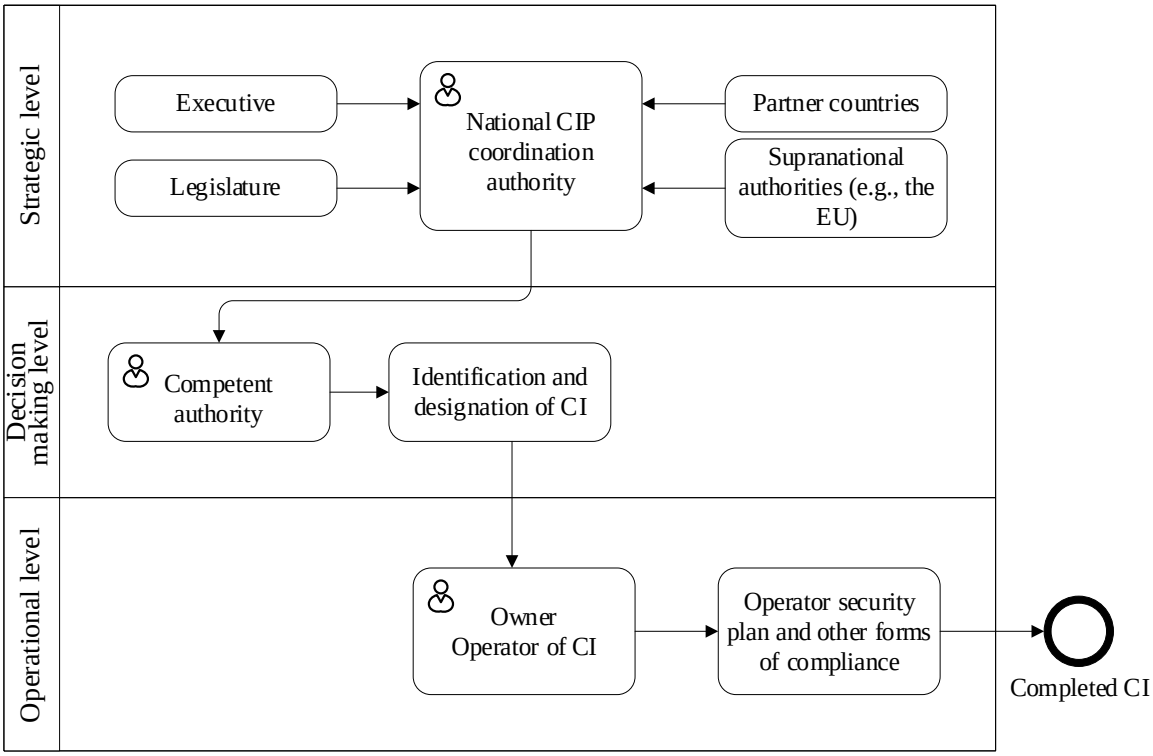

FIG. 2: A simplified version of the classic CIP model

5.4 Limitations of the classic CIP model

As discussed in the section above, the current approach (i.e., the classic CIP model) is to have national authorities (or European authorities in concert with national ones for European Critical Infrastructures impacting two or more Member States as part of EPCIP) identify and designate national CIs following a series of quantitative and qualitative criteria. However, the same infrastructure is usually not designated or recognized as critical (or incipiently critical) during earlier stages, such as design, planning, and construction, for the purposes of ensuring an added level of protection. We have presented some of the few exceptions to this state of fact. This is a critical security gap because of a) normal construction-related accidents, which are random disruptions due to complexity and unintended system interactions and behaviors; b) systemic weaknesses due to errors of design and building

philosophies; and c) deliberate threats such as those posed by state actors and their proxies engaged in hybrid warfare which may affect an operational infrastructure due to the inconsistencies which took place during the planning, design, and construction stage, or they may target future infrastructures to corrupt or disrupt them from the design and construction phases. That is before it has ever had the opportunity to become critical to the security of one or more states and before the said asset has been integrated into a wider CI system-of-systems. For example, in a recent incident, hackers gained access to the Target (a well-known retailer in the US) network and stole personal and financial information of the customers due to the vulnerability of a heating ventilation and air conditioning (HVAC) vendor that worked on the project (Shu et al., 2017).

Negative occurrences may result not only in vitiated functioning of the asset or system but also delays in the completion of the project or wider disruptions in its area based on geographic, physical, and other interdependencies between the construction site and its surroundings. This is especially true when it comes to infrastructure being built in cities, which are an agglomeration of CIs and where all of the types of disruptions take place (Rinaldi et al., 2001), such as a) common cause disruptions, where multiple CI malfunction because of the same cause; b) escalating disruptions, where disruptions build on each other to reach unanticipated levels of harm; and c) cascading disruptions, where disruptions reverberate throughout a system through the dependency links between different CI.

This gap has always been present, but the cyber vulnerabilities of the Construction 4.0 paradigm make it imperative to address this issue by integrating it into an existing framework of security governance. Prior to the introduction of CIP, security governance already featured legislative and administrative frameworks for physical asset security, the protection of persons and privileged information, and foresight measures diminishing the impact of disruptions such as interruptions in fuel and raw materials supply. CIP simply systematized these and offered a holistic view of the resulting CI system-of-systems that enabled a better measurement of risk, the anticipation of threat scenarios, and the formation of a toolbox to perform security governance processes, first from an all-hazards-approach and, afterward, from a resilience perspective. Therefore, the authors believe that existing CIP efforts can accommodate the processes required to address systemic risks, vulnerabilities, and threats in the new security environment underlined by the emergence of Construction 4.0. Recent developments, such as Complex System Governance, offer new tools for understanding and conceptualizing complex systems and their interactions, which result in pathologies that may affect system viability. (Keating and Katina, 2016). The following section describes the proposed integration of construction in the traditional CI model to address these gaps.

6. CONSIDERATION OF THE CONSTRUCTION PHASE IN THE TRADITIONAL CIP MODEL

The authors propose to introduce a new element in the CIP framework – the construction phase of a potential CI – involving not just the actual site but also the design, bidding, regulatory approval, construction processes, and other related elements about the entities involved before the handing over of the infrastructure. This enables security decision-makers to respond to the future state of the CI system-of-systems, rather than just the current one. Treating the construction site as if it was a CI is useful. The construction site respects certain aspects of the CI definition. Having it disrupted or destroyed can generate significant human or material losses. It does not produce critical goods or services. However, the completed asset will meet the thresholds of criticality envisioned by the existing regulations based on the business plan or technical proposal, which led to the construction project.

FIG. 3 outlines the proposed process. In certain countries, such as the European ones, there is usually a Ministry dedicated to Construction and Infrastructure projects, which would be an additional authority to keep in the process, aside from the sectoral authority related to the corresponding potential infrastructure being built. It is important to note that this study discusses the protection activities for critical infrastructure, not the regulation of the fundamental activity of the critical infrastructure, even though there may be overlaps for operational security. Therefore, this section discusses the high-level organization of CIP activities for construction projects, which may be labeled critical either through their eventual result or through the impact which their disruption or destruction would have on the broader security environment.

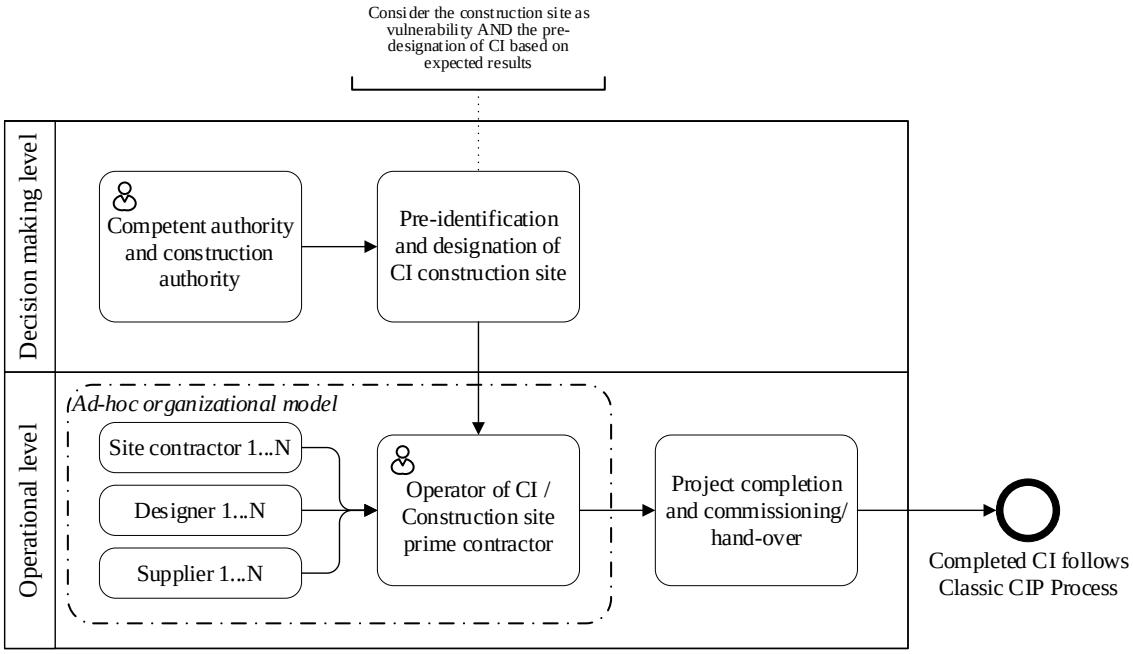

FIG. 3: A model for CIP integrating the construction site as CI

Contrasting with FIG. 2 and the classic CIP model, the strategic level of the updated model remains the same. The following two steps register changes due to the specificities of the construction sector:

6.1 Decision-making level

A future candidate for CI status will be pre-designated as a CI even from the proposal stage, regardless of whether it will become a CI once complete. This designation needs to be made by applying the existing criteria for CI designation to the anticipated future functioning of the asset being built, as detailed in the business plan, the investment projections, and other relevant documentation. Therefore, a future port facility with a planned capacity will be pre-designated as a CI based on the systemic relevance of its planned capacity in the current methodology for CI designation. This pre-designation results in the designation of the project, from the design phase to the finalization of the construction work and delivery to the beneficiary, as a critical construction infrastructure.

6.2 Operational level

The lead integrating organization (or prime contractor) for the construction site becomes the equivalent of the CI owner (or operator) and must file an operator's security plan following existing rules. They may also have to abide by specialized rules that involve a more frequent updating of the security plan due to the steadily transforming nature of the construction site as it heads towards completion.

Following the completion of construction, commissioning, and handing over to the beneficiary who will own it and operate it (possibly through a third-party facility manager), the site loses its critical construction site status, and the national regulating authority must go through the normal identification and designation process for a CI, presented in Section 5. The construction sector will remain involved through its facilities' management branch or through the issues of maintenance, upgrade, and decommissioning of critical infrastructure sites. However, these phases are already included in the CIP framework.

7. DISCUSSION AND FUTURE OUTLOOK

Aside from the evolving nature of the CI construction site, another difference compared to the classic CIs stems from the challenges of the organizational make-up. The prime contractor takes on the role of CI operator for the duration of the existence of the project until it is completed. However, the prime contractor coordinates an ad-hoc assembly of many specialized companies and subcontractors formed for this particular project. This is still a valid and relevant approach, as complex system theory allows us to delineate a system of any given complexity so long

as there is a system boundary that differentiates the complex system from the surrounding environment (not just in a physical sense) (Keating and Bradley, 2015). The challenge and the justification for the extra governance capacity of the CIP framework lie in the disparate security standards (especially in cyber) of all of the contractors working on- and off-site. It will require new instruments and methodologies to adequately assess the cyber vulnerabilities of such an assembly and mitigate them to ensure site security. This is in contrast to classical CI, where there is an operator (who is sometimes the owner) who is the sole and permanent CI protection agent who liaises with the competent authority, at least until the CI or critical asset, most of which are owned and operated by private entities, passes into other hands. The nature of the consortia executing important constructing projects (e.g., civil, industrial, energy) with the capacity of becoming CIs presents specific challenges.

The construction site as CI adaptation may require other specific instruments, such as compliance with mandatory cybersecurity standards for all contractors or becoming subject to a security audit. Future research into the subject may have to also deal with the impact that added security regulations from the CIP system will have on overall cost and complexity and establish policies for providing cost-effective regulations.

The security liaison officer (SLO) system, where the CI, the regulatory authority, the highest national level CIP authority, and (in the European Union) the European authority all have officers responsible for the exchange of relevant information, may have to be adjusted for the construction site CI. Rather than being a high-ranking member of the Security Department as close as possible in the hierarchy to the executive suite of the owner (or operator), the SLO for construction site CI may be directly under the particular Project Director since companies may be involved in multiple projects, some or each of them being a different pre-designated CI.

This study addresses an important gap in the security of CI in the context of the necessity to invest in the inventory of next-generation CI, not just in the maintenance and upgrade of the current ones. At the same time, the construction site as CI proposal causes minimum disruption to existing ways of doing things and is compatible with existing national frameworks and even supranational ones, such as European initiatives like the European Reference Network for Critical Infrastructure Protection (ERNCIP) and Critical Infrastructure Warning Information Network (CIWIN). It can also be compatible with future projects, such as an expanded EPCIP or a European CIP Agency. Recent developments regarding EPCIP include the proposed Critical Entities Resilience (CER) Directive (European Commission, 2020a). Following the experience of the pandemic in highlighting European interdependencies in previously unregulated European CI sectors, this directive proposes, in addition to the pre-existing energy and transport, an additional eight sectors (i.e., banking, financial market, health, drinking water, waste water, digital infrastructure, public administration, space) for Critical European Infrastructure identification, designation, and governance. In the current ongoing effort to update EU CIP legislation, which also saw a proposal for a NIS2 Directive (European Commission, 2020b) aligned with the CER Directive in terms of CI taxonomy, it may also be possible to consider additional developments, such as the concept of critical construction infrastructures proposed in this paper.

7.1 Transborder CIP

The Construction 4.0 paradigm is also useful from the perspective of the emerging transborder CI chains. This is a growing issue since globalization has resulted in globalized integrated supply and production chains built on the back of globalized transport, data, and finance infrastructure (Georgescu et al., 2019). The fragmented nature of national CIP governance processes creates gaps in surveillance, detection, and action against crisis and emergency situations (natural or man-made), resulting in globally distributed CI networks being only as strong as their weakest link. More and more, various states are implementing regional and global CI creation and management initiatives as a tool for economic growth and geopolitical influence, such as the Belt and Road Initiative, the recently announced EU Global Gateway project, and many more. This will require collective governance mechanisms for various issues. In the past, several issues have been identified, such as environmental impact, financial sustainability, or the avoidance of corruption and labor issues, but CIP will have to be on the agenda of these initiatives as well.

The most well-developed supranational CIP initiative is that of the EU. Beginning in 2004, the EU has pursued CIP as a framework for managing the risks of complex and interdependent socio-technical systems. With the release of Directive 114/2008 (Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European CIs and the assessment of the need to improve their protection), the EPCIP assumed an important role in managing the systemic energy, cyber, transport and space vulnerabilities of an “ever-closer

Union." With specific projects, such as the integrated European electricity and gas network, or the development of European transport corridors, the EU is generating a new security environment in which risks, vulnerabilities, and threats gain transborder valences and become increasingly hard to understand, manage and mitigate by jurisdictionally limited national authorities. EPCIP is becoming not only more in-depth but also more comprehensive, designating European Critical Infrastructures (ECI) in health, finance, and other areas hitherto managed exclusively at national levels.

The Member States of the EU have an obligation to transpose its Directives into national law and at least meet, if not exceed, the minimum levels of CIP security and best practices recommended by the EU. In practice, this has not led to full convergence of organizational systems, legislation, division of authority, or even taxonomies of CIs, as well as definitions. CIP has become, however, a principal concern of all EU Member States. This involves the identification and designation of the CI, the regulation of the functioning of its security apparatus, clear lines of communication with the authorities, and, where necessary, with European authorities and other Member States and exchanges of information. The constant and consistent development of EPCIP parallels that of national systems, where a growing taxonomy of CI is taken into account as the vulnerabilities from a wide variety of interconnected systems become apparent, both in the day to day functioning, as well as a direct or indirect result of systemic shocks (Bouchon et al., 2006) such as the SARS-CoV-2 Pandemic.

Mureșan and Georgescu (2019) discussed CIP in the context of China's Belt and Road Initiative, which they argued was a developing system-of-systems composed of existing physical infrastructures, new ones (ports, highways, railways, pipelines), and organizational CIs (financial institutions) with important sectorial offshoots in digital technology (the Digital Silk Road) and, more recently, in health (the Health Silk Road). The Belt and Road Initiative, should it come to fruition, will result in globally distributed CI chains whose main risks will have to be managed collectively in order to present cascading transborder disruptions, and this cooperation will be necessary on a technical and policy level regardless of the political situation and tensions between infrastructure hosting countries. The Belt and Road Initiative is also characterized by high levels of construction activity for infrastructures that contribute to the strategic objective of enhancing trade and other exchanges.

All regional integration initiatives advancing beyond a certain point will experience this emergence of CI networks that the countries involved will have to manage collectively – the EU's Global Gateway, the Eurasian Economic Union, the International North-South Transport Corridor (INSTC) between India, Iran, and Russia, the Ashgabat Agreement for facilitating transport between Central Asia and the Persian Gulf, the Three Seas Initiative for creating North-South infrastructure links in Eastern Europe, which is supported by the US, and many more. All of these involve the creation and maintenance of transborder infrastructure networks with significant construction and design efforts, which will result in critical dependencies on distributed systems. This will result in the need to address growing security concerns arising both from a challenging security environment (terrorism, political instability, sectarian strife, inter and intra-state conflict, hybrid and asymmetric warfare), as well as from the operation of complex, interconnected infrastructure systems predicated on higher efficiency through tighter couplings between systems.

The Blue Dot Network proposed by the US as a response to China's Belt and Road Initiative specifically addresses the issue of governance concerning infrastructure creation, especially transborder infrastructure – it provides certification for infrastructure projects which *"exemplify quality infrastructure principles as set out in the G20 Principles for Quality Infrastructure Investment, the G7 Charlevoix Commitment on Innovative Financing for Development and the Equator Principles. The Blue Dot Network aims to promote quality infrastructure investment that is open and inclusive, transparent, economically viable, financially, environmentally and socially sustainable, and compliant with international standards, laws, and regulations"* (United States Department of State, 2020). From here, the addition of CIP as a component of quality infrastructure investment is just another step toward greater awareness of the added value it brings, and adding the Construction 4.0 perspective enhances the positive effect of CIP efforts and responds to the changing security environment.

At the same time, the emergence of Construction 4.0 will result in greater attention paid to the AECO industry and its projects within the framework for systemic governance of cyber issues, including as it relates to international cooperation, which involves standard-setting, international agreements on regulation, accords on cyber aggression and its discouragement and moving onto the transborder regulation of critical cyber infrastructure protection (Georgescu et al., 2020).

8. CONCLUSION

Construction 4.0 creates opportunities for added value in terms of efficiency, safety, growth, and comfort but also fosters new risks, vulnerabilities, and threats related to the increasingly autonomous cyber-physical systems. In some form, the concerns raised by the Construction 4.0 paradigm can be addressed through Critical Infrastructure Protection (CIP), starting from the already existing overlap between CIP and facility management (i.e., one of the life cycle phases of a construction project). This paper provides a few suggestions for further integration in a way that emphasizes compatibility with the existing CIP philosophy and current practice. The inclusion of Construction 4.0 in CIP offers an opportunity to enhance the existing framework by considering and better managing the realities of complex interdependent systems and the systemic changes in the security environment. The vision is compatible with the expansion or reform of national frameworks for CIP, whether in the US, European states, or elsewhere where there have been additions in recent years, such as critical financial infrastructures, national monuments, and cultural legacy as cultural infrastructures. At the same time, it can be of use to transborder CIP efforts, especially the most institutionalized ones, such as the European Programme for Critical Infrastructure Protection (EPCIP).

ACKNOWLEDGMENTS

This paper was conceived during the 1st Workshop on Cybersecurity Implications of Construction 4.0 (CIC4-2020) that took place at New York University Abu Dhabi (NYUAD) in February 2020. The workshop was organized by the S.M.A.R.T. Construction Research Group and funded by the NYUAD Institute. The authors thank the Center for Cyber Security at New York University Abu Dhabi (CCS-NYUAD) for the support provided for this study.

REFERENCES

Adzroe, E., and Ingirige, B. (2017). Innovation in e-business: Issues related to adoption for micro and SME organisations. In S. Perera, B. Ingirige, K. Ruikar, and E. Obonyo (Eds.), *Advances in Construction ICT and e-Business* (1st ed., pp. 316–339). Routledge. https://doi.org/10.4324/9781315690698

Alguliyev, R., Imamverdiyev, Y., and Sukhostat, L. (2018). Cyber-physical systems and their security issues. *Computers in Industry*, *100*, 212–223. https://doi.org/10.1016/j.compind.2018.04.017

Alsaadoun, O. (2019). A cybersecurity prospective on industry 4.0: Enabler role of identity and access management. *International Petroleum Technology Conference 2019, IPTC 2019*. https://doi.org/10.2523/iptc-19072-ms

Alshammari, K., Beach, T., and Rezgui, Y. (2021). Cybersecurity for digital twins in the built environment: Current research and future directions. *Journal of Information Technology in Construction*, *26*(March), 159–173. https://doi.org/10.36680/j.itcon.2021.010

Andersson, J., Balduzzi, M., Hilt, S., Lin, P., Maggi, F., Urano, A., and Vosseler, R. (2019). *A Security Analysis of Radio Remote Controllers for Industrial Applications*. https://documents.trendmicro.com/assets/white_papers/wp-a-security-analysis-of-radio-remote-controllers.pdf

Ani, U. D., Watson, J. D. M. K., Nurse, J. R. C., Cook, A., and Maple, C. (2019). A review of critical infrastructure protection approaches: Improving security through responsiveness to the dynamic modelling landscape. *PETRAS/IET Conference Living in the Internet of Things: Cybersecurity of the IoT - 2019*. https://doi.org/10.1049/cp.2019.0131

Aoyama, T., Nakano, T., Koshijima, I., Hashimoto, Y., and Watanabe, K. (2017). On the complexity of cybersecurity exercises proportional to preparedness. *Journal of Disaster Research*, *12*(5), 1081–1090. https://doi.org/10.20965/jdr.2017.p1081

Beatty, S. (2016). *6 simple search tips: Lessons learned from the Scopus Webinar*. Scopus (Blog). https://blog.scopus.com/posts/6-simple-search-tips-lessons-learned-from-the-scopus-webinar

Bobowska, B., Chorás, M., and Woźniak, M. (2018). Advanced analysis of data streams for critical infrastructures protection and cybersecurity. *Journal of Universal Computer Science*, *24*(5), 622–633.

Bock, T., and Linner, T. (2016). *Construction Robots: Elementary Technologies and Single-Task Construction Robots* (Vol. 3). Cambridge University Press. https://doi.org/10.1017/CBO9781139872041

Bouchon, S., Gheorghe, A. V., and Birchmeier, J. (2006). Toward Guidelines for Regional Assessment of Vulnerability against Service Disruption of Critical Infrastructures. *EsReDa, the 29th Seminar "System Analysis for a More Secure World" Proceedings*, 81–95.

Bouchon, Sara. (2006). *The Vulnerability of interdependent Critical Infrastructures Systems: Epistemological and Conceptual State-of-the-Art*.

Boyes, H. (2015). Security, Privacy, and the Built Environment. *IT Professional*, *17*, 25–31. https://doi.org/10.1109/MITP.2015.49

Bucovetchi, O., Georgescu, A., Badea, D., Stanciu, R.D. (2019). Agent-based modeling (ABM)— support for emphasizing the air transport infrastructure dependence on space systems. *Sustainability*, Vol. 11(19):5331. https://doi.org/10.3390/su11195331

Butrimas, V. (2020). Ensuring the security and availability of critical infrastructure in a changing cyber-threat environment: Living dangerously. In E. Tikk and M. Kerttunen (Eds.), *Routledge Handbook of International Cybersecurity* (pp. 122–133). Routledge.

Carr, M. (2016). Public–private partnerships in national cyber-security strategies. *International Affairs*, *92*(1), 43–62. https://doi.org/10.1111/1468-2346.12504

Chen, Q., García de Soto, B., and Adey, B. T. (2018). Construction automation: Research areas, industry concerns and suggestions for advancement. *Automation in Construction*, *94*, 22–38. https://doi.org/10.1016/j.autcon.2018.05.028

Ciotta, V., Mariniello, G., Asprone, D., Botta, A., and Manfredi, G. (2021). Integration of blockchains and smart contracts into construction information flows: Proof-of-concept. *Automation in Construction*, *132*. https://doi.org/10.1016/j.autcon.2021.103925

Clark-Ginsberg, A., and Slayton, R. (2019). Regulating risks within complex sociotechnical systems: Evidence from critical infrastructure cybersecurity standards. *Science and Public Policy*, *46*(3), 339–346. https://doi.org/10.1093/scipol/scy061

Council Directive. (2008). Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. *Official Journal of the European Union*.

Cuinas, I. (2020). An introduction to cybersecurity at physical layer: Obstacles at radio channel to mitigate hackers' chance. *Elektronika Ir Elektrotechnika*, *26*(6), 58–65. https://doi.org/10.5755/j01.eie.26.6.28006

de Best, R. (2021). Global construction industry spending 2014-2019, with forecasts up until 2035. Statista.com study, 22 July 2021, https://www.statista.com/statistics/788128/construction-spending-worldwide/ Accessed: December 15, 2021

Department of Homeland Security. (2003). *National Strategy for The Physical Protection of Critical Infrastructures and Key Assets, as DHS (2003)*. https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf

Doss, A., and Saul Ewing Arnstein & Lehr LLP. (2019). *Cybersecurity in the Construction Industry: Protecting Against a Growing Threat*. Jdsupra. https://www.jdsupra.com/legalnews/cybersecurity-in-the-construction-22150/

Elsevier. (2021). *Content*. Elsevier. https://www.elsevier.com/solutions/scopus/how-scopus-works/content

European Commission. (2020a). Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the resilience of critical entities. COM/2020/829 final, December 16 2020, Brussels. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:829:FIN. Accessed December 15, 2021.

European Commission. (2020b). Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive

(EU) 2016/1148. COM/2020/823 final, December 16, 2020, Brussels. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:823:FIN. Accessed December 15, 2021

Erri Pradeep, A. S., Yiu, T. W., Zou, Y., and Amor, R. (2021). Blockchain-aided information exchange records for design liability control and improved security. *Automation in Construction*, *126*. https://doi.org/10.1016/j.autcon.2021.103667

Frederiksen, L., and Phelps, S. F. (2018). *Literature Reviews for Education and Nursing Graduate Students* (First). Rebus Community. http://solr.bccampus.ca:8001/bcc/file/8af49997-4d25-43fe-b6fa-8ab09f3ca64f/1/Literature-Reviews-for-Education-and-Nursing-Graduate-Students.pdf

Gambill, J., and Giszczak, J. J. (2017). *Construction contractors must remain vigilant to minimize cybersecurity risks*. McDonald Hopkins (Blog). https://mcdonaldhopkins.com/Insights/November-2017/Construction-contractors-must-remain-vigilant-to-m

García de Soto, B. (2019, June 25). Building Data Security: Construction industry's long-overdue shift to digital raises threat of cyber attacks. *NYUAD*. https://nyuad.nyu.edu/en/news/latest-news/science-and-technology/2019/june/building-data-security.html

García de Soto, B., Agustí-Juan, I., Joss, S., and Hunhevicz, J. (2019). Implications of Construction 4.0 to the workforce and organizational structures. *International Journal of Construction Management*, 1–13. https://doi.org/10.1080/15623599.2019.1616414

García de Soto, B., Georgescu, A., Mantha, B. R. K., Turk, Ž., and Maciel, A. (2020). Construction Cybersecurity and Critical Infrastructure Protection: Significance, Overlaps, and Proposed Action Plan. *Preprints 2020*. https://doi.org/10.20944/preprints202005.0213.v1

GCP. (2015). *Global Construction 2030: A global forecast for the construction industry to 2030*. https://www.ciob.org/media/105/download

Georgescu, A., Vevera, V., and Cirnu, C. E. (2020). The diplomacy of systemic governance in cyberspace. *International Journal of Cyber Diplomacy*, *1*(1), 81–90.

Georgescu, Alexandru, Gheorghe, A. V., Piso, M.-I., and Katina, P. F. (2019). *Critical Space Infrastructures: Risk, Resilience and Complexity*. Springer International Publishing. https://doi.org/10.1007/978-3-030-12604-9

Ghadiminia, N., Mayouf, M., Cox, S., and Krasniewicz, J. (2021). BIM-enabled facilities management (FM): a scrutiny of risks resulting from cyber attacks. In *Journal of Facilities Management*. Emerald Group Holdings Ltd. https://doi.org/10.1108/JFM-01-2021-0001

Gheorghe, A. V., and Schlapfer, M. (2006). Ubiquity of Digitalization and Risks of Interdependent Critical Infrastructures. *2006 IEEE International Conference on Systems, Man and Cybernetics*, 580–584. https://doi.org/10.1109/ICSMC.2006.384447

Gheorghe, A. V., Vamanu, D. V., Katina, P. F., and Pulfer, R. (2018). *Critical Infrastructures, Key Resources, Key Assets: Risk, Vulnerability, Resilience, Fragility, and Perception Governance*, *Topics in Safety, Risk, Reliability and Quality*. Springer International Publishing. https://doi.org/10.1007/978-3-319-69224-1

Gračanin, D., D'Amico, A., Manuel, M., Carson, W., Eltoweissy, M., and Cheng, L. (2018). Biologically inspired safety and security for smart built environments: Position paper. *2018 IEEE Symposium on Security and Privacy Workshops (SPW)*, 293–298. https://doi.org/10.1109/SPW.2018.00047

Grundy, C. (2017). Cybersecurity in the built environment: Can your building be hacked? *Corporate Real Estate Journal*, *7*(1), 39–50.

Harašta, J. (2018). Legally critical: Defining critical infrastructure in an interconnected world. *International Journal of Critical Infrastructure Protection*, *21*, 47–56. https://doi.org/10.1016/j.ijcip.2018.05.007

Hunhevicz, J. J., and Hall, D. M. (2020). Advanced Engineering Informatics Do you need a blockchain in construction ? Use case categories and decision framework for DLT design options. *Advanced Engineering Informatics*, *45*. https://doi.org/10.1016/j.aei.2020.101094

Jia, M., Komeily, A., Wang, Y., and Srinivasan, R. S. (2019). Adopting Internet of Things for the development of

smart buildings: A review of enabling technologies and applications. *Automation in Construction*, *101*(January), 111–126. https://doi.org/10.1016/j.autcon.2019.01.023

Jones, K. (2016). *Data Breaches, Cybersecurity, and the Construction Industry*. Construct Connect (Blog). https://www.constructconnect.com/blog/data-breaches-cyber-security-construction-industry

Kanan, R., Elhassan, O., and Bensalem, R. (2018). An IoT-based autonomous system for workers' safety in construction sites with real-time alarming, monitoring, and positioning strategies. *Automation in Construction*, *88*, 73–86. https://doi.org/10.1016/j.autcon.2017.12.033

Karabacak, B., Ozkan Yildirim, S., and Baykal, N. (2016a). A vulnerability-driven cyber security maturity model for measuring national critical infrastructure protection preparedness. *International Journal of Critical Infrastructure Protection*, *15*, 47–59. https://doi.org/10.1016/j.ijcip.2016.10.001

Karabacak, B., Ozkan Yildirim, S., and Baykal, N. (2016b). Regulatory approaches for cyber security of critical infrastructures: The case of Turkey. *Computer Law and Security Review*, *32*(3), 526–539. https://doi.org/10.1016/j.clsr.2016.02.005

Keating, C. B., and Bradley, J. M. (2015). Complex system governance reference model. *International Journal of System of Systems Engineering*, *6*, 33–52.

Keating, C. B., and Katina, P. F. (2016). Complex system governance development: a first generation methodology. *International Journal of System of Systems Engineering*, *7*, 43–74.

Kim, J., Kim, K., and Jang, M. (2019). Cyber-Physical Battlefield Platform for Large-Scale Cybersecurity Exercises. *11th International Conference on Cyber Conflict: Silent Battle*, 1–19. https://doi.org/10.23919/CYCON.2019.8756901

Klinc, R., and Turk, Ž. (2019). Construction 4.0 - digital transformation of one of the oldest industries. *Economic and Business Review*, *21*(3), 393–410. https://doi.org/10.15458/ebr.92

Knopf, J. W. (2006). Doing a Literature Review. *PS: Political Science & Politics*, *39*(1), 127–132. https://doi.org/10.1017/S1049096506060264

Lamb, K. (2018). Blockchain and Smart Contracts: What the AEC sector needs to know. *CDBB_REP_003*. https://doi.org/10.17863/CAM.26272

Lee, D., Lee, S. H., Masoud, N., Krishnan, M. S., and Li, V. C. (2021). Integrated digital twin and blockchain framework to support accountable information sharing in construction projects. *Automation in Construction*, *127*. https://doi.org/10.1016/j.autcon.2021.103688

Li, J., Greenwood, D., and Kassem, M. (2019). Blockchain in the built environment and construction industry: A systematic review, conceptual models and practical use cases. *Automation in Construction*, *102*, 288–307. https://doi.org/10.1016/j.autcon.2019.02.005

Maciel, A. (2019a). *Construction Blockchain Consortium Conference 2019: Closing Remarks*. Construction Blockchain Consortium Conference 2019. https://drive.google.com/file/u/1/d/1NTNc842bLo36k6hQJaoxkDQvLhSHiFI0/view?usp=sharing&usp=embed_facebook

Maciel, A. (2019b). *Forge DevCon 2019: BIM, Blockchain & Smart Contracts*. Forge DevCon Germany. https://www.youtube.com/watch?v=Wb28HudjkyI

Maciel, A. (2020). Use of Blockchain for enabling Construction 4.0. In A. Sawhney, M. Riley, and J. Irizarry (Eds.), *Construction 4.0: An Innovation Platform for the Built Environment* (1st ed., pp. 441–459). Routledge. https://doi.org/10.1201/9780429398100-20

Mantha, B. R. K., and García de Soto, B. (2019). Cyber security challenges and vulnerability assessment in the construction industry. *In Proceedings of the Seventh Creative Construction Conference (CCC 2019), 29 June - 2 July 2019, Budapest, Hungary. DOI: https://doi.org/10.3311/CCC2019-005*

Mantha, B. R. K., García de Soto, B., and Karri, R. (2021). Cyber security threat modeling in the AEC industry: An example for the commissioning of the built environment. *Sustainable Cities and Society*, *66*, 102682.

https://doi.org/https://doi.org/10.1016/j.scs.2020.102682

Mantha, B. R. K., García de Soto, B., Menassa, C. C., and Kamat, V. R. (2020). Robots in indoor and outdoor environments. In A. Sawhney, M. Riley, and J. Irizarry (Eds.), *Construction 4.0: An Innovation Platform for the Built Environment* (1st ed., pp. 441–459). Routledge. https://doi.org/10.1201/9780429398100-16

Melenbrink, N., Werfel, J., and Menges, A. (2020). On-site autonomous construction robots: Towards unsupervised building. *Automation in Construction*, *119*, 103312. https://doi.org/10.1016/j.autcon.2020.103312

Merriam, S. B., and Simpson, E. L. (2000). *A Guide to Research for Educators and Trainers of Adults* (2nd Update). Krieger Publishing Company.

Mohamed Shibly, M. U. R., and García de Soto, B. (2020). Threat Modeling in Construction: An Example of a 3D Concrete Printing System. *ISARC 2020 - 37th International Symposium on Automation and Robotics in Construction*, 625–632. https://doi.org/10.22260/isarc2020/0087

Mureșan, L., and Georgescu, A. (2019). A Critical Infrastructure Perspective on the Belt and Road Initiative and its Opportunities and Challenges. In J. Yang and Z. Obradovic (Eds.), *The Belt and Road and Central and Eastern Europe* (pp. 205–228). Shanghai Foreign Language Education Press.

Mureșan, L., Georgescu, A., Jivănescu, I., Popa, Ș., and Arseni, Ș-C. (2018). Charting Critical Energy Infrastructure Dependencies on Space Systems – New Frontiers in Risks, Vulnerabilities and Threats. In G. Gluschke, M. H. Caşın, and M. Macori (Eds.), *Critical Energy Infrastructure Protection and Cyber Security Policies*. Institute for Security and Safety of the Brandenburg University of Applied Sciences.

Nawari, N. O., and Ravindran, S. (2019). Blockchain and Building Information Modeling (BIM): Review and applications in post-disaster recovery. *Buildings*, *9*(6), 149. https://doi.org/10.3390/BUILDINGS9060149

Nweke, L. O., and Wolthusen, S. (2020). Legal Issues Related to Cyber Threat Information Sharing among Private Entities for Critical Infrastructure Protection. *12th International Conference on Cyber Conflict (CyCon)*, 63–78. https://doi.org/10.23919/CyCon49761.2020.9131721

Pärn, E. A., and Edwards, D. (2019). Cyber threats confronting the digital built environment: Common data environment vulnerabilities and block chain deterrence. *Engineering Construction & Architectural Management*, *26*(2), 245–266. https://doi.org/10.1108/ECAM-03-2018-0101

Pärn, E. A., and García de Soto, B. (2020). Cyber threats and actors confronting the Construction 4.0. Chapter 22. In A. Sawhney, M. Riley & J. Irizarry (Eds.). Construction 4.0: An Innovation Platform for the Built Environment (pp. 441-459). 1st Edition. London: Routledge, ISBN-13: 978-0367027308. DOI: https://doi.org/10.1201/9780429398100-22

PDD-63. (1998). *The White House (1998) Presidential Decision Directive/NSC-63*. https://clinton.presidentiallibraries.us/items/show/12762

Pescaroli, G., and Alexander, D. (2016). Critical infrastructure, panarchies and the vulnerability paths of cascading disasters. *Natural Hazards*, *82*(1), 175–192. https://doi.org/10.1007/s11069-016-2186-3

Randolph, J. (2009). A Guide to Writing the Dissertation Literature Review. *Practical Assessment, Research and Evaluation*, *14*. https://doi.org/10.7275/b0az-8t74

Raveendran, R., and Tabet Aoul, K. A. (2021). A meta-integrative qualitative study on the hidden threats of smart buildings/cities and their associated impacts on humans and the environment. *Buildings*, *11*(6), 251. https://doi.org/10.3390/buildings11060251

Richey, E., and Sawyer, T. (2015). *Know Your Enemy: Construction Industry Needs Better Information About Cyber Crime Risk*. ENR (Engineering News-Record). https://www.enr.com/articles/9023-know-your-enemy-construction-industry-needs-better-information-about-cyber-crime-risk?page=1

Rinaldi, S. M., Peerenboom, J. P., and Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, *21*, 11–25. https://doi.org/10.1109/37.969131

Shemov, G., García de Soto, B., and Alkhzaimi, H. (2020). Blockchain Applied to the Construction Supply Chain: A Case Study with Threat Model. *Frontiers of Engineering Management*, *7*(4), 564–577. https://doi.org/10.1007/s42524-020-0129-x

Sheng, D., Ding, L., Zhong, B., Love, P. E. D., Luo, H., and Chen, J. (2020). Construction quality information management with blockchains. *Automation in Construction*, *120*(August), 103373. https://doi.org/10.1016/j.autcon.2020.103373

Shu, X., Tian, K., Ciambrone, A., and Yao, D. (2017). *Breaking the Target: An Analysis of Target Data Breach and Lessons Learned*. ArXiv.Org. https://arxiv.org/abs/1701.04940

Slayton, R., and Clark-Ginsberg, A. (2018). Beyond regulatory capture: Coproducing expertise for critical infrastructure protection. *Regulation and Governance*, *12*(1), 115–130. https://doi.org/10.1111/rego.12168

Sonkor, M. S., and García de Soto, B. (2021a). Is Your Construction Site Secure? A View from the Cybersecurity Perspective. *In Proceedings of the 38th International Symposium on Automation and Robotics in Construction (ISARC 2021 Online)*. Dubai, November 2-4, 2021. https://doi.org/https://doi.org/10.22260/ISARC2021/0117

Sonkor, M. S., and García de Soto, B. (2021b). Towards Secure Construction Networks: A Data-Sharing Architecture Utilizing Blockchain Technology and Decentralized Storage. *In Proceedings to the Construction Blockchain Consortium Conference 2021 (CBC2021): Blockchain & The Digital Twin*. 20 - 22 October 2021. https://doi.org/10.47330/CBC.2021.NOKH7555

Sonkor, M. S., and García de Soto, B. (2021c). Operational Technology on Construction Sites: A Review from the Cybersecurity Perspective. *Journal of Construction Engineering and Management*, *147*(12), 4021172. https://doi.org/10.1061/(ASCE)CO.1943-7862.0002193

Sonkor, M. S., Xu, X., Prieto, S.A., and García de Soto, B. (2022). Vulnerability Assessment of Construction Equipment: An Example for an Autonomous Site Monitoring System. *In Proceedings of the 39th International Symposium on Automation and Robotics in Construction* (ISARC 2022). Colombia, Bogota. July 13-16, 2022

Stamatescu, G., Stamatescu, I., Arghira, N., and Fagarasan, I. (2020). Cybersecurity Perspectives for Smart Building Automation Systems. *Proceedings of the 12th International Conference on Electronics, Computers and Artificial Intelligence, ECAI 2020*. https://doi.org/10.1109/ECAI50035.2020.9223152

Tang, S., Shelden, D. R., Eastman, C. M., Pishdad-Bozorgi, P., and Gao, X. (2019). A review of building information modeling (BIM) and the Internet of things (IoT) devices integration: Present status and future trends. *Automation in Construction*, *101*, 127–139. https://doi.org/10.1016/j.autcon.2019.01.020

Tatar, U., Karabacak, B., and Gheorghe, A. (2016). An assessment model to improve national cyber security governance. *Proceedings of the 11th International Conference on Cyber Warfare and Security, ICCWS 2016*, 312–319.

Tatar, U., Karabacak, B., Katina, P. F., and Igonor, A. (2019). A complex structure representation of the US critical infrastructure protection program based on the Zachman framework. *International Journal of System of Systems Engineering*, *9*(3), 221–234. https://doi.org/10.1504/IJSSE.2019.102869

The United Nations. (2018). *The Protection of Critical Infrastructure Against Terrorist Attacks: Compendium of Good Practices*. https://www.un.org/sc/ctc/wp-content/uploads/2018/06/Compendium-CIP-final-version-120618_new_fonts_18_june_2018_optimized.pdf

Toliupa, S., Parkhomenko, I., and Shvedova, H. (2019). Security and regulatory aspects of the critical infrastructure objects functioning and cyberpower level assesment. *3rd International Conference on Advanced Information and Communications Technologies, AICT 2019*, 463–468. https://doi.org/10.1109/AIACT.2019.8847746

Turk, Ž., and Klinc, R. (2017). Potentials of Blockchain Technology for Construction Management. *Procedia Engineering*, *196*, 638–645. https://doi.org/10.1016/j.proeng.2017.08.052

United Nations Security Council. (2017). *Resolution 2341: Threats to international peace and security caused by*

terrorist acts. Resolution 2341 (2017) Adopted by the Security Council at its 7882nd meeting, on 13 February 2017, S/RES/2341 (2017). http://unscr.com/en/resolutions/doc/2341

United States Department of State. (2020). *Blue Dot Network*. US Department of State. https://www.state.gov/blue-dot-network/

Urquhart, L., Schnädelbach, H., and Jäger, N. (2019). Adaptive Architecture: regulating human building interaction. *International Review of Law, Computers and Technology*, *33*(1), 3–33. https://doi.org/10.1080/13600869.2019.1562605

Warren, M., and Leitch, S. (2018). Australian cyber security policy through a European lens. *European Conference on Information Warfare and Security, ECCWS*, 489–495.

Watanabe, K. (2019). PPP (public-private partnership)-based cyber resilience enhancement efforts for national critical infrastructures protection in Japan. In E. Luiijf, I. Žutautaitė, and B. M. Hämmerli (Eds.), *CRITIS 2018: Critical Information Infrastructures Security* (Vol. 11260, pp. 169–178). Springer International Publishing. https://doi.org/10.1007/978-3-030-05849-4_13

Weiss, M., and Biermann, F. (2021). Cyberspace and the protection of critical national infrastructure. *Journal of Economic Policy Reform*. https://doi.org/10.1080/17487870.2021.1905530

White, R., George, R., Boult, T., and Chow, C. E. (2016). Apples to apples: RAMCAP and emerging threats to lifeline infrastructure. *Homeland Security Affairs*, *12*. https://www.hsaj.org/articles/12012

Wilner, A. (2017). Cyber deterrence and critical-infrastructure protection: Expectation, application, and limitation. *Comparative Strategy*, *36*(4), 309–318. https://doi.org/10.1080/01495933.2017.1361202

World Economic Forum. (2016). *Shaping the Future of Construction: A Breakthrough in Mindset and Technology*. http://www3.weforum.org/docs/WEF_Shaping_the_Future_of_Construction_full_report__.pdf

Xue, F., and Lu, W. (2020). A semantic differential transaction approach to minimizing information redundancy for BIM and blockchain integration. *Automation in Construction*, *118*. https://doi.org/10.1016/j.autcon.2020.103270

Yang, R., Wakefield, R., Lyu, S., Jayasuriya, S., Han, F., Yi, X., Yang, X., Amarasinghe, G., and Chen, S. (2020). Public and private blockchain in construction business process and information integration. *Automation in Construction*, *118*. https://doi.org/10.1016/j.autcon.2020.103276

Ye, Z., Yin, M., Tang, L., and Jiang, H. (2018). Cup-of-Water Theory: A Review on the Interaction of BIM, IoT and blockchain During the Whole Building Lifecycle. *Proceedings of the 35th International Symposium on Automation and Robotics in Construction (ISARC 2018)*. https://doi.org/10.22260/ISARC2018/0066

Zheng, R., Jiang, J., Hao, X., Ren, W., Xiong, F., and Zhu, T. (2019a). CaACBIM: A context-aware access control model for BIM. *Information*, *10*(2), 47. https://doi.org/10.3390/info10020047

Zheng, R., Jiang, J., Hao, X., Ren, W., Xiong, F., and Ren, Y. (2019b). bcBIM: A Blockchain-Based Big Data Model for BIM Modification Audit and Provenance in Mobile Cloud. *Mathematical Problems in Engineering*, *2019*, 5349538. https://doi.org/10.1155/2019/5349538

APPENDIX A

TABLE 3: List of publications remaining after the abstract screening

ID	Title	Authors	Year	Source	Document Type[a]	Search Category
1	Cyber threats confronting the digital built environment: Common data environment vulnerabilities and block chain deterrence	Parn E.A., Edwards D.	2019	Engineering, Construction and Architectural Management	Review	
2	Biologically inspired safety and security for smart built environments: Position paper	Gračanin D., D'Amico A., Manuel M., Carson W., Eltoweissy M., Cheng L.	2018	Proceedings - 2018 IEEE Symposium on Security and Privacy Workshops, SPW 2018	Conference Paper	
3	Cyber security threat modeling in the AEC industry: An example for the commissioning of the built environment	Mantha B., García de Soto B., Karri R.	2021	Sustainable Cities and Society	Article	
4	Threat Modeling in Construction: An Example of a 3D Concrete Printing System	Mohamed Shibly M.U.R., García de Soto B.	2020	Proceedings of the 37th International Symposium on Automation and Robotics in Construction, ISARC 2020	Conference Paper	
5	A cybersecurity prospective on industry 4.0: Enabler role of identity and access management	Alsaadoun O.	2019	International Petroleum Technology Conference 2019, IPTC 2019	Conference Paper	
6	Cybersecurity for digital twins in the built environment: Current research and future directions	Alshammari K., Beach T., Rezgui Y.	2021	Journal of Information Technology in Construction	Article	
7	Cybersecurity Perspectives for Smart Building Automation Systems	Stamatescu G., Stamatescu I., Arghira N., Fagarasan I.	2020	Proceedings of the 12th International Conference on Electronics, Computers and Artificial Intelligence, ECAI 2020	Conference Paper	Construction and Cybersecurity
8	BIM-enabled facilities management (FM): a scrutiny of risks resulting from cyber attacks	Ghadiminia N., Mayouf M., Cox S., Krasniewicz J.	2021	Journal of Facilities Management	Review	
9	A meta-integrative qualitative study on the hidden threats of smart buildings/cities and their associated impacts on humans and the environment	Raveendran R., Tabet Aoul K.A.	2021	Buildings	Review	
10	Data Breaches, Cyber Security and the Construction Industry	Jones K.	2016	Construct Connect	Article	
11	Cyber security challenges and vulnerability assessment in the construction industry	Mantha B.R., García de Soto B.	2019	Proceedings of the 2019 Creative Construction Conference, June 29 – July 2, 2019, Budapest, Hungary	Conference Paper	
12	Construction Contractors Must Remain Vigilant to Minimize Cybersecurity Risks _ Cybersecurity in the Construction Industry	Gambill J., Giszczak J.	2017	McDonald Hopkins	Article	
13	Cybersecurity in the built environment: Can your building be hacked?	Grundy C.	2017	Corporate Real Estate Journal	Article	

14	Cybersecurity in the Construction Industry: Protecting Against a Growing Threat	Doss A., Saul Ewing Arnstein & Lehr LLP	2019	JD Supra	Article	
15	Adaptive Architecture: regulating human building interaction	Urquhart L., Schnädelbach H., Jäger N.	2019	International Review of Law, Computers and Technology	Article	
16	CaACBIM: A context-aware access control model for BIM	Zheng R., Jiang J., Hao X., Ren W., Xiong F., Zhu T.	2019	Information (Switzerland)	Article	
17	An introduction to cybersecurity at physical layer: Obstacles at radio channel to mitigate hackers' chance	Cuinas I.	2020	Elektronika ir Elektrotechnika	Article	
18	Potentials of Blockchain Technology for Construction Management	Turk Ž., Klinc R.	2017	Procedia Engineering	Conference Paper	
19	Blockchain in the built environment and construction industry: A systematic review, conceptual models and practical use cases	Li J., Greenwood D., Kassem M.	2019	Automation in Construction	Article	
20	BcBIM: A Blockchain-Based Big Data Model for BIM Modification Audit and Provenance in Mobile Cloud	Zheng R., Jiang J., Hao X., Ren W., Xiong F., Ren Y.	2019	Mathematical Problems in Engineering	Article	
21	Public and private blockchain in construction business process and information integration	Yang R., Wakefield R., Lyu S., Jayasuriya S., Han F., Yi X., Yang X., Amarasinghe G., Chen S.	2020	Automation in Construction	Article	
22	Blockchain and Building Information Modeling (BIM): Review and applications in post-disaster recovery	Nawari N.O., Ravindran S.	2019	Buildings	Review	
23	Do you need a blockchain in construction? Use case categories and decision framework for DLT design options	Hunhevicz J.J., Hall D.M.	2020	Advanced Engineering Informatics	Article	
24	A semantic differential transaction approach to minimizing information redundancy for BIM and blockchain integration	Xue F., Lu W.	2020	Automation in Construction	Article	
25	Construction quality information management with blockchains	Sheng D., Ding L., Zhong B., Love P.E.D., Luo H., Chen J.	2020	Automation in Construction	Article	
26	Integrated digital twin and blockchain framework to support accountable information sharing in construction projects	Lee D., Lee S.H., Masoud N., Krishnan M.S., Li V.C.	2021	Automation in Construction	Article	
27	Blockchain-aided information exchange records for design liability control and improved security	Erri Pradeep A.S., Yiu T.W., Zou Y., Amor R.	2021	Automation in Construction	Article	
28	Integration of blockchains and smart contracts into construction information flows: Proof-of-concept	Ciotta V., Mariniello G., Asprone D., Botta A., Manfredi G.	2021	Automation in Construction	Article	
29	Public-private partnerships in national cyber-security strategies	Carr M.	2016	International Affairs	Article	CIP

30	Beyond regulatory capture: Coproducing expertise for critical infrastructure protection	Slayton R., Clark-Ginsberg A.	2018	Regulation and Governance	Article
31	A vulnerability-driven cyber security maturity model for measuring national critical infrastructure protection preparedness	Karabacak B., Yildirim S.O., Baykal N.	2016	International Journal of Critical Infrastructure Protection	Article
32	Regulatory approaches for cyber security of critical infrastructures: The case of Turkey	Karabacak B., Ozkan Yildirim S., Baykal N.	2016	Computer Law and Security Review	Article
33	Security and regulatory aspects of the critical infrastructure objects functioning and cyberpower level assesment	Toliupa S., Parkhomenko I., Shvedova H.	2019	2019 3rd International Conference on Advanced Information and Communications Technologies, AICT 2019 - Proceedings	Conference Paper
34	Legally critical: Defining critical infrastructure in an interconnected world	Harašta J.	2018	International Journal of Critical Infrastructure Protection	Article
35	On the complexity of cybersecurity exercises proportional to preparedness	Aoyama T., Nakano T., Koshijima I., Hashimoto Y., Watanabe K.	2017	Journal of Disaster Research	Review
36	An assessment model to improve national cyber security governance	Tatar U., Karabacak B., Gheorghe A.	2016	Proceedings of the 11th International Conference on Cyber Warfare and Security, ICCWS 2016	Conference Paper
37	Cyber deterrence and critical-infrastructure protection: Expectation, application, and limitation	Wilner A.	2017	Comparative Strategy	Article
38	Advanced analysis of data streams for critical infrastructures protection and cybersecurity	Bobowska B., Chorás M., Woźniak M.	2018	Journal of Universal Computer Science	Article
39	Legal Issues Related to Cyber Threat Information Sharing among Private Entities for Critical Infrastructure Protection	Nweke L.O., Wolthusen S.	2020	International Conference on Cyber Conflict, CYCON	Conference Paper
40	Regulating risks within complex sociotechnical systems: Evidence from critical infrastructure cybersecurity standards	Clark-Ginsberg A., Slayton R.	2019	Science and Public Policy	Article
41	A review of critical infrastructure protection approaches: Improving security through responsiveness to the dynamic modelling landscape	Ani U.D., Watson J.D.McK., Nurse J.R.C., Cook A., Maple C.	2019	IET Conference Publications	Conference Paper
42	A complex structure representation of the US critical infrastructure protection program based on the Zachman framework	Tatar U., Karabacak B., Katina P.F., Igonor A.	2019	International Journal of System of Systems Engineering	Article
43	Cyber-Physical Battlefield Platform for Large-Scale Cybersecurity Exercises	Kim J., Kim K., Jang M.	2019	International Conference on Cyber Conflict, CYCON	Conference Paper
44	Cyberspace and the protection of critical national infrastructure	Weiss M., Biermann F.	2021	Journal of Economic Policy Reform	Article

45	Apples to apples: RAMCAP and emerging threats to lifeline infrastructure	White R., George R., Boult T., Chow C.E.	2016	Homeland Security Affairs	Article
46	Australian cyber security policy through a European lens	Warren M., Leitch S.	2018	European Conference on Information Warfare and Security, ECCWS	Conference Paper
47	PPP (public-private partnership)-based cyber resilience enhancement efforts for national critical infrastructures protection in Japan	Watanabe K.	2019	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	Conference Paper
48	Ensuring the security and availability of critical infrastructure in a changing cyber-threat environment: Living dangerously	Butrimas V.	2020	Routledge Handbook of International Cybersecurity	Book Chapter
49	Construction Cybersecurity and Critical Infrastructure Protection: Significance, Overlaps, and Proposed Action Plan	García de Soto B., Georgescu A., Mantha B., Turk Ž., Maciel A.	2020	Preprints 2020	Preprint

[a] Document types for all publications were taken from the Scopus database, excluding the secondary documents that did not have such information on Scopus. These secondary documents are 10, 11, 12, 13, 14, and 49, and the document types were assigned manually by the authors for them.