Construction 4.0 – a New Cybersecurity Paradigm

Adrian Victor VEVERA, Carmen Elena CÎRNU, Alexandru GEORGESCU
National Institute for Research and Development in Informatics – ICI Bucharest
victor.vevera@ici.ro, carmen.cîrnu@ici.ro, alexandru.georgescu@ici.ro

Abstract: The digitalization of economic, political and social life has not been homogeneous. Certain domains have digitalized faster than others. This has led to early exposure to the worsening cybersecurity environment and an early awakening of awareness regarding the need for research and investment into cybersecurity as an ongoing concern. The corollary is that there are fields which feature a delayed onset of digitalization, and they are becoming more exposed to a complex and dynamic security environment without having absorbed important lessons or introduced measures to increase resilience. One such field is the AECO industry (architecture, engineering, construction and operation), which is a crucial economic domain, and which is rapidly digitalizing. The article explains the Construction 4.0 concept and highlights the need for research and investment into the cybersecurity gaps stemming from the specific characteristics of the field.
Keywords: Cybersecurity, Cyber research, Construction 4.0, Construction Industry, Critical Infrastructures

INTRODUCTION

Cybersecurity considerations are at the forefront of efforts to improve security outcomes for private, civil and state actors. We are facing a complex and challenging security environment, in which rapid digitalization and networking of all economic, social and political domains not only provides benefits, but also generates new risks, vulnerabilities and threats.

The spectrum of deliberate threats is also expanding – from cybercriminals to state-backed actors and the states themselves, engaging in hybrid, unconventional and asymmetric warfare in which cyber-attacks are emerging as a preferred means to strike an adversary with good cost-benefit ratio and with deniability.

The purpose of this article is to highlight the digitalization of the construction industry. We refer to it, in accordance with the industry practice and the specialty literature, as the AECO industry (architecture, engineering, construction, operation/maintenance); sometimes, decommissioning facilities is also included. We will discuss the cyber

threats facing this industry and lean on the specialty literature to argue that cybersecurity is lacking and needs to be addressed in the context of Construction 4.0, the ubiquitous digitalization and automation of the AECO industry, which parallels and is a component of the more well-known Industry 4.0 paradigm.

CONSTRUCTION 4.0

AECO is a hugely important segment of the global economy, contributing an estimated 12 trillion dollars to global spending in 2019 (with an incalculable GDP impact) and moving towards 19.2 trillion dollars by 2035 (Figure 1). The industry provides for a vast supply and production chain, providing employment at all socio-economic and educational levels. At its core, human civilization is sustained by the built environment which facilitates all aspects of our lives. Therefore, AECO may represent 10% of GDP in advanced economies, according to de Best (2021), but the other 90% is almost entirely created or mediated by the built environment.

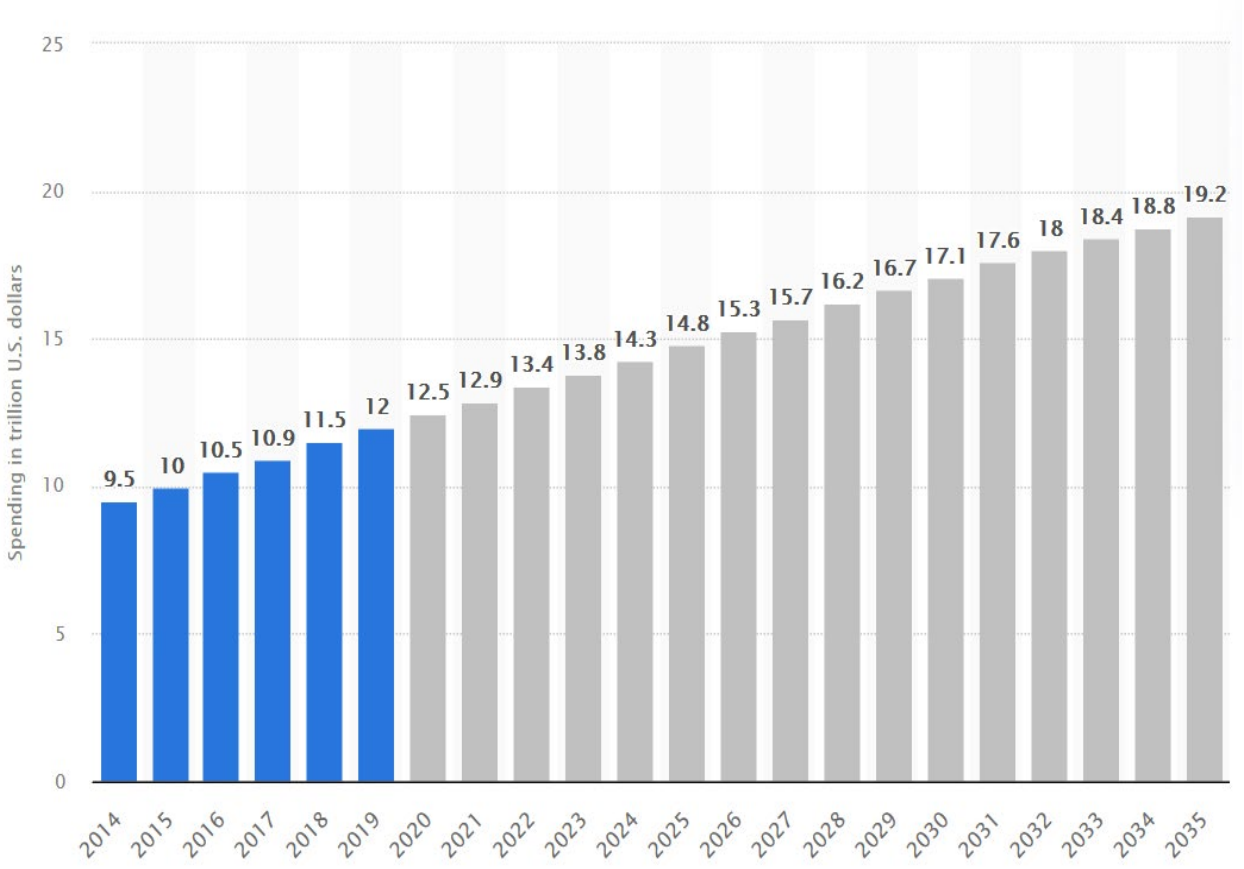

Fig. 1: *Global construction spending estimates until 2035 in trillions of dollars (source: de Best, 2021)*

The AECO industry was, by comparison to others, under-digitalized and saw the late introduction of digital technologies, which was also unequally distributed within its component activities and, of course, across geographical space. Coburn et al. (2019) analyzed the degree of digitalization across multiple economic sectors, such as pharmaceutics, finance and so on. The AECO industry is not present, but the constructions component was evaluated and found to be one of the least digitalized, surpassed only by agriculture and hunting (Figure 2).

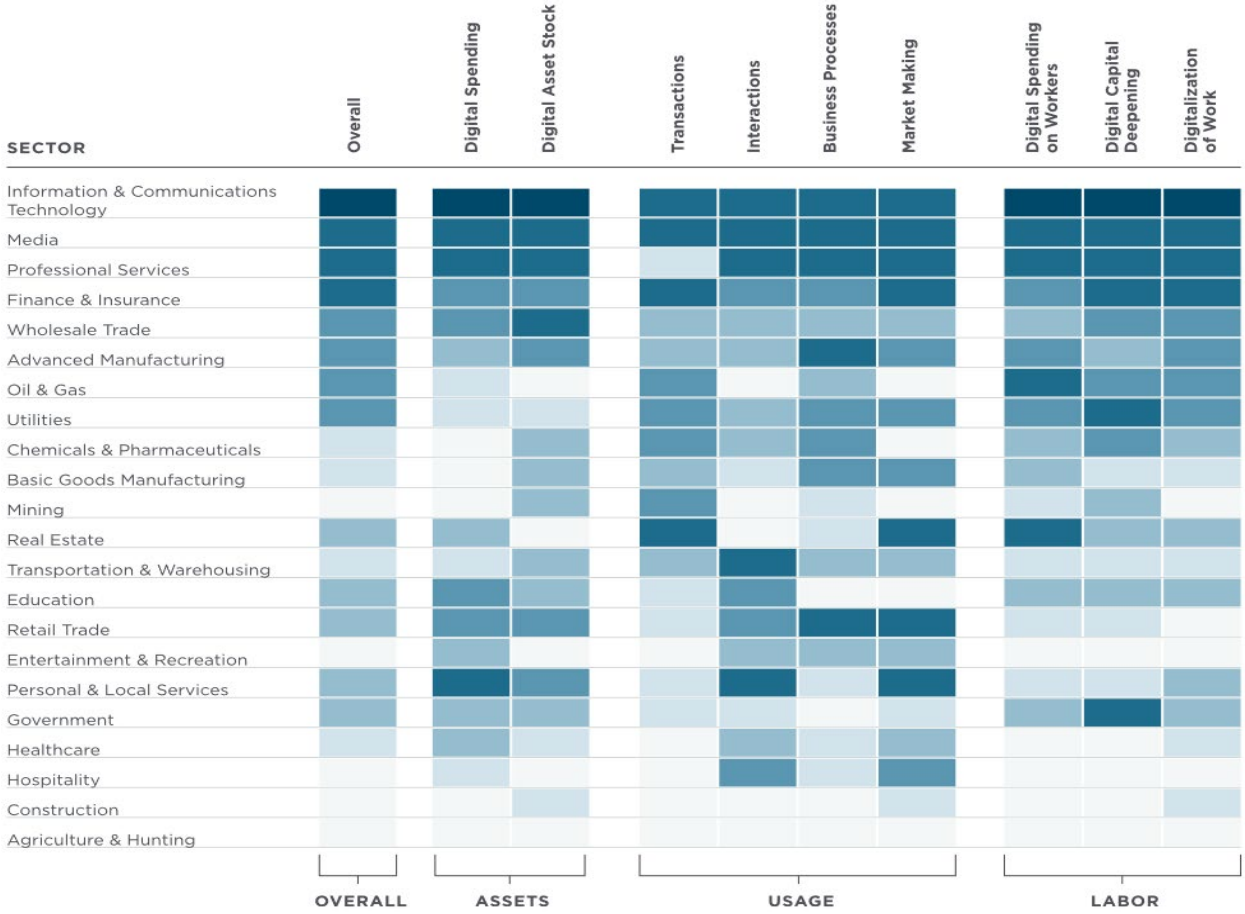

Fig. 2: *The degree of digitalization across economic sectors (Coburn et al, 2019)*

Garcia de Soto et al (2020) write that "the construction sector possesses large amounts of data that is created in dynamic, multi-stakeholder settings in the course of cooperation between several entities (including businesses)". The data is stored not just by the main company involved in a project, but also by contractors, subcontractors, designers, consultants, and suppliers, and this data includes:

- engineering designs;
- calculations and specifications;
- pricing, profit / loss data;
- employee / client information;
- intellectual property;
- banking records.

The use of Building Information Modelling (BIM) and Common Data Environment (CDE) software is revolutionizing the capability of the AECO industry, and we can also indicate the use of emerging technologies such as 3D printing, blockchain, robotics, machine learning, drones, big data, the Internet of Things (IoT), artificial intelligence, predictive analytics, augmented reality, and real-time graphic engines. At the same time, Boyes (2013) stated that: "Unauthorised access to BIM [Building Information Model.ing] data could jeopardise security of sensitive facilities, such as banks, courts, prisons and defence establishments, and in fact most of the Critical National Infrastructure".

We can summarize the transformation of the AECO industry through the formula Construction 4.0, which parallels Industry 4.0 conceptually and is a part of it, in practice. It refers to a new paradigm where digitalization, automation and other cyber-mediated processes (Mantha et al., 2020) lead to the predominance of cyber-

physical systems improving productivity, efficiency and enabling new capabilities (Klinc and Turk, 2019). This is a monumental transformation for an otherwise quite conservative industry.

CYBER THREATS TO CONSTRUCTION 4.0

Coburn et al (2019) emphasizes trends in cybersecurity which can also affect the AECO industry. We mention:

- Increasing Exposure to Digital Attack and Disruption;
- Increasing Propensity for Cyber-Induced Business Interruption;
- Attacks on Digital Supply Chains;
- Growing Potential for Cyber-Physical Loss Events;
- Cyber Attacks Becoming Increasingly Political;
- Changing Motivations of Threat Actors.

The diversity of the AECO industry leads to a wide array of potential threats. We may mention the theft of data, including plans for buildings, the sabotage of designs and plans, the sabotage of automated systems such as construction site robots, the sabotage of control systems, the falsification of data and many other scenarios are possible. Table 1 highlights the likely cyber attacks by the phase of an AECO industry project.

Table 1: *Type of malicious actions in the various phases of an AECO project (source: authors)*

Phase	Common types of attacks
Design phase	data theft, internal and external, sabotage through data falsification or through delaying actions (ransomware)
Building phase	data theft, interference with smart machinery, data manipulation during transmission
Operations phase (and maintenance)	interference with facility functioning, data theft

Several cyberattacks have already occurred in the AECO industry with an intent to steal proprietary information, gain access unauthorized to files, and damage physical elements. As the construction industry becomes more connected and digital platforms become the norm, cyber-attacks will increase. It is true that there is a key overlap between the AECO industry and other domains through the facilities operation component, which is, in some cases, indistinguishable from the operation of other domains which are operationally dependent on the build environment (energy, finance etc.). Nevertheless, AECO offers us the architecture, engineering, construction and possibly decommissioning as the novel areas in which new risks, vulnerabilities and threats stemming from digitalization are manifesting.

The following list of cyber-attacks related to the AECO industry should underscore that diversity (Turk et al, 2022):

- Famously, the Stuxnet worm that destroyed the centrifuges of the Iranian Uranium enrichment program in 2010 qualifies as an AECO incident since the facility management system was compromised to falsify the valuable data that enabled the safe operation of the centrifuges;
- The 2012 Shamoon attack on the ARAMCO petroleum company resulted in the inaccessibility of a large number of computers and the destruction of content in many workstations;
- The CAD drawings of the Australian intelligence headquarters were stolen in 2013;
- Komatsu, a Japanese construction machinery manufacturer, was affected in

2015 by a fraudulent operation targeting deposit collection thorough fictitious websites from applicants;

- A subsidiary of Konecranes (crane manufacturer) fell victim of identity theft, and lost about 17.2 million euros through unwarranted payments;
- Personal details including social security numbers of more than 500 employees of Turner (US based construction company) were exposed due to a phishing attack;
- Hackers exploited the vulnerability of a HVAC (heating, ventilation, and air conditioning) vendor and gained access to unauthorized data in one of the most devastating data breaches at the US retail company, Target;
- The December 2015 Ukraine power grid cyberattack, considered to be the first known successful cyberattack on a power grid, affected 30 substations and left 225,500 customers without electricity for up to six hours;
- The power outage in June 2019 that affected most of Argentina, all of Uruguay, and parts of Paraguay might have been a cyber-attack.

In addition, there is a looming threat of financial frauds, of distributed-denial-of-service attacks and of outages in the cloud infrastructure.

O'Gorman et al (2019) emphasized that the cybercrime field is also reorienting itself towards the extraction of value from enterprises, through ransomware attacks against enterprise, through supply chain attacks, an emphasis on infected attachment in office-related emails.

THE SPECIFICITIES OF THE AECO INDUSTRY

The AECO industry is unlike other domains in which cybersecurity has become a concern. The AEC segment (architecture, engineering and construction), to which we can maybe add the decommissioning process for facilities, is markedly different from the domains in which the operation and facility management segment makes its contributions.

Firstly, the AECO industry features large numbers of participant entities of necessarily varying sizes, sophistication and roles, as can be seen from Figure 3. These entities are brought together into ad-hoc groupings that are constantly shifting (one contractor finishes a type of work and another is signed on for the next phase) and which are temporary in nature, for the duration of the project.

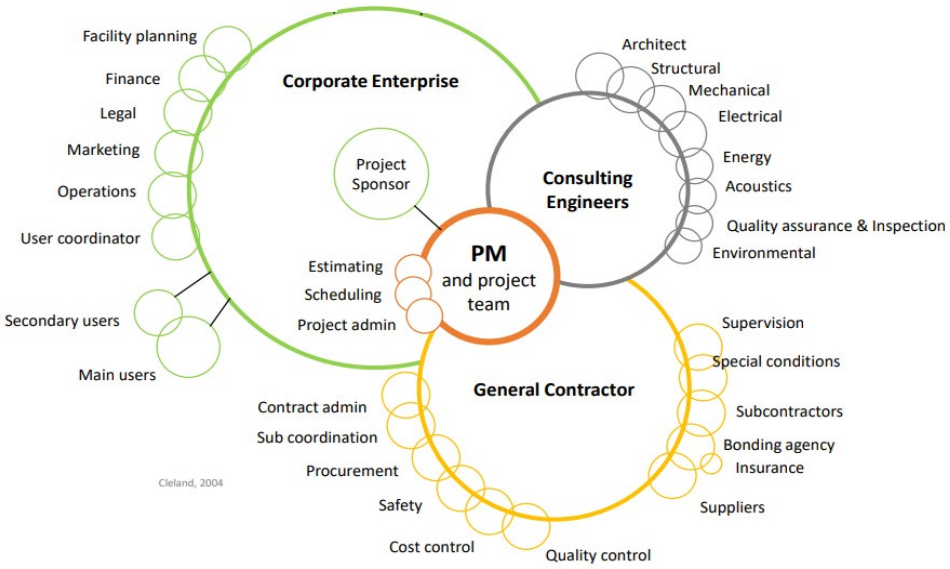

Fig. 3: *An incomplete list of participants in the AECO supply and production chain (Garcia de Soto, 2020)*

From this issue, other considerations spring forth:

- Dynamic workforces and workplaces – an ever shifting roster of personnel and workplaces, in time with the evolution of a particular project, its development phase determining whether an engineer will work in an off-site location (corporate offices) or on-site in a trailer, and what workforce is actually engaged in the project;
- The procession of subcontractors and other specialized entities entering and exiting the project, in a configuration which is unique to each project, makes it difficult to establish a baseline for cybersecurity training for personnel;
- The complex organizations feature important secure communication challenges, especially in a digitalized setting, when the sharing of confidential and sensitive information takes place outside of the main company's secure network;
- There are challenges related to interoperability, as multidisciplinary teams need to cooperate across multiple platforms. Subcontractors and various specialized groups utilize their own software, and cross-checking the various design models or other pieces of data or accessing them from a single platform is usually impossible. These problems are only partially mitigated through the use of Building Information Modelling and Common Data Environment software;
- The construction workforce is incredibly diverse from a socio-economic perspective, with different cultures, education levels, social classes and geographic regions being represented. This heterogeneity is a challenge for cybersecurity education, for security culture and for confidence in achieving a minimum necessary level of protection;
- The challenge of applying conventional thinking about cybersecurity strategy formulation and implementation in organizations. The consortia that actually implement construction projects are fluid and formed on a case-by-case basis. Each project will feature partial or total change in membership. New approaches are needed at strategic level to cope with this complexity.

From a technical standpoint, we can also point out specificities of AECO industry cyber systems compared to those of other entities. Table 2 compares in a structured manner the difference between conventional corporate IT systems and the facility management systems of the operational segment of the AECO industry, which are sometimes complex enough to be designated industrial control systems. One can see that the challenges are different and will require specific approaches and, in certain regards, the AECO associated control systems are less secure and feature more stringent requirements.

Table 2: *Differences between corporate IT systems and building control systems (Turk, 2020)*

Characteristics	Corporate IT Systems	Facilities' systems (ICS)
Lifetime	3-5 years	5-20 years
Availability	Outages have lower impact if they occur outside normal work schedule	Facilities typically require continuous operation of control systems
Time-critical	Delays may be acceptable	Safety-critical elements
Patching	Frequent, even daily	Can be rare
User accounts	Individual users with permissions according to business roles	Shared functional accounts, based on specific role, such as engineer or operator
Outsourcing	Frequent	Depends on situation, but rarer for production systems
Antivirus	Widely used	Difficult/impossible to deploy
Security skills	Limited/good	Non-existent/poor
Security awareness	General awareness	Non-existent/poor
Security testing	Widely employed	Rare, especially since it can damage control systems
Physical security	Secure and manned	Remote and unmanned

Lastly, we can point to another difference – the main threats faced by corporate IT systems are financial losses, denial of service and data losses. The first two feature significant financial and reputational risks. The latter is an operational risk. Whereas, for facility management systems and, at the higher end, Industrial Control Systems, the potential for loss of information is accompanied by two other operational and safety risks – the loss of control over systems, and the loss of accurate perspective over systems (ex: corrupted data in feedback systems) (Turk, 2020).

THE WAY AHEAD

The changing realities of the AECO industry will also leave their mark on Romania. Information is scarce on the extent of digitalization, but it is a likely assumption that the country features examples of the latest trends in digitalization and of under-digitalization, depending on the characteristics of the actors involved (modern facilities or offices, large and sophisticated coordinating entity etc.). The growing exposure to cyber risks and threats of the AECO industry must be first understood and then addressed. In this regard, we consider it necessary for research on digitalization and on the cybersecurity culture, preparation and spending to focus also on the AECO industry. Targeted research can be performed or, for more general studies, the AECO industry can be featured as a separate domain, while acknowledging the overlaps with many of the other domains which are reliant on the built environment (at least the facilities operation segment of the AECO industry). The dearth of research needs to be addressed in order for decision makers to employ of a mix of regulation and other incentives to promote sustainable cyber investment and behaviors on the part of AECO industry participants, especially in the context of the specific challenges facing the industry, as detailed in the previous section.

It is not enough to raise awareness of the issues, since the aforementioned specificities call for tailored responses and specific tools, which need to be developed and implemented, starting with construction-specific cybersecurity frameworks and standards and ending with customized products (Mantha and Garcia de Soto, 2021).

Lastly, decision makers at national but also European levels may consider innovative policy approaches for regulation that emphasize the importance of the construction sector while minimizing the burden on the industry. One such move, taking advantage of pre-existing, mature and well-developed regulatory frameworks for security, would be to add construction projects as a potential critical infrastructure sector (Garcia de Soto et al, 2020). This would involve identifying and designating construction projects/sites from the design phase as temporary critical infrastructures, until they have been completed and the beneficiary has received them. The status could be justified through the proximity of the site to important urban areas or critical infrastructures, through the impact that destruction or disruption would have on the surroundings and through whether the construction project aims to develop a likely critical infrastructure (a new power plant, pipelines, or port facilities) whose delay, subversion or damage would be attractive to adversaries and have an impact on national/European security over a certain threshold. Following the completion of the project, the resulting facility can enter the standard procedure for identifying and designating critical infrastructures (Garcia de Soto et al, 2020).

CONCLUSIONS

Construction 4.0 is an emerging paradigm of digitalization and automation on the AECO industry. While these transformations are not evenly distributed, we can anticipate that future development and the demands placed on the newly built environment (environmental friendliness, efficiency, security, comfort) will lead to the Construction 4.0 paradigm

becoming entrenched also in the developing world. Along with the benefits, there is also an array of new risks, vulnerabilities and threats, which are heightened by the unique characteristics of the construction industry, by the insufficient awareness on the part of industry actors regarding the threat and what should be done about it, and by the dearth of specialized research in the field. Additionally, we must also point out that the cybersecurity environment is continuously evolving towards newer and greater threats, as yearly assessments emphasize. These threats stem not just from the advanced of cybercrime in all its variations, but also from the growth of inter-state competition in the online environment, utilizing cyber-attacks and other operations as a form of hybrid, asymmetrical, unconventional warfare with difficulties in detection, attribution and recovery.

REFERENCE LIST

Boyes, H. (2013). Resilience and Cyber Security of Technology in the Built Environment. The Institution of Engineering and Technology, IET Standards Technical Briefing, London. Available at: https://www.theiet.org/resources/standards/-files/cyber-security.cfm?type=pdf

Coburn, A.W., Daffron, J., Quantrill, K., Leverett, E., Bordeau, J., Smith, A., & Harvey, T. (2019). Cyber risk outlook. Centre for Risk Studies, University of Cambridge, in collaboration with Risk Management Solutions, Inc. Available at: https://www.jbs.cam.ac.uk/faculty-research/centres/risk/publications/technology-and-space/cyber-risk-outlook/cyber-risk-outlook-2019/

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/

Garcia de Soto, B. (2020). Cybersecurity Implications of Construction 4.0. Presentation during the Cybersecurity Implications of Construction 4.0 (CIC) international workshop, New York University of Abu Dhabi, 2 February 2020.

García de Soto, B.; Georgescu, A.; Mantha, B.; Turk, Ž.; Maciel, A. (2020). Construction Cybersecurity and Critical Infrastructure Protection: Significance, Overlaps, and Proposed Action Plan. Preprints 2020, 2020050213 (doi: 10.20944/preprints202005.0213.v1)

Klinc, R., & Turk, Ž. (2019). Construction 4.0–Digital Transformation of One of the Oldest Industries. Economic and Business Review, 21(3), 393-410, DOI: https://doi.org/10.15458/ebr.92

Mantha, B. R., Garcia de Soto, B., Menassa, C. C., & Kamat, V. R. (2020a). Robots in indoor and outdoor environments. Chapter 16. 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/10.1201/9780429398100-16

Mantha, B., García de Soto, B. (2021). Cybersecurity in Construction: Where Do We Stand and How Do We Get Better Prepared?. Frontiers in Built Environment. 7:612668. https://doi.org/10.3389/fbuil.2021.612668

O'Gorman, B., Wueest, C., O'Brien, D., Cleary, G., Lau, H., Power, J.P., Corpin, M., Cox, O., Wood, P., & Wallace, S. (2019) Internet Security Threat Report. Volume 24, Symantec, February 2019, Available at https://docs.broadcom.com/doc/istr-24-2019-en

Turk, Ž. (2020). Cybersecurity – current and related work. Presentation during the Cybersecurity Implications of Construction 4.0 (CIC) international workshop, New York University of Abu Dhabi, 2 February 2020.

Turk, Ž., García de Soto, B., Mantha, B., Georgescu, A., and Maciel, A. (2021). A systemic framework for addressing cybersecurity in construction. Automation in Construction, Vol. 133, Elsevier, https://doi.org/10.1016/j.autcon.2021.103988