Cyber Threats Confronting the Digital Built Environment: Common Data Environment Vulnerabilities and Block Chain Deterrence

[A Literature Review Paper]

ABSTRACT

Purpose: Smart cities provide fully integrated and networked connectivity between digital infrastructure assets and physical infrastructure to form digital economies. However, industrial espionage, cyber-crime and deplorable politically driven cyber-interventions threaten to disrupt and/ or physically damage the critical infrastructure that supports national wealth generation and preserves the health, safety and welfare of the populous. This research presents a comprehensive review of cyber-threats confronting critical infrastructure asset management reliant upon a common data environment (CDE) to augment building information modelling (BIM) implementation.

Design: An interpretivist, methodological approach to reviewing pertinent literature (that contained elements of positivism) was adopted. The ensuing mixed methods analysis: reports upon case studies of cyber-physical attacks; reveals distinct categories of hackers; identifies and reports upon the various motivations for the perpetrators/ actors; and explains the varied reconnaissance techniques adopted.

Findings: The paper concludes with direction for future research work and a recommendation to utilize innovative block chain technology as a potential risk mitigation measure for digital built environment vulnerabilities.

Originality: Whilst cyber security and digitisation of the built environment have been widely covered within the extant literature in isolation, scant research has hitherto conducted an holistic review of the perceived threats, deterrence applications and future developments in a digitized Architecture, Engineering, Construction and Operations (AECO) sector. This review presents concise and lucid reference guidance that will intellectually challenge, and better inform, both practitioners and researchers in the AECO field of enquiry.

KEYWORDS: cyber-security, critical infrastructure, cyber–physical attack, BIM, digital assets, block chain, cyber-deterrence.

INTRODUCTION

We will neglect our cities to our peril, for in neglecting them we neglect the nation - John F. Kennedy

Throughout history, buildings and infrastructure (that cumulatively constitute the built environment) have provided physically secure sanctuaries, protecting inhabitants from theft and malicious attacks (Toy, 2006). Today’s built environment is no exception and conserves this utilitarian physicality. However, contemporary operations and maintenance (O&M) works have become increasingly dependent upon an expansive web of cyber-physical connectivity. Such connectivity has been achieved via an amalgamation of *smart* sensor-based network technologies (Lin *et al.,* 2006), advanced computerization (Pärn and Edwards, 2017) and computational intelligence techniques (Bessis, and Dobre 2014).

Contextualized as *virtual assets*, the voluminous data and information generated throughout a development's whole lifecycle (i.e. design, construction and operations phases) constitutes the basis for knowledge propagation, insightful business intelligence and an invaluable commercial commodity (Edwards *et al.,* 2017). Intelligence on infrastructure asset performance augments decision making via automated analytics geared towards driving economic prosperity, business profitability and environmental conservation (Lin *et al.,* 2006; Ryan, 2016). These palpable benefits have steered government reforms globally towards embedding digitalization throughout the Architecture, Engineering, Construction and Operations (AECO) sector – a sector that encapsulates includes the whole lifecycle of a building's development and subsequent use (Nye, 2017). For example, the UK government's mandated policy 'Digital Built Britain 2025' represents a prominent epitome of ambitious plans to coalesce digitized economies and infrastructure deployment (HM Gov, 2015). This strategic vision has been enacted via the building information modelling (BIM) Level 2 mandate to extend the frontiers of digitized asset handover for building and infrastructure asset owners (HM Gov, 2013). BIM has orchestrated a paradigm shift in the way that information is managed, exchanged and transformed, to stimulating greater collaboration between stakeholders who interact within a common data environment (CDE) throughout the whole lifecycle of a development (Eastman *et al.*, 2011).

Adaptation of a CDE for critical infrastructure developments (i.e. the processes, systems, technologies and assets essential to economic security and/ or public safety) constitutes a key facet of effective asset digitalization and offers potential 'long-term' lifecycle savings for both government and private sector funded projects (Bradley *et al.,* 2016). In the 'short-term', a precipitous amount of *front-loaded* government expenditure earmarked to augment operations management means that a concerted effort has been made to develop accurate BIM asset information models (AIM) for large infrastructure asset managers (e.g. utility companies, Highways England, Network Rail, Environment Agency) (BSI, 2014a).

Government policy edict will continue to transform the *modus operandi* for developing and maintaining buildings and infrastructure within the smart built environment (Bessis, and Dobre, 2014). However, the proliferation of cyber-physical connectivity inherent within a CDE has inadvertently created opportunities for hackers and terrorists, and an omnipresent threat of cyber-crime prevails (Boyes, 2013a) - yet surprisingly, extant literature is overtly sanguine about the conspicuous benefits accrued from digitalization (BSI, 2014a, b, and c; HM Government, 2015). Infrastructure stakeholders (e.g. clients, project managers and designers and coordinators) are unwittingly confronted by clandestine cyber-assailants targeting critical infrastructures through a digital portal facilitated by the CDE's integral networked systems that support O&M activities (Ficco *et al.*, 2017). Curiously, pertinent literature is replete with examples of public policy considerations that evaluate critical infrastructure exposed to intentional attacks, natural disasters or physical accidents (Mayo, 2016). However, the discourse is comparatively silent on substantial cyber-physical security risks posed by a wholesale digital shift within the AECO sector (Kello, 2013). Significant risks posed could disrupt the stream of virtual data produced and in turn, have a profound detrimental impact upon a virtually enabled built environment, leading to physical interruption and/ or destruction of infrastructure assets (e.g. electricity generation) thereby endangering members of the public.

Given this prevailing worldwide menace, a comprehensive literature review of cyber-threats impacting upon the built environment, and specifically critical infrastructure, is conducted. Concomitant objectives are to: i) report upon case studies of cyber-physical attack to better comprehend distinct categories of hackers, their motivations and the reconnaissance techniques adopted; and ii) explore innovative block chain technology as a potential risk mitigation measure for digital built environment vulnerabilities. The research concludes with new hypothesis and research questions that will initiate much needed future investigations and an expanded academic/practitioner discourse within this novel area.

THE DIGITAL JACQUERIE

Globally, an insatiable desire within rural communities for economic migration to cities, continues to engender an upsurge in urbanization – a trend further exacerbated by a projected 9.7 billion population growth by 2050 (UN, 2014a; UN, 2015). For both developed and developing countries, relentless urbanization presents a complex socio-economic conundrum and raises portentous political issues such as: deficiencies in health care provisions (UN, 2014b); lack of resources and malnutrition (UN, 2015); and environmental degradation and pollution (*ibid*). These dystopian challenges can be alleviated through for example, shrewd allocation of resources via social circumscription measures (UN, 2014b). However, politicians worldwide have also contemplated the *implicit assumption of technology inertia* as an impediment to government reform (c.f. Mokyr, 1992). Policies subsequently developed have responded accordingly by mandating advanced technologies within *smart city development* as a panacea to these challenges within the AECO sector – a sector *sensu stricto* berated for its reluctance to innovate (BSI, 2014a). Despite a notable disinclination to change, the AECO sector is widely espoused as being a quintessential economic stimulus (Eastman *et al.*, 2011) - significantly contributing to gross domestic product (HM Gov, 2015) and providing mass-labor employment (DBIS, 2013). Consequently, the AECO sector was a prime candidate for the UK government's Building Information Modelling (BIM) Level 2 mandate that seeks to immerse it within a digital economy. Specifically, the Digital Built Britain report (HM Gov, 2015) aspires that:

> "*The UK has the potential to lead one of the defining developments of the 21st century, which will enable the country to capture not only all of the inherent value in our built assets, but also the data to create a digital and smart city economy to transform the lives of all.*"

Within this digital insurgency, critical infrastructures are at the forefront of the UK government's strategic agenda (Bradley *et al.*, 2016). Unabated advancements in computerization have widened the capability of decision support to providing appropriate resolutions to pertinent infrastructure challenges such as: optimizing planning and economic development (Ryan, 2017); ensuring resilient clean air, water and food supply (*ibid*); and/ or safeguarding integrated data and security systems (BSIa 2014). Throughout the various stages of an infrastructure asset's lifecycle this transition is further fortified by BIM technology and the use of a CDE that can improve information and performance management (Pärn and Edwards, 2017). The palpable benefits of BIM and CDE extend beyond the design and construction phases into the operations phase of asset occupancy and use. BIM technology's innate capability is essential during the asset's operational phase which constitutes up to 80% of the overall whole lifecycle expenditure. In congruence with this statistic, the McNulty (2011) report ambitiously predicts that the potential savings associated with digital asset management and supply chain management may reach up to £580m between 2018/ 2019 and will be facilitated through: i) effective communications; ii) the right speed of action; iii) a focus on detail and change; and iv) incentives and contractual mechanisms that encourage cost reduction. For the purpose of this review, digitization is acknowledged to proliferate throughout all stages of an infrastructure asset's lifecycle in a smart cities and digital economies context; such has potentially severe implications businesses and governments who may be exposed to cyber-crime and -espionage.

Smart Cities and Digital Economies

The British Standards Institute (BSI, 2014a) defines smart cities as:

> *"The effective integration of physical, digital and human systems in the built environment to deliver a sustainable, prosperous and inclusive future for its citizens."*

Within practice, the term smart cities is a linguistic locution that encapsulates fully integrated and networked connectivity between *digital infrastructure* assets and *physical infrastructure* assets to form digital economies (BSI, 2014a). A perspicacious hive mentality is inextricably embedded within smart city philosophy and serves to augment intelligent analysis of real-time data and information generated to rapidly optimize decisions in a cost effective manner (Szyliowicz, 2013; Zamparini and Shiftan, 2013). Consequently, smart cities within the digital built environment form a cornerstone of a *digital economy* that seeks to i) provide more with less; ii) maximize resource availability; iii) reduce cost and carbon emissions (whole lifecycle); iv) enable significant domestic and international growth; and v) ensure that an economy remains in the international vanguard (HM Gov, 2015). The unrelenting pace of digitization worldwide is set to continue with an expected $400bn (US Dollars) investment allocated for smart city development by 2020; where smart infrastructure will consist of circa 12% of the cost (DBIS, 2013). Yet, despite this substantial forecast expenditure, scant academic attention has hitherto been paid to the complex array of interconnected arteries of infrastructural asset management (e.g. roads, ports, rail, aviation and telecommunications) that provide an essential gateway to global markets (*ibid*.).

The Omnipresent Threat of Cyber-Espionage and Crime

Prior to meticulous review of papers an established understanding of the omnipresent threat of cyber-espionage and crime is required. The implementation of smart city technologies has inadvertently increased the risk of cyber-attack facilitated through expansive networked systems (Mayo, 2016). However, cyber-crime has been largely overlooked within the built environment and academic consensus concurs that a cavernous gap exists between the state of security in practice and the achieved level of security maturity in standards (Markets and Markets, 2014). Security specialists and practitioners operating smart buildings, grids and infrastructures are said to coexist in a redundant dichotomy. Instead, academic and policy attention has focused upon either: i) hypothesized scenarios within international security studies (e.g. the protection of military, industrial and commercial secrets) (Rid, 2012); ii) policy planning for cyber-warfare (McGraw, 2013); and/ or iii) the safety of computer systems or networks *per se* rather than cyber-physical attack (activities that could severely impact upon nuclear enrichment, hospital operations, public building operation and maintenance, and traffic management) (Stoddart, 2016). Threats from cyber-crime have arisen partially because of the increased adoption rate of networked devices but also as a result of industry's operational dependency upon IT systems (Boyes, 2013b).

Cyber-criminals are particularly adept at harnessing the intrinsic *intangible value* of digital assets (BSI, 2015) and can decipher the digital economy and its intricacies more perceptively than their counterpart industrialists and businesses that are under attack (Kello, 2013). The most recent 'WannaCry' ransomware attack personified the sophisticated measures deployed by cyber-criminals in navigating networks and identifying, extracting and monetizing data found (Hunton, 2012). While the inherent value of digital assets to owners and creators is often indeterminate, cyber-criminals manipulate data and information to encrypt, ransom or sell it piecemeal (Marinos, 2016). Several prominent instances of unsecure critical infrastructure assets being physically damaged by persistent cyber-crime have been widely reported upon (Peng, *et al.*, 2015). These include: the STUXNET worm that disarmed the Iranian industrial/ military assets at a nuclear facility (Lindsay, 2013); and the malware 'WannaCry' that caused significant damage to the UK's National Health Service (NHS) patient databases, German railway operations and businesses globally (Clarke and Youngstein, 2017). Cyber-attacks remain an omnipresent national security threat to a digital economy's prosperity and digital built environment's functionality and safety. Reporting upon a veritable plethora of threats posed presents significant challenges, as cyber-attacks engender greater anonymity as a malicious activity (Fisk, 2012). Nevertheless, known cases and revolutionary deterrents will form the premise upon which this literature review is based.

METHODOLOGY

The methodology adopted an interpretivist research approach to reviewing extant literature (Walsham, 1995) that contained elements of positivism, where the latter was founded upon the assumption that published material has already been scientifically verified by a robust peer review process. A systematic literature review conducted collected and critically analyzed results emanating from existing studies found within extant literature, where the literature constituted data and the population frame (Levy and Ellis, 2006). An iterative, three stage process was implemented that consisted of: i) *a review of cyber-space and cyber-physical attacks* – case studies of cyber-attacks extracted from the Repository of Industrial Security Incidents (RISI) on-line incident database were reviewed to identify the motivations for hacking and to delineate and define the various types of hackers (otherwise known as actors); ii) a *componential analysis of literature* – a mixed methods componential analysis was conducted to provide a richer understanding of the established, but fragmented, topic of cyber-crime. A componential analysis is a manual qualitative technique that assigns the meaning of a word(s) or other linguistic unit(s) to discrete semantic components (Fisher *et al.*, 2018). In this instance, a cross comparative tabulation matrix of key industries studied and recurrent emergent themes identified was constructed to present analysis findings; and iii) *a report upon innovative* c*yber-deterrence techniques* – an iterative process flow diagram is utilized to explain how 'block chain' can be successfully employed to provide superior protection against ensuing cyber-threats (when compared to encryption and firewalls). Collectively, this chain of documentary evidence and analysis of such, provided a thorough and holistic contextualization of cyber threats confronting the digital built environment.

CYBERSPACE, CYBER-PHYSCIAL ATTACKS AND CRITICAL INFRASTRUCTURE HACKS

In the UK, security analysts from MI5 and MI6 have warned that industrial cyber-espionage is increasing in prevalence, sophistication and maturity, and could enable an entire shut down of critical infrastructure and services including power, transport, food and water supplies (Hjortdal, 2011). A number of pre-eminent politically driven infrastructure intrusions support this assertion and serve as illustrative examples that a prediction of a global pandemic may prove to be distressingly accurate. These intrusions include: the Russian led cyber-attacks on digital infrastructures (banking, news outlets, electronic voting systems) in Estonia in 2007 (Lesk, 2007); the Chinese led hacking of the US electricity network in 2009 (Hjortdal, 2011); and the US led intrusion of Iranian nuclear plant facilities in 2005 (Dennington, 2012).

Cyber-space constitutes the global, virtual, computer based and networked environment, consisting of 'open' and 'air gapped' internet which directly or indirectly interconnects systems, networks and other infrastructures critical to society's needs (European Commission, 2013). Within the vast expanse of cyber-space, Kello (2013) proffers that three partially overlapping territories coexist, namely: i) the world wide web of nodes accessible via URL; ii) the internet consisting of interconnected computers; and iii) the 'cyber-archipelago' of computer systems existing in isolation from the internet residing within a so-called air gap. A CDE hosted on any of the aforementioned territories is precariously exposed to *cyber-physical attack.*

<Insert Figure 1 about here>

Cyber-attack utilizes code to interfere with the functionality of a computer system for strategic, ambiguous, experimental or political purposes (Nye, 2017). Ghandi *et al.*, (2011) expand upon this definition, stating that cyber-attack constitutes: *"any act by an insider or an outsider that compromises the security expectations of an individual, organization, or nation."* Cyber-attacks can take many forms, for example, from publicized web defacements, information leaks, denial-of-service attacks (DoS), and other cyber actions sometimes related to national security or military affairs. *Cyber-physical attacks* can cause disruption or damage to physical assets thus posing serious threats to public health and safety, and/ or the desecration of the environment (Peng *et al.*, 2015). One of the earliest publicly disclosed cyber-physical attacks took place during the Cold War period, when a Soviet oil pipeline exploded due to a so-called logic bomb. The NIST (2014) framework for enhancing the ability of critical infrastructures to withstand cyber-physical attacks proposes that two distinct dichotomous domains must be secured, namely: information technologies (IT) and industrial control systems (ICS) (Rittinghouse and Hancock, 2003). Common threats incurred via IT and ICS include: i) theft of intellectual property; ii) massive disruption to existing operations; and iii) destruction, degradation or disablement of physical assets and operational ability (Szyliowicz, 2013). The European Union Agency for Network and Information Security (ENISA) outlines multiple common sources of nefarious attacks in its malware taxonomy, including: viruses; worms; trojans; botnets; spywares; scarewares; roguewares; adwares; and greywares (Marinos, 2016).

Such attacks are made possible via a huge cyber-attack surface within cyber-space, where every circa 2,500 lines of code presents a potential vulnerability that is identified by a hacker's *reconnaissance* (Nye, 2017). Reconnaissance is the first and most important stage for a successful cyber-attack and seeks to determine the likely strategy for the intrusion (Marinos, 2016). Strategies vary but prominent methods include: scanning; fingerprinting; footprinting; sniffing; and social engineering (refer to Table 3).

<Insert Table 3 about here>

CYBER-ATTACK MOTIVATIONS AND CYBER ACTORS AND INCIDENT ANALYSIS

The RISI database contains a comprehensive record of cyber-physical attack incidents categorized as either *confirmed* or *likely but confirmed* (RISI, 2015). However, prominent commentators contend that attacks are more prevalent than reports suggest and that victims are often reluctant to disclose malicious cyber-attacks against themselves due to potential reputational damage being incurred (Reggiani, 2013). Cyber-physical attacks are therefore shrouded in secrecy by states and private companies, and many states have already conceded the current digital arms race against a panoply of *cyber-actors* (or ‘hackers’) including: hacktivists, malware authors, cyber-criminals, cyber-militias, cyber-terrorists, patriot hackers and script kiddies.

Cyber-actors are frequently classified within one of three thematic categories, namely: i) White Hats; ii) Grey Hats; and ii) Black Hats, where the colour of the hat portrays their intrinsic intentions. White Hats are predominantly legitimately employed security researchers who perform simulated penetration testing hacks to assess the robustness of an organization’s cyber-enabled systems (Cavelty, 2013). They do not have malevolent intentions but rather act on behalf of security companies and concomitant public interest (F-Secure, 2014). Contemporary cyber-*Robin Hood(s)* (or *hacktivists*) fall within the Grey Hat category and act as vigilantes to puncture prevailing power structures (such as Government) by embarrassing them with denial of dervice (DDos) attacks, web defacements, malware, ransomware and trojans. These hacktivists often dabble with illegal means to hack but believe that they are addressing a social injustice and/ or otherwise supporting a good cause. Black Hats are often affiliated with a criminal fraternity or have other malicious intent (Cavelty, 2013). These criminals deploy the same tools used by grey and white hat hackers, but with the deliberate intention to cause harm, vandalism, sabotage, website shutdown, fraud or other illegitimate activities. Many states have increasingly focused upon Grey Hats who have become the new uncontrolled source of hacking

(Betz and Stevens, 2013). Table 4 highlights a number of prominent critical infrastructures hacks extracted from the RISI database and cross references these against the motivations and cyber-actors.

<Insert Table 4 about here >

Blurred Lines: Governments and Civilians

State and non-state actors represent a two pronged source of malicious attacks or threats facing the AECO sector; motivations for these actors are fueled by various catalysts, including patriotism, liberal activism, political ideology, criminal intent and hobby interests (Hjortdal, 2011; Rahimi, 2011). A state is a political entity ('government') that has sovereignty over an area of territory and the people within it (*ibid*.). Within this entity, *state actors* are persons who are authorized to act on its behalf and are therefore subject to regulatory control measures (Betz and Stevens, 2013). A state actor's role can be myriad but often it strives to create positive policy outcomes through approaches such as social movement coalitions (cf. Stearns and Almeida, 2004). Conversely, *non-state actors* are persons or organizations who have sufficient political influence to act or participate in international relations for the purpose of exerting influence or causing change even though they are not part of government or an established institution (Betz and Stevens, 2013). Three key types of legitimate non-state actors exist: i) intergovernmental organizations (IGOs) such as the United Nations, World Bank Group and International Monetary Fund, which are established by a state usually through a treaty (*ibid*); ii) international non-government organizations (NGOs) such as Amnesty International, Oxfam and Greenpeace which are non-profit, voluntary organizations that advocate or otherwise pursue the public good (i.e. economic development and humanitarian aid) (UN); and iii) multinational corporations (MNCs) who pursue their own business interests largely outside the control of national states (UN). Illegitimate non-state actors include terrorist groups and hacktivists acting upon a range of different motivations including personal gain, digital coercion, malevolence and indoctrination of others using ideological doctrine (Brantly, 2014). Since the millennium, governments globally have become increasingly aware of cyber-crime and threats stemming from such non-state actors. Some of the more notable actors include: Anonymous (Betz and Stevens, 2013); Ghost Net (Hunton, 2012); The Red Hacker Alliance (Fisher, 2018); Fancy Bear 'Прикольный медведь' (Canfil, 2016); and Iranian Cyber Army (Rahimi, 2011).

However, the boundary delineation between state actors and non-state actors engaging in cyber-physical attacks has become increasingly blurred (Betz and Stevens, 2013, Papa, 2013). Such attribution has wider implications for the national security of states and national responsibility for non-state actors who often act on behalf of the state, under incitement of nationalistic and ideological motivation (Brantly, 2014). Henderson (2008) aptly describes such blurred lines between governments and civilians by using Chinese cyber-patriot hackers as an exemplar:

> *"The alliance is exactly who and what they claim to be: an independent confederation of patriotic youth dedicated to defending China against what it perceives as threats to national pride."*

A COMPONENTIAL ANALYSIS OF LITERATURE

From an operational perspective, the review protocol sourced published journal materials contained within Science Direct, Web of Science, Scopus and Research Gate databases. Keyword search terms used included: *cyber-security*, *hacking* and any of the following variations of the word *cyber crime*/ *cybercrime*/ or *cyber-crime*. Following a comprehensive review of the journals, four prominent and pertinent clusters of industrial settings were selected to provide the contextual sampling framework and knowledge base for the analysis, namely: i) AECO; ii) transport and infrastructure; iii) information technology; and iv) political science/ international relations. These clusters were selected because they contained the majority of the journal publications on cyber-crime. Within the clusters, six recurrent leitmotifs were identified: i) national and global security; ii) smart cities; iii) critical infrastructure; iv) industrial control systems; v) mobile or cloud computing; and vi) digitalization of the built environment. A cross comparative componential analysis was then conducted (refer to Table 1).

<Insert Table 1 about here >

The componential analysis reveals: i) the percentage frequency that each of the identified thematic groups occur across the four industrial classifications; and ii) the percentage frequency that each thematic group occurs within each individual industrial classification. In ascending order of frequency across all four sectors, the most popular discussed topics were: mobile cloud computing (59.5%); national global security (54.7%) and critical infrastructure

(50%); smart cities (40.4%); industrial control systems (40.4%); and digitization of the built environment (28.5%). Yet curiously within the AECO sector, an inordinate amount of effort was input into mobile and cloud computing (90%); and digitization of the built environment (60%) while far less attention was paid to critical infrastructure (30%); and national and global security (20%). Moreover, none of the papers reviewed were heavily focused upon expounding the virtues and concomitant benefits of digitization but were similarly obvious to the omnipresent threat of cyber-crime posed via the vulnerable CDE portal.

A CDE is commonly established during the feasibility or concept design phases of a development (BSI2014a, b). An information manager will then manage and validate the processes and procedures for the exchange of information across a network for each key decision gateway stage (including: work in progress (WIP), shared, published and archive stages). Cloud-based CDE platforms are ubiquitous but common solutions include: ProjectWise; Viewpoint (4P); Aconex; Asite; and SharePoint (Shafiq *et al.*, 2013). The internal work flow and typical external information exchange in BIM relies upon the re-use and sharing of information in a CDE. Integrating BIM (and other file databases e.g. IFC, GBXML, CSV, DWG, XML) within a CDE ensures a smooth flow of information between all stakeholders and is specified and articulated through its levels of development or design (Eastman, 2011; Lin and Su, 2013). The level of design (LOD) is classified on a linear scale ranging from LOD 1 (covering a conceptual 'low definition' design) to LOD 7 (for an as-built 'high definition' model). With each incremental increase in LOD, the range and complexity of asset information within models built begins to swell and the data contained within becomes accessible to an increased amount of stakeholders. As a consequence, the magnitude of potential cyber-crime also increases and it is imperative therefore, that effective cyber-security deterrence measures are set.

Perhaps the most crippling aspect of deterrence is the poor rate of attribution (also known as *tracebacking* or *source tracking*); where attribution seeks to determine the identity or location of an attacker or attacker's intermediary (Brantly, 2014). Affiliation further exacerbates aattribution rates, for example, nefarious and malicious attacks on critical infrastructure by non-state 'patriot' actors who proclaim cyber-warfare in the name of nationalist ideologies can create ambiguity with state actors (Lindsay, 2015). Extant literature widely acknowledges that states actively recruit highly skilled hackers to counter-attack other state governed cyber-activities, in particular against critical infrastructure assets (Thomas, 2009). Yet the paucity of identification or disclosure of attacker identities has made the hacking culture even more enticing for both non-state actors and state actors. Whilst network attribution or IP address traceability to a particular geographical region is possible, lifting the cyber veil to reveal the affiliation between the attacker and their government remains difficult (Canfil, 2016). In the case of potential threats to the AECO sector, attribution of industrial cyber-espionage remains an imminent threat not only to the business in operation but also for the nation state security.

CYBER-DETERRENCE

Cyber-deterrence measures rely largely upon good practice adopted from standards ISO 27001 and ISO 27032 (ISO, 2013; ISO, 2012). In the context of the digital built environment (and specifically BIM), recently published cyber-security good practice manual PAS 1198-Part 5 suggests deploying five measures of deterrence: i) a built asset security manager; ii) a built asset security strategy (BASS); iii) a built asset security management plan (BASMP); iv) a security breach/ incident management plan (SB/IMP); and v) built asset security information requirements (BASIR). For other sources of cyber-security guidance PAS 1198-Part 5 recommends adherence to other pre-existing legislative documentation – refer to Table 2.

<Insert Table 2 about here>

Other ambiguous guidance notes that refer to taking ‘appropriate mitigation strategies’ have largely ignored the increased vulnerability of semantic and geometric information that is sustained within a BIM (BSI, 2013; BSI, 2014c). For example Institute of Engineering and Technology (Boyes, 2013b) report, entitled: ‘Resilience and Cyber Security of Technology in the Built Environment’, states that:

> *“Unauthorised access to BIM data could jeopardise security of sensitive facilities, such as banks, courts, prisons and defence establishments, and in fact most of the Critical National Infrastructure.”*

Deterrence measures recommended in PAS 1192-5 have largely overlooked BIM data contained within a CDE and the onslaught of cyber-physical connectivity in critical infrastructures (Liu *et al.*, 2012). Currently, the most common means of deterrence for cyber-physical connectivity in critical BMS infrastructures is via network segregation (the firewall) (Mayo, 2016) and secure gateway protection (encryption) for securing from external threats complicit with ANSI/ISA-99 (ANSI, 2007). However, in a digital economy where over 50 billion devices are continuously communicating, neither firewalls nor encryption alone can guarantee effective cyber-security. Hence, a more robust systemic means of data integrity is required in the digital built environment.

Block Chain - A New Frontier for Cyber-Deterrence

Under the alias Satoshi Namamoto, the Bitcoin (cryptocurrency) was published as the first block chain application on the internet (Turk, and Klinc, 2017). This advancement opened a springboard of applications that utilize block chain technology to remove third party distribution of digital assets using peer-to-peer sharing (*ibid*). Whilst the majority of current applications have utilized crypto currency and smart contracts, the applications for digital asset transference seem limitless. Block chain's earliest applications were in economics (Huckle *et al.*, 2016); software engineering (Turk, and Klinc, 2017); Internet of Things (Zhang and Wen, 2016); and medicine (Yue *et al.*, 2016) – albeit, more recently applications within the built environment have been explored (Sun *et al.*, 2016). Block chain technology has the potential to overcome the aforementioned cyber-security challenges faced in the digital environment, as a result of its distributed, secure and private nature of data distribution. A positive correlation exists between an increasing number of collaborators (or peers) within a CDE and the potential to secure such assets in a peer-to-peer environment which thrives and increases in security.

Block chain technology is suitable for sectors with increased risk of: i) *fraud* – such as susceptible, crucial infrastructures containing sensitive industrial information that is at risk from industrial espionage, ii) *intermediaries* - for example, providers of BMS systems and other IT software vendors hosting sensitive infrastructure asset details; iii) *throughput* – such as operators updating and sharing asset information in a CDE; and iv) *stable data* - for instance, data generated for built assets can be utilized for up to 40 years post project inception. Block chain technology offers better encryption against hacking than any other current deterrence measures available and is commonly suggested in the cyber-security standards available (Turk, and Klinc, 2017).

<Insert Figure 2 about here >

The application of block chain technology within digital built asset information exchange is suggested due to its secure framework for data transference. Block chain technology has been hailed as a hacker/ tamper safe ecosystem for digital asset transfers (*ibid*). Figure 2 delineates a ten stage process to demonstrate how the existing functionality of block chain technology can be harnessed in a CDE environment when sharing sensitive digital information about assets - viz: i) asset information is securely shared via a network (e.g. url nodes, interconnected computer networks or an air gapped internet); ii) asset data (whether a 3D or digital model) is converted into a block which represents a digital transaction of asset data; iii) stakeholder interaction within a federated CDE environment will receive a tracked record of the individual transaction created by nodes sharing the block; iv) block chain miners (usually computer scientists) validate and maintain the newly created block chain; v) payment methods for block chain miners vary but a group of miners enter into a competitive process where the first to validate the block chain receives payment; vi) the federated block chain environment is approved; vii) the new block is added to the existing chain of digital transactions to extend the block chain; viii) the digital asset can now be securely shared upon validation; ix) to hack the network, assailants would need to hack every single node within the block chain, thus making the task far more difficult; x) the network of nodes created by multiple stakeholders' transactions provides a more sophisticated and secure approach to protecting digital assets when compared to encryption and firewalls. Herein lies the novelty of this review – blockchain technology can offer a potential framework to future AECO software applications and systems designed to secure the transfer of sensitive project data in a BIM and CDE environment.

DISCUSSION AND FUTURE WORK

Contrary to within the fields of computer science, political science/ international relations and international law, cyber-security is far less understood within the AECO sector (Mayo, 2016). Consequently, existing controls are inadequate and poorly managed. Key findings emanating from these other eminent fields provide invaluable insights into the cyber-security technologies and developments that can be successfully transferred and applied to critical infrastructure within the AECO sector to address current deficiencies (Baumeister, 2010). However, successful practitioner alignment and knowledge enhancement requires time and investment for additional research and testing of such concepts (Metke and Ekl, 2010) - such exceeded the current confines of this review paper. Within the international security research realm, the following predispositions have weakened scholarly understanding of cyber-threat occurrences and the likelihood of attacks on critical infrastructure. These limitations require future work, namely:

i) *Improved understanding of motivations* – an inordinate amount of attention is paid to 'cyber-threats' under the guise of malevolent lines of code. Yet finding a resolution to the root cause of cyber-crime requires a deeper understanding of the motivations behind such malicious scripts and attacks;

ii) *Address the specific operational threats to bespoke critical infrastructure* – each individual critical infrastructure project (e.g. hospitals, nuclear facilities, traffic management systems) has bespoke operational functionality and hence different vulnerabilities. Mapping of these vulnerabilities is required as a first step to developing efficient and effective risk mitigation strategies to better secure assets;

iii) *Distinguish between physical destruction and theft* – literature and standards have predominantly focused upon data protection within the context of cyber-attack. However, physical damage has received far less attention even though such could lead to catastrophic economic damage. Greater distinction between physical destruction and theft is therefore needed to delineate the scale and magnitude of cyber-crime;

iv) *Consolidate greater international governmental collaboration* - cyber-attacks can readily cross international borders and national law enforcement agencies often find it difficult to take action in jurisdictions where limited extradition arrangements are available. Although standard international agreements have been made on such issues (c.f. the Budapest Convention on Cyber-crime), which seek to criminalize malevolent cyber-activities, notable signatories (such as China and Russia) are absent. Far greater cooperation between sovereign states is therefore urgently needed to develop robust international agreements that are supported by all major governments.;

v) *Gauge practitioner awareness* – future work should seek to identify existing predispositions and awareness of cyber-attack and cyber-crime amongst AECO professionals either through in depth interviews or practitioner surveys. Case studies are also required to measure and report upon contemporary industry practice and how any cyber-crime incidents were managed; and

vi) *Proof of concept* – Development and testing of an innovative proof of concept blockchain application specifically designed for AECO professionals. Such developmental work would allow the thorough testing of blockchain technology in practice to confirm or otherwise its effectiveness.

To reconcile the challenges of future work, researchers and practitioners within the AECO sector will have to investigate how to adopt cyber-deterrence approaches applied within more technologically advanced and sensitive industries such as aerospace and automotive. Such knowledge transference may propagate readily available solutions to challenges posed. Cyber-security awareness and deterrence measures within the BIM and CDE process will help secure critical infrastructure, developed, built and utilized – the challenges and opportunities identified here require innovative solutions such as block chain technologies to transform standard industry practice and should be augmented with far greater industry-academic collaboration.

CONCLUSION

Infrastructure provides the essential arteries and tributaries of a digital built environment that underpins a contemporary digital economy. However, cyber-attack threatens the availability and trustworthiness of interdependent networked services on both corporate and national security levels. At particular risk are the critical infrastructure assets (such as energy networks, transport and financial services) hosted on large networks connected to the internet (via a CDE) to enable cost-efficient remote monitoring and maintenance. Any disruption or damage to these assets could have an immediate and widespread impact by jeopardizing the well-being, safety and security of citizens. To combat the potential threat posed, greater awareness among AECO stakeholders is urgently needed; this must include governments internationally and private sector partners collaborating together to expand upon existing ISO and BIM-related standards for improved response to a cyber incident. As well as preventative measures, reactive national plans are required (i.e. raising cyber security awareness on government funded BIM projects) to quickly deal with breaches in security and ensure services are provided with minimum disruption.

It is argued in this paper that the CDE adopted with BIM in the AECO sector acts as a springboard for the wider stakeholder engagement with networked data sharing in a centralized manner yielding such systems vulnerable for future cyber-physical attacks. The pinnacle of cyber-security research breakthroughs in cryptography have resulted in the development of decentralized block chain technology. It is hypothesized that block chain technology offers a novel and secure approach to storing information, making data transactions, performing functions, and establishing trust, making it suitable for sensitive digital infrastructure data contained in BIM and CDE environment high security requirements. Whilst block chain applications are largely at a nascent stage of development within the AECO sector, this review paper has highlighted its novel application to fortify security of digital assets residing within a

BIM and CDE environment – thus extending applications beyond its origins in cryptocurrency. Future research will be required to prove, modify or disprove this hypothesis presented. However, block chain alone cannot guarantee total immunity to cyber–attacks so additional research is required to: understand the motivations for cyber-attack/ crime; identify the specific operational threats to bespoke critical infrastructure and develop appropriate strategies to mitigate these; develop more exhaustive international standards (or enhance existing standards) to distinguish between physical destruction and theft; and establish measures needed to consolidate greater international governmental collaboration.

REFERENCES

Ani, U. P. D., He, H. and Tiwari, A. (2017) Review of Cybersecurity Issues in Industrial Critical Infrastructure: Manufacturing in Perspective. Journal of Cyber Security Technology, Vol. 1, pp.32-74.

ANSI (2007) ISA-99.00.01-2007 Security for Industrial Automation and Control Systems; Part 1: Terminology, Concepts, and Models, ISA Available via: https://web.archive.org/web/20110312111418/http://www.isa.org/Template.cfm?Section=Shop_ISA&Template=%2FEcommerce%2FProductDisplay.cfm&Productid=9661 [Accessed: February, 2018].

Baumeister, T. (2010) Literature Review on Smart Grid Cyber Security, Collaborative Software Development Laboratory at the University of Hawaii. Available via: http://www.tbaumeist.com/publications/LiteratureReviewOnSmartGridCyberSecurity_2010.pdf [Accessed: February, 2018].

Bessis, N., Dobre, C. (2014) Big Data and Internet of Things: A Roadmap for Smart Environments, London: Springer International Publishing. ISBN: 978-3-319-05029-4.

Betz, D., J. and Stevens, T. (2013) Analogical Reasoning and Cyber Security, Security Dialogue Vol. 44, No. 2, pp. 147–164.

Boyes, H. (2013a) Cyber Security of Intelligent Buildings. 8th IET International System Safety Conference incorporating the Cyber Security Conference 2013, Cardiff, UK.

Boyes H. (2013b) Resilience and Cyber Security of Technology in the Built Environment The Institution of Engineering and Technology, IET Standards Technical Briefing, London. Available via: https://www.theiet.org/resources/standards/-files/cyber-security.cfm?type=pdf [Accessed: February, 2018].

Bradley, A, Li, H., Lark, R. and Dunn, S. (2016) BIM for Infrastructure: An Overall Review and Constructor Perspective, Automation in Construction, Vol. 71, No. 2, pp. 139-152.

Brantly, A. F. (2014) The Cyber Losers. Democracy & Security, Vol. 10, No. 2, pp. 132-155.

BSI (2014a) PAS 180 Smart Cities. Vocabulary. British Standards Institution, London. Available via: https://www.bsigroup.com/en-GB/smart-cities/Smart-Cities-Standards-and-Publication/PAS-180-smart-cities-terminology/ [Accessed: February, 2018].

BSI (2014b) PAS 1192-3 Specification for Information Management for the Operational Phase of Assets Using Building Information Modelling, British Standards Institution, London. Available via: https://shop.bsigroup.com/ProductDetail/?pid=000000000030311237 [Accessed: February, 2018].

BSI (2014c) PAS 754:2014 Software Trustworthiness. Governance and Management. Specification Available via: https://shop.bsigroup.com/ProductDetail/?pid=000000000030284608 [Accessed: February, 2018].

BSI (2015) PAS 1192-5 (2015) Specification for Security Minded Building Information Modelling, Digital Built Environments and Smart Asset Management. British Standards Institution, London. Available via: https://shop.bsigroup.com/ProductDetail/?pid=000000000030314119 [Accessed: February, 2018].

BSI (2013) PAS 555:2013 Cyber Security Risk. Governance and Management Specification Available via: https://shop.bsigroup.com/ProductDetail/?pid=000000000030261972 [Accessed: February, 2018].

Canfil, J. K. (2016) Honing Cyber Attribution: A Framework for Assessing Foreign State Complicity, Journal of International Affairs, Vol. 70, No. 1, pp 217. Available via: https://www.questia.com/read/1G1-476843518/honing-cyber-attribution-a-framework-for-assessing [Accessed: February, 2018].

Cavelty, M.D. (2013) From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. International Studies Review, Vol. 15, pp. 105-122.

Chong, H.Y., Wong, J. S. and Wang, X. (2014) An Explanatory Case Study on Cloud Computing Applications, Automation in Construction, Vol. 44, pp. 152-162.

Clarke, R. and Youngstein, T. (2017) Cyberattack on Britain's National Health Service, New England Journal of Medicine, Vol. 377, pp. 409-411.

DBIS (2013) Smart City Market: Opportunities for the UK, Department for Business, Innovation and Skills, BIS Research Papers Ref: BIS/13/1217, DBIS: London. Available via: https://www.gov.uk/government/publications/smart-city-market-uk-opportunities [Accessed: February, 2018].

Denning, D. (2012) Stuxnet: What has Changed? Future Internet, Vol. 4, No. 3, pp. 672-687;

Eastman, C., Eastman, C.M., Teicholz, P., Sacks, R. and Liston, K. (2011) BIM Handbook: A Guide to Building Information Modeling for Owners, Managers, Designers, Engineers and Contractors, Hoboken: John Wiley & Sons. ISBN: 978-0-470-54137-1

Edwards, D. J., Pärn, A. E., Love, P.E.D. and El-Gohary, H (2017) Research Note: Machinery, Manumission, and Economic Machinations, Journal of Business Research, Volume 70, January 2017, pp. 391-394.

European Commission (2013) Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN 1 Final, Brussels: European Commission. Available via:

https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf [Accessed: February, 2018]

Eom S-J and Paek J-H (2006). Planning Digital Home Services Through an Analysis of Customers Acceptance, ITcon Vol. 11, Special issue IT in Facility Management, pg. 697-710, Available via: http://www.itcon.org/2006/49 [Accessed: February, 2018].

Ficco M., Choraś, M., and Kozik, R. (2017) Simulation Platform for Cyber-security and Vulnerability Analysis of Critical Infrastructures, Journal of Computational Science, Vol. 22, pp. 179-186..

Fisher, R., D. (2018) Cyber Warfare Challenges and the Increasing use of American and European Dual-use Technology for Military Purposes by the People's Republic of China (PRC). United States House of Representatives, Committee on Foreign Affairs. Available via: http://archives-republicans-foreignaffairs.house.gov/112/Fis041511.pdf [Accessed: February, 2018]

Fisk, D. (2012) Cyber Security, Building Automation, and the Intelligent Building, Intelligent Buildings International, Vol. 4, No. 3, pp. 169-181.

Formby, D., Srinivasan, P., Leonard, A., Rogers, J. and Beyah, R. A. (2016) Who's in Control of your Control System? Device Fingerprinting for Cyber-physical Systems. Network and Distributed System Security Symposium (NDSS), February 26 to March 1, San Diego, California.

F-Secure Labs (2014) Havex Hunts for ICS and SCADA Systems. Available via: https://www.f-secure.com/weblog/archives/00002718.html [Accessed: February, 2018]

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., and Laplante, P. (2011) Dimensions of Cyber-attacks: Cultural, Social, Economic, and Political, in IEEE Technology and Society Magazine, Vol. 30, No. 1, pp. 28-38.

Govinda, K. (2015) Design of Smart Meter Using Atmel 89S52 Microcontroller. Procedia Technology, Vol. 21, pp. 376-380.

Henderson, S. (2008) Beijing's Rising Hacker Stars: How Does Mother China React? IO Sphere Journal February 28th, 2008. Available via: https://www.noexperiencenecessarybook.com/jplV6/beijing-39-s-rising-hacker-stars-how-does-mother-china-react.html [Accessed: February, 2018].

Hjortdal, M. (2011) China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence, Journal of Strategic Security, Vol. 4, No. 2, pp. 1-24.

HM Government (2015) Digital Built Britain: Level 3 Building Information Modelling - Strategic Plan, 26 February 2015, London: HM Publications. Available via: https://www.gov.uk/government/publications/uk-construction-industry-digital-technology [Accessed: February, 2018].

HM Government (2013) Building Information Modeling Industrial Strategy: Government and Industry in Partnership, Government Construction Strategy, London. Available via: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/34710/12-1327-building-information-modelling.pdf [Accessed: February, 2018].

Howell, S., Rezgui, Y. and Beach, T. (2017) Integrating Building and Urban Semantics to Empower Smart Water Solutions, Automation in Construction, Vol. 81, pp. 434-448.

Huckle S., Bhattacharya R., White M. and Beloff, N. (2016) Internet of Things, Blockchain and Shared Economy Applications, Procedia Computer Science, Vol. 98, pp. 461-466.

Hunton, P. (2012) Data Attack of the Cybercriminal: Investigating the Digital Currency of Cybercrime, Computer Law & Security Review, Vol. 28, No. 2, pp. 201-207.

IET - Institution of Engineering and Technology (2014) Code of Practice for Cyber Security in the Built Environment Available via: https://electrical.theiet.org/books/standards/cyber-cop.cfm? [Accessed: February, 2018].

IET - Institution of Engineering and Technology (2013) Resilience and Cyber Security of Technology in the Built Environment, Available via: https://www.theiet.org/resources/standards/cyber-buildings.cfm?origin=pr [Accessed: February, 2018].

ISO (2013) 27001 The International Information Security Standard, International Organization for Standardization (ISO), Geneva, Switzerland. Available via: https://www.itgovernance.co.uk/iso27001 [Accessed: February, 2018].

ISO (2012) 27032 Information Technology – Security Techniques – Guidelines for Cybersecurity, International Organization for Standardization (ISO), Geneva, Switzerland. Available via: https://www.itgovernance.co.uk/shop/product/iso27032-iso-27032-guidelines-for-cybersecurity [Accessed: February, 2018].

ISO (2011) ISO/IEC 29100:2011 Information Technology - Security Techniques - Privacy framework, ed.1 Available via: https://www.iso.org/standard/45123.html [Accessed: February, 2018].

Jones, L. (2016) Securing the Smart City: Built Environment Cyber Security. Engineering and Technology, Vol. 11, pp.30-33. DOI: 10.1049/et.2016.0501

Jaatun, M.G., Røstum, J., Petersen, S. and Ugarelli, R. (2014) Security Checklists: A Compliance Alibi, or a Useful Tool for Water Network Operators?, Procedia Engineering, Vol. 70, pp. 872-876,.

Kello, L. (2013) The Meaning of the Cyber Revolution: Perils to Theory and Statecraft, International Security, Vol. 38, pp. 7-40.

Kochovski, P. and Stankovski, V. (2017) Supporting Smart Construction with Dependable Edge Computing Infrastructures and Applications, Automation in Construction, Volume 85, 2018, pp. 182-192..

Koo, D., Piratla, K. and Matthews, C. J (2015). Towards Sustainable Water Supply: Schematic Development of Big Data Collection Using Internet of Things (IoT). Procedia Engineering, Vol. 118, pp.489-497.

Levy, Y., and Ellis, T. J. (2006) A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research, Informing Science, Vol. 9, pp. 181-212. Available via: http://inform.nu/Articles/Vol9/V9p181-212Levy99.pdf [Accessed: February, 2018].

Lesk, M. (2007) The New Front Line: Estonia Under Cyber Assault, IEEE Security & Privacy, Vol. 5, No. 4, pp. 76-79, July-Aug. 2007.

Lin, S., Gao, J. and Koronios, A. (2006) Key Data Quality Issues for Enterprise Asset Management in Engineering Organisations, International Journal of Electronic Business Management (IJEBM), Vol. 4, No. 1, pp. 96-110. Available via: http://ijebm.ie.nthu.edu.tw/IJEBM_Web/IJEBM_static/Paper-V4_N1/A10-E684_3.pdf [Accessed: February, 2018].

Lin, Y.C. and Su, Y.C. (2013) Developing Mobile-and BIM-based Integrated Visual Facility Maintenance Management System, The Scientific World Journal.

Lindsay, J. R. (2013) Stuxnet and the Limits of Cyber Warfare. Security Studies, Vol. 22, No. 3, pp. 365-404.

Lindsay, J. R. (2015) The Impact of China on Cybersecurity: Fiction and Friction. International Security, Vol. 39, No. 3, pp. 7-47.

Liu, J., Xiao, Y., Li, S., Liang, W. and Chen, C. P. (2012) Cyber Security and Privacy Issues in Smart Grids. IEEE Communications Surveys & Tutorials, Vol. 14, pp. 981-997.

Marinos, L. (2016) ENISA Threat Taxonomy A Tool for Structuring Threat Information, European Union Agency for Network and Information Security. Available via: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/etl2015/enisa-threat-taxonomy-a-tool-for-structuring-threat-information/view [Accessed: February, 2018].

Markets and Markets (2014) Smart HVAC Controls Market by Product Type, Components, Application, Operation & Geography - Analysis and Forecast to 2014 - 2020. Available via: http://goo.gl/Ay2LjI. [Accessed: February 2018].

McGraw, G. (2013) Cyber War is Inevitable (Unless We Build Security In), Journal of Strategic Studies, Vol. 36, No. 1, pp. 109-119.

McNulty (2011) Realising the Potential of GB Rail - Final Independent Report of the Rail Value for Money Study - Summary Report, London, UK: Department for Transport. Available via: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/4203/realising-the-potential-of-gb-rail-summary.pdf [Accessed: February, 2018].

Mayo G. (2016) Bas and Cyber Security: A Multiple Discipline Perspective, Proceedings of the American Society for Engineering Management 2016 International Annual Conference S. Long, E-H. Ng, C. Downing, & B. Nepal eds. Available via: https://www.researchgate.net/publication/309480358_BAS_AND_CYBER_SECURITY_A_MULTIPLE_DISCIPLINE_PERSPECTIVE [Accessed: February, 2018].

Metke, A. R. and Ekl, R. L. (2010) Security Technology for Smart Grid Networks. IEEE Transactions on Smart Grid, Vol. 1, No. 1, pp. 99-107.

Mike, T. (2006) Integrated Building Systems: Strengthening Building Security While Decreasing Operating Costs. Journal of Facilities Management, Vol. 4, No. 1, pp.63-71.

Mokyr J. (1992) Technological Inertia in Economic History, The Journal of Economic History Vol. 52, No. 2, pp. 325-338.

National Institute of Standards and Technology (NIST) (2017) Framework for Improving Critical Infrastructure Cybersecurity, Draft Vesion 1.1, January 10th 2017. Available via: https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0ahUKEwiq0orLhOHUAhVkBsAKHfJLB6oQFgg8MAE&url=https%3A%2F%2Fwww.nist.gov%2Fdocument%2Fdraft-cybersecurity-framework-v11pdf&usg=AFQjCNGCtebSkMYn_Eo8A-49ANj7TEz2NA&cad=rjt [Accessed: February, 2018].

Nye J., S. (2017) Deterrence and Dissuasion in Cyberspace, International Security, Vol. 41, No. 3 (Winter 2016/17), pp. 44–71.

Papa, P. (2013) US and EU Strategies for Maritime Transport Security: A Comparative Perspective, Transport Policy, Vol. 28, pp. 75-85.

Pärn, E.A. and Edwards, D.J. (2017) Conceptualizing the FINDD Toolkit: A Case Study of BIM/ FM Integration, Automation in Construction, Vol. 80, pp. 11-21.

Paridari K. MadyA., E., La Porta, S., Chabukswar, R.,Blanco, J.,Teixeira, A.,Sandberg, H., Boubekeur, M., (2016) Cyber-Physical-Security Framework for Building Energy Management System, 2016 ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS), Vienna, 2016, pp. 1-9. DOI: 10.1109/ICCPS.2016.7479072

Patel, S. C., Bhatt, G. D. and Graham, J. H. (2009) Improving the Cyber Security of SCADA Communication Networks, Communications of the ACM, Vol. 52, No. 7, pp.139-142.

Peng,Y., Wang,Y., Xiang, C., Liu, X., Wen,Z. and Chen, D. (2015) Cyber-physical Attack-Oriented Industrial Control Systems (ICS) Modeling, Analysis and Experiment Environment, International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 322- 326.

Rahimi, B. (2011) The Agonistic Social Media: Cyberspace in the Formation of Dissent and Consolidation of State Power in Postelection Iran. The Communication Review, Vol. 14, pp. 158-178.

Rasmi, M. and Jantan, A. (2013) A New Algorithm to Estimate the Similarity Between the Intentions of the Cyber Crimes for Network Forensics. Procedia Technology, Vol. 11, pp. 540-547.

Reggiani, A. (2013) Network Resilience for Transport Security: Some Methodological Considerations. Transport Policy, Vol. 28, pp. 63-68.

Reniers, G. L. L. and Dullaert, W. (2013) A Method to Assess Multi-modal Hazmat Transport Security Vulnerabilities: Hazmat Transport SVA. Transport Policy, Vol. 28, pp. 103-113.

Rid, T. (2012) Cyber War will not Take Place, Journal of Strategic Studies, Vol. 35, No. 1, pp. 5–32.

Rittinghouse, J. and Hancock, W. M. (2003) Cybersecurity Operations Handbook, Amsterdam, Netherlands: Elsevier Science. ISBN: 978-1-55558-306-4

RISI (2015) The Repository of Industrial Security Incidents Database, Available via: http://www.risidata.com/Database [Accessed: February, 2018].

Ryan, D., J. (2016) Engineering Sustainable Critical Infrastructures, International Journal of Critical Infrastructure Protection, Vol. 15, pp. 47-59.

Safavi, S., Shukur, Z. and Razali, R. (2013) Reviews on Cybercrime Affecting Portable Devices. Procedia Technology, Vol. 11, pp. 650-657.

Shafiq M. T., Matthews, J. Lockley, S. R. (2013) A Study of BIM Collaboration Requirements and Available Features in Existing Model Collaboration Systems, Journal of Information Technology in Construction (ITcon), Vol. 18, pg. 148 – 161.

Shitharth, S. and Winston, D. P. (2015) A Comparative Analysis Between Two Countermeasure Techniques to Detect DDoS with Sniffers in a SCADA Network. Procedia Technology, Vol. 21, pp. 179-186.

Stearns, L.B. and Almeida, P.D. (2004) The Formation of State Actor-Social Movement Coalitions and Favorable Policy Outcomes, Social Policy, Vol. 51, No. 4, pp. 478-504.

Stoddart, K. (2016) Live Free or Die Hard: U.S-UK Cybersecurity Policies, Political Science Quarterly, Vol. 131, No. 4, pp. 803-842.

Sun J., Yan J., and Zhang K.Z. (2016) Blockchain-based Sharing Services: What Blockchain Technology can Contribute to Smart Cities, Financial Innovation, Vol. 2, p. 26.

Szyliowicz, J. S. (2013) Safeguarding Critical Transportation Infrastructure: The US Case, Transport Policy, Vol. 28, pp. 69-74.

Tan, S., Song, W. Z., Stewart, M., Yang, J. and Tong, L. (2018) Online Data Integrity Attacks Against Real-Time Electrical Market in Smart Grid. IEEE Transactions on Smart Grid, Vol. 9, pp.313-322.

Toy, S. (2006) History of Fortification from 3000 BC to AD 1700 (No. 75) Barnsley, UK: Pen and Sword Military Classics. ISBN: 1-88415-358-4.

Turk, Ž. and Klinc, R. (2017) Potentials of Blockchain Technology for Construction Management. Procedia Engineering, Vol. 196, pp. 638-645.

Thomas, N. (2009) Cyber Security in East Asia: Governing Anarchy, Asian Security, Vol. 5, pp. 3-23.

UN (2014a) 2014 Revision of the World Urbanization Prospects. Available via: https://goo.gl/xwOSDS [Accessed: February 2018].

UN (2014b) World Urbanization Trends 2014: Key Facts. Statistical Papers - United Nations (Ser. A), Population and Vital Statistics Report. United Nations.

UN (2015) World Population Projected to Reach 9.7 Billion by 2050. Available via: http://www.un.org/en/development/desa/news/population/2015-report.html [Accessed: February, 2018].

Walsham, G. (1995) The Emergence of Interpretivism in IS Research, Information Systems Research, Vol. 6, No. 4, pp. 376-394.

Wang, S., Zhang, G., Shen, B. and Xie, X. (2011). An Integrated Scheme for Cyber-physical Building Energy Management System. Procedia Engineering, Vol. 15, pp. 3616-3620.

Wang, W. and Lu, Z. (2013) Cyber Security in the Smart Grid: Survey and Challenges. Computer Networks, Vol. 57, pp. 1344-1371.

Weber, R. H. and Studer, E. (2016) Cybersecurity in the Internet of Things: Legal Aspects. Computer Law & Security Review, Vol. 32, pp. 715-728.

Xue, N., Huang, X. and Zhang, J. (2016) S2Net: A Security Framework for Software Defined Intelligent Building Networks. 2016 IEEE Trustcom/BigDataSE/ISPA, 23-26 Aug. 2016 2016. pp. 654-661.

Yue, X., Wang, H., Jin, D., Li M., Jiang W. (2016) Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control, Journal of Medical Systems, Vol. 40, No. 10, p. 218.

Zhang Y. and Wen J. (2016) The IoT Electric Business Model: Using Blockchain Technology for IoT, Peer-to-Peer Networking and Applications, Vol. 10, No. 4, pp. 1-12.

Zamparini, L. and Shiftan, Y. (2013) Special Issue - Transport Security: Theoretical Frameworks and Empirical Applications, Transport Policy, Vol. 28, pp. 61-62.

Table 1 - Emerging Thematic Groups in Extant Literature

Industrial Sector	Author(s)	Journal	Thematic group: National and Global Security	Smart Cities	Critical Infrastructure	Industrial Control Systems	Mobile or Cloud Computing	Digitalisation of built Environment
Percentage Frequency Across the Four Journal Types			54.7%	40.4%	50%	40.4%	59.5%	28.5%
Architecture, Engineering, Construction and Owner-operated (AECO)	Chong *et al.*, 2014	Automation in Construction		✓			✓	✓
	Howell *et al.*, 2017	Automation in Construction		✓	✓	✓	✓	
	Kochovski *et al.*, 2016	Automation in Construction		✓			✓	✓
	Fisk, 2012	Intelligent Buildings International		✓				
	Mike, 2006	Journal of Facilities Management				✓	✓	✓
	Eom and Paek, 2006	Journal of Information Technology in Construction (ITcon)					✓	✓
	Jaatun *et al.*, 2014	Procedia Engineering	✓		✓	✓	✓	
	Koo *et al*, 2014	Procedia Engineering	✓		✓	✓	✓	
	Nicał and Wodyński, 2016	Procedia Engineering					✓	✓
	Wang *et al.*, 2011	Procedia Engineering				✓	✓	✓
Percentage Frequency in AECO Journals			20%	40%	30%	50%	90%	60%
Transport and Infrastructure	Patel *et al.*, 2009	Communications of the ACM			✓	✓	✓	
	Wang and Lu, 2013	Computer Networks	✓	✓	✓		✓	
	Liu *et al.*, 2012	IEEE, Communications Surveys & Tutorials	✓	✓	✓			
	Jones, 2016	IEEE, Engineering & Technology	✓	✓	✓		✓	✓
	Paridari, *et al.*, 2016	IEEE, International Conference on Cyber-Physical Systems (ICCPS)		✓		✓	✓	✓
	Ryan, 2016	International Journal of Critical Infrastructure Protection	✓	✓	✓			
	Papa, 2013	Transport Policy	✓		✓			
	Reggiani, 2013	Transport Policy			✓			
	Reniers and Dullaert, 2013	Transport Policy		✓		✓		
	Szyliowicz, 2013	Transport Policy	✓		✓			
	Zamparini and Shiftan, 2013	Transport Policy			✓			
Percentage Frequency in Transport and Infrastructure Journals			54.5%	54.5%	81.8%	27.2%	36.3%	18.1%

Table 1 conti… - Emerging Thematic Groups in Extant Literature

			Thematic group					
Industrial Sector	**Author(s)**	**Journal**	National and Global Security	Smart Cities	Critical Infrastructure	Industrial Control Systems	Mobile or Cloud Computing	Digitalisation of built Environment
Information Technology	Hunton, 2012	Computer Law & Security Review	✓		✓		✓	
	Weber and Studer, 2016	Computer Law & Security Review	✓	✓	✓		✓	
	Metke and Ekl, 2010	IEEE Transactions on Smart Grid		✓	✓			
	Tan *et al.*, 2018	IEEE Transactions on Smart Grid	✓		✓		✓	
	Xue *et al.*, 2016	IEEE Trustcom/BigDataSE/ISPA		✓	✓		✓	✓
	Ani *et al.*, 2016	Journal of Cyber Security Technology		✓	✓	✓	✓	✓
	Govinda, 2015	Procedia Technology		✓	✓		✓	✓
	Rasmi and Jantan, 2013	Procedia Technology	✓				✓	
	Safavi *et al.*, 2013	Procedia Technology					✓	
	Shitharth and Winston, 2015	Procedia Technology		✓	✓	✓	✓	
Percentage Frequency in Information Technology Journals			40%	60%	80%	20%	90%	30%
Political Science/ International Relations	Brantly, 2014	Democracy and Security	✓			✓	✓	
	Kello, 2013	International Security	✓					
	Lindsay, 2015	International Security	✓	✓		✓	✓	✓
	Nye, 2017	International Security	✓			✓	✓	
	Cavelty, 2013	International Studies Review	✓					
	Canfil, 2016	Journal of International Affairs	✓					
	Hjortdal, 2011	Journal of Strategic Security	✓			✓		
	McGraw, 2013	Journal of Strategic Studies	✓			✓		
	Stoddart, 2016	Political Science Quarterly	✓			✓		
	Betz and Stevens, 2013	Security Dialogue	✓		✓	✓		
	Lindsay, 2013	Security Studies	✓		✓			
Percentage Frequency in Political Science/ International Relations Journals			100%	9%	18.2%	63.6%	27.2%	9%

Table 2 – Industry Standards and Codes of Best Practice on Cyber Security in the AECO Sector.

Standard	Title	Description
BS ISO/IEC 29100:2011 (ISO,2011)	Information Technology. Security Techniques. Privacy Framework	This standard is applicable to organizations and businesses, providing a privacy framework for those "*involved in specifying, procuring, architecting, designing, developing, testing, maintaining, administering, and operating information and communication technology systems or services*" with personally identifiable information (PII).
BS ISO/IEC 27001:2013 (ISO, 2013)	Information Technology. Security Techniques. Information Security Management Systems. Requirements	This international standard provides a framework for the management of an information security management system (ISMS) in order to keep digital information assets secure from cyber-criminal activities and information breaches; it encompasses procedures for creating, implementing, operating, auditing and maintaining an ISMS. The standard can be applied within organizations of any size, nature or type.
IET/CPNI Techical Briefing (IET, 2013)	Resilience and Cyber Security of Technology in the Built Environment	This document applies to professionals involved in the development, procurement and operation of intelligent or smart buildings. The guidance considers the whole building lifecycle and examines the potential threats to resilience and cyber security arising from the merging of technical infrastructure and computer-based systems and their connection in cyberspace. Case studies are provided plus a set of 20 critical measures which could be applied to reduce threats.
PAS 555:2013 (BSI, 2013)	Cyber Security Risk. Governance and Management. Specification	The specification uses a business-led, "*outcomes-based approach*" which studies physical, cultural and behavioral features alongside technical ones, to aid organizations in detecting which of their business assets need most protection, e.g. corporate and customer data, intellectual property, brand or reputation. The approach can be applied to any size / type of organization, throughout its business activities.
PAS 754:2014 (BSI, 2014c)	Software Trustworthiness. Governance and Management. Specification	This document identifies five principles of software trustworthiness (safety, reliability, availability, resilience and security) which should be attained when implementing software on distributed applications in order to reduce the risks from potential malicious threats. These principles are based upon four concepts: governance measures; risk assessment; control application for risk management (physical, procedural and technical) and a compliance regime to ensure execution of the first three.
IET Standards (IET, 2014)	Code of Practice for Cyber Security in the Built Environment	This book provides good practice guidance on the need for, and development of, cyber security strategy and policy related to a building's complete lifecycle as an integral part of an organization's management systems, with particular emphasis on cyber physically connected building-related systems. The pertinence of cyber security to each of the multidisciplinary roles and responsibilities within an organization is provided.
PAS 1192-5:2015 (BSI, 2015)	Specification for Security-minded Building Information Modelling, Digital Built Environments and Smart Asset Management	This is the first standard published for security minded use of BIM and digitalization of built assets. Relevant to all owners and stakeholders of digitally built assets, it assists in assessing security risks to the asset and implementing measures to reduce the risk of loss or disclosure of information which could impact on the safety and security of: the built asset; personnel and other users of the asset and its services; and commercial and other asset data and information.

Table 3 - Common Reconnaissance Techniques

	Reconnaissance Technique		Definition	Example
	Scanning	**Ping sweep** **Port scan** **Network Mapping**	Network scanning is integral to stealthy information gathering from a computer system. Prior knowledge of the operating system (OS) is combined with the use of one of a plethora of readily available tools, in order to identify and map out potential vulnerabilities on a target network.	Techniques include: port scanning to identify the available and open ports, DNS enumeration to locate the domain name server and IP address, and PING sweeping to map the IP address to a live host (Rittinghouse and Hancock, 2003).
	Fingerprinting (OS)		Device fingerprinting endeavors to break the privacy of URL developers by revealing user actions and anonymity. It utilizes the information collected from a remote computing device for the purpose of uniquely identifying the device (Formby *et al.*, 2016). Fingerprinting can be used to identify the OS used on the target system.	In an active manner to monitor network packets passing between hosts, or passive manner to transmit specially created packets to the target machine and analyze the response (Peng *et al.*, 2015).
	Footprinting		Footprinting is a process of obtaining as much information about the target to be hacked as possible by drawing down open source information from the internet. Footprinting is the most convenient way of gathering information about a computer system and/ or parties such belong to.	During footprinting a hacker can use passive or active means to obtain information such as: domain name; IP addresses; namespaces; employee information; phone numbers; e-mails; and job information.
	Sniffing		Sniffing has been likened to wiretapping and can be used to obtain sensitive information that is being transferred over a network, such as: FTP passwords; email traffic; web traffic; telnet passwords; router configurations; chat sessions; and DNS traffic. "Industrial Control Systems (ICS)/ Supervisory Control and Data Acquisition (SCADA) sniffing" activities pose an imminent threat to cyber-physical connected devices in buildings, factories and large industrial plants.	'Havex' Malware reported, by F-Secure laboratories, is the first of its kind since STUXNET and attempts to 'sniff' factory automation gear such as ICS and SCADA systems (F-Secure Labs, 2014). Anonymized victims have included: two major educational institutions in France; two German industrial machine producers; one French industrial machine producer; and a Russian structural engineering construction company (*ibid.*)
	Social Engineering		Social engineering is an attack vector that relies upon tricking people into breaking security procedures. Consequently, these are used to exploit an individual's weaknesses, typically employees and other individuals who are familiar with the system. When successfully implemented, hackers can help obtain information about the targeted system.	Two common methods adopted are the physical gaining of access to a computer through deception or the use of phishing emails, which involves sending personalized emails to targeted employees in an attempt to make them click malicious links contained within.

Table 4 - Snapshot of Cyber-physical Hacking Examples from the RISI Online Incident Database [available online at http://www.risidata.com/]

Motivation	Actor	Example
Black Hat	Hacktivists	**USA, 2014 - Power and utilities -** Hackers took advantage of a weak password vulnerability where mechanical devices were disconnected from the control system for scheduled maintenance.
	Script kiddies	**Poland, 2008 - Transport -** A 14-year old Polish student hacked into the tram system, enabling him to change track points in Lodz. Four trams were derailed and as a consequence twelve people were injured.
Ego, personal animosity, economic gain.	Cyber insiders	**USA, 2001- Petroleum -** The network monitoring personal computer (PC) provided a path from the internet, via the company business network, onto the automation network. This made the company vulnerable to the Code Red Worm, used to deface the automation web pages of a large oil company
	Cyber terrorists	**Spain, 2011- Traffic** - Spanair flight 5022 crashed just after take-off from Madrid-Brajas International Airport killing 154 with 18 survivors. Trojan malware detected on the central computer system is speculated to have played a role in the crash by causing the computer to fail to deliver power to the take-off early warning system and detect three technical problems with the aircraft.
	Malware authors	**Iran, 2012 - Petroleum -** Iran was forced to disconnect key oil facilities after suffering a malware attack which it is believed hit the internal computer systems at Iran's oil ministry and its national oil company.
	Organized cyber criminals	**USA and Europe, 2014 - Energy sector** – Operating since 2011, the Dragonfly group has targeted defence and aviation companies in U.S. and Canada cyber-espionage with the likely intention of sabotage. In 2013, the group targeted U.S. and European energy firms, gaining entry through: spear phishing emails, malware, watering hole attacks and infecting legitimate software from three different industrial control systems (ICS) equipment manufacturers.
	Patriot hackers	**Canada, 2012 - Energy sector -** Telvent Canada Ltd., provider of software and services for remote administration of large sections of the energy industry, was subject to information theft. Installed malware was used to steal project files related to one of its key products. The digital fingerprints were traced to a Chinese hacking group (the "Comment Group"), linked to cyber-espionage against Western interests .
	Cyber militias	**Iran, 2010 - Nuclear** –The Stuxnet malworm was responsible for damaging crucial centrifugal devices used for Uranium enrichment at the Natanz nuclear plant causing it to be shut down for week. This remains as one of the most profilic cyber-physical attacks in an exemplified case of government and civilian blurred lines and created a new forefront of cyber militia, becoming the first proclaimed cyber weapon.
Grey Hat	Script kiddies	**USA, 2012 - Water/waste management** – A former employee of the Key Largo Wastewater Treatment District hacked the company resulting in modification and deletion of files.
Ambiguous	Ordinary citizens	**Venezuela, 2002 –Petroleum -** Venezuela's state oil company became embroiled in a bitter strike when it was extensively sabotaged by an employee who gained remote access to a program terminal and erased all Programmable Logic Controller (PLC) programs in port facility.
White Hat	Hacktivists	**Canada, 2002 - Petroleum-** A white hat hacker simulated an attack on a data center security (DCS), where network access to the control local area network (LAN) was used to connect to selected DCS operator stations and obtain full administration privileges. This was accomplished through the vulnerabilities in the Windows operating system and a number of Netbios that lacked proper password protection.
Idealism, creativity, respect for the law	Script kiddies	**USA, 2014 - Traffic -** One of the first hacks on a traffic management system was incurred on road signs in San Francisco, where the signs were photographed flashing "Godzilla Attack! Turn Back".

Figure 1 - Cyber Vulnerabilities of CDE Environment adapted from BSI Levels of BIM

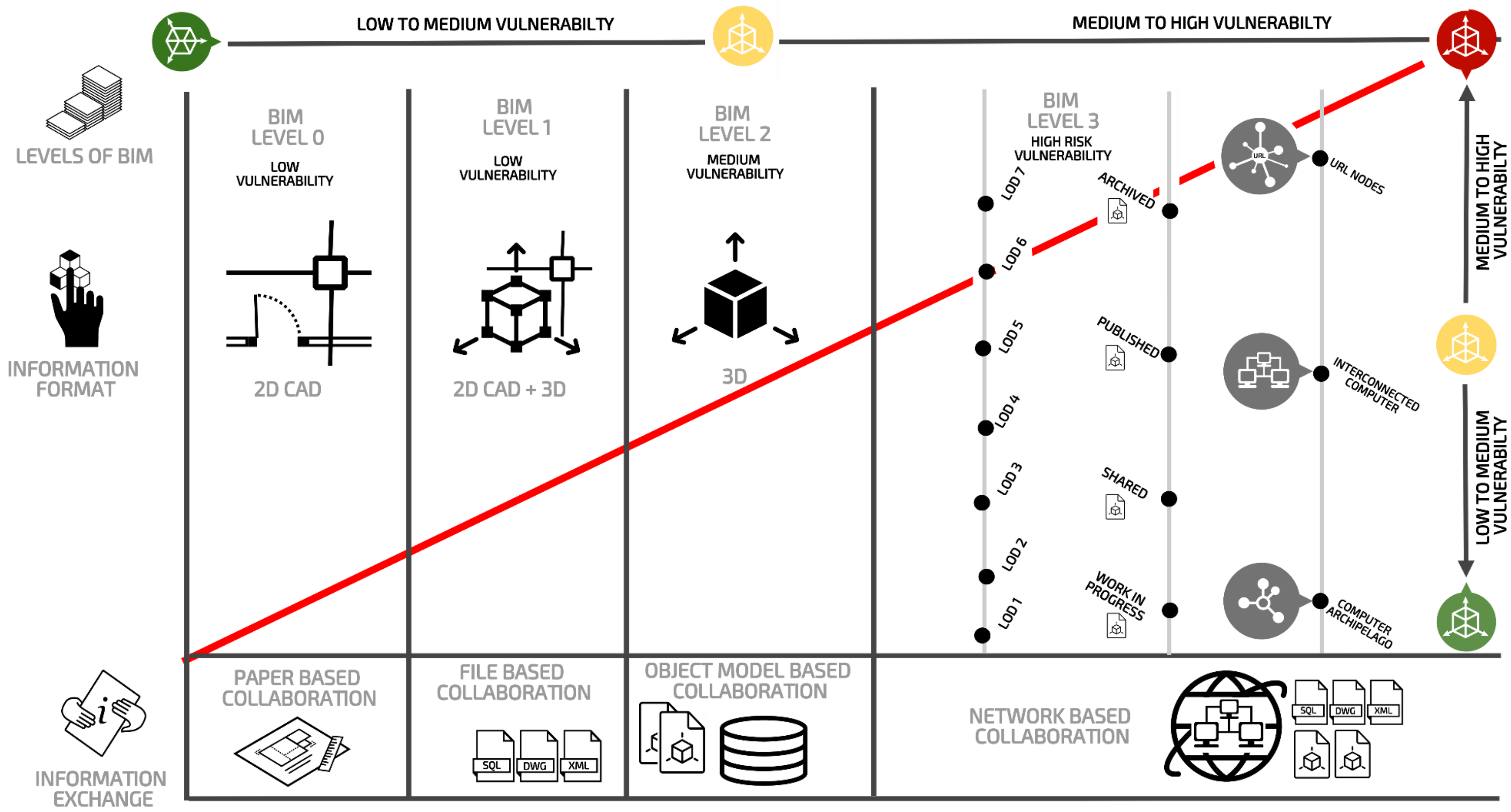

Figure 2 - Block Chain Technology Application with Digital Built Asset Information Exchange