applied sciences

Article

A Cyber-Physical Risk Assessment Approach for Internet of Things Enabled Transportation Infrastructure

Konstantinos Ntafloukas [1,*], Daniel P. McCrum [1] and Liliana Pasquale [2]

[1] School of Civil Engineering, University College of Dublin, D07 R2WY Dublin, Ireland
[2] School of Computer Science, University College of Dublin, D07 R2WY Dublin, Ireland
* Correspondence: konstantinos.ntafloukas@ucdconnect.ie

Featured Application: Cyber and physical security of transportation infrastructure.

Abstract: A critical transportation infrastructure integrated with the Internet of Things based wireless sensor network, operates as a cyber-physical system. However, the new form of IoT enabled transportation infrastructure is susceptible to cyber-physical attacks in the sensing area, due to inherent cyber vulnerabilities of IoT devices and deficient control barriers that could protect it. Traditional risk assessment processes, consider the physical and cyber space as isolated environments, resulting in IoT enabled transportation infrastructure not being assessed by stakeholders (i.e., operators, civil and security engineers) for cyber-physical attacks. In this paper, a new risk assessment approach for cyber-physical attacks against IoT based wireless sensor network is proposed. The approach relies on the identification and proposal of novel cyber-physical characteristics, in the aspect of threat source (e.g., motives), vulnerability (e.g., lack of authentication mechanisms) and types of physical impacts (e.g., casualties). Cyber-physical risk is computed as a product of the level and importance of these characteristics. Monte Carlo simulations and sensitivity analysis are performed to evaluate the results of an IoT enabled bridge subjected to cyber-physical attack scenarios. The results indicate that 76.6% of simulated cases have high-risk and control barriers operating in physical and cyber space can reduce the cyber-physical risk by 71.8%. Additionally, cyber-physical risk differentiates when the importance of the characteristics that are considered during risk assessment is overlooked. The approach is of interest to stakeholders who attempt to incorporate the cyber domain in risk assessment procedures of their system.

Keywords: IoT; transportation infrastructure; threat source; vulnerability; physical impact; cyber-physical risk; control barriers; Monte Carlo; sensitivity analysis

check for updates

Citation: Ntafloukas, K.; McCrum, D.P.; Pasquale, L. A Cyber-Physical Risk Assessment Approach for Internet of Things Enabled Transportation Infrastructure. *Appl. Sci.* **2022**, *12*, 9241. https://doi.org/10.3390/app12189241

Academic Editors: Leandros Maglaras, Helge Janicke and Mohamed Amine Ferrag

Received: 19 August 2022
Accepted: 11 September 2022
Published: 15 September 2022

1. Introduction

Until recently, critical infrastructure was considered to operate in an isolated cyber or physical environment. However, the increasing reliance of critical infrastructure on advanced technologies (e.g., Internet of Things (IoT)) has enabled the integration of the physical world with computational facilities and the operation of critical infrastructure as a cyber-physical system [1]. In the domain of critical transportation infrastructure, a significant number of IoT applications have been recently introduced, providing reliable services with less human intervention [2]. These services include, but are not limited to, early warning system against hazards (e.g., scour) [3], or a smart management system in a bridge life cycle assessment [4]. In the field of structural health monitoring and damage assessment, advancements of IoT technology have revealed the potential for several applications (e.g., monitoring through image processing) [5,6]. These IoT applications enhance the ability to automate processes, enabling civil engineering professionals to make well-informed decisions regarding the structural health statuses of their systems. Such IoT applications, could not be materialized without the use of IoT based wireless sensors network (WSN), as a key technology that enables the connection with the physical environment within their layered architecture [7]. The fundamental three-layer IoT architecture includes the sensing, network, and application layer, each one defined by its functions and the devices that are used in it [8]. Specifically, IoT devices (e.g., sensors, gateways) located in the physical space (e.g., deck of a bridge) as part of the sensing layer, collaboratively detect, collect, and process data. The network layer enables the wireless transmission of data, availing of recent advances in wireless network protocols (e.g., ZigBee, Bluetooth). This data is sent to the end-user for data analytics and processing, through the application layer. The convergence of traditional urban critical transportation infrastructure (i.e., bridge, roadways, highways, tunnels, embankments) with IoT applications, facilitates the transition to an IoT enabled transportation infrastructure, which serves as the intersection between the physical and cyber space. Although in the past cyber or physical attacks assumed to have an impact on either the cyber or physical space alone, now an exploitation of a cyber vulnerability (e.g., lack of authentication mechanisms) by a threat source (i.e., attacker) can result in physical impact(s) (e.g., economic losses), facilitating cyber-physical attacks against critical infrastructure [9]. The security breach of confidentiality, integrity, availability (CIA) can result in severe consequences [10]. Successful cyber-physical attacks against IT systems in the transportation domain exploited cyber vulnerabilities to cause severe physical impacts (e.g., injuries) [11]. In one of these attacks, the European Union Agency for Cybersecurity reported a two-days Denial of Services attack (DoS) against the Swedish Transport Administration, resulting in major delays and degraded services to customers [12].

Despite the promising IoT applications in the critical transportation infrastructure domain, IoT devices that comprise an IoT based WSN in the sensing layer, suffer from inherent technical weaknesses and vulnerabilities. Technical weaknesses refer to issues such as limited energy resources, low memory, and computational capacity of IoT devices, while vulnerabilities refer to security gaps that can be exploited by an attacker [13]. Vulnerabilities can originate from deficiencies in the wireless network protocol adopted in IoT devices [14–16]. As critical transportation infrastructure has been an appealing target for threat sources (e.g., terrorist) due the level of impact that can be obtained from its disruption, the application of an IoT based WSN in the sensing layer is increasing the risks of cyber-attacks [17]. Thus, the cyber-physical risk assessment of an IoT enabled transportation infrastructure against cyber-physical attacks in the sensing layer has become more crucial than ever.

Although approaches to assess the risks of transportation infrastructure against natural hazards (e.g., earthquake) have been proposed in previous work [18], those aimed to assess risks against cyber-physical attacks are limited. For example, an increased need for security awareness, has been outlined for railway systems [19]. However relevant studies, such as the EU projects PROTECTRAIL [20], SECRET [21], CARONTE [22], CIPSEC [23,24], target to inform stakeholders, about emerging security issues (e.g., access control, electromagnetic attacks etc.), rather than assessing the risk brought by the exploitation of vulnerabilities of IoT devices. Other approaches in the transportation domain (see Section 2 for more details), integrate cyber security international standards, mainly derived from the National Institute of Standards and Technology (NIST), such as NIST SP800-30 [25]. By considering a qualitative likelihood-impact matrix, based on organizational deficiencies (e.g., lack of employees training), stakeholders can assess risks and apply control measures strictly related to business organization assets (e.g., disclosure of sensitive data) and operations overlooking the impact to physical space. Additionally, despite the recent advances of machine learning methods (e.g., signature-based method) in the critical infrastructure domain these are mainly implemented for network anomaly detection as a second line of defence rather than the proactive management of risk [26], which is the main focus of this paper. Other limitations of machine learning methods include the possibility of adversarial machine learning (i.e., an attacker performs reverse engineering to avoid detection) [27] and the complexity of converging both cyber and physical detection methods [28], due to coexistence of a physical infrastructure that is enabled through operation in cyberspace.

The gradual transformation to an IoT enabled transportation infrastructure has created a knowledge gap, in cyber-physical risk assessment, leading to the consideration of cyber threats as separated from the physical ones [29]. This knowledge gap rises due to underreporting, that has led to a lack of statistical data about cyber-attacks [30]. Additionally, new threat sources based on complex human profile characteristics (e.g., motives), and vulnerabilities have arisen from cyber space [31]. The absence of unified risk assessment methodologies for critical infrastructure domains makes it more difficult to identify how cyber-physical risks can be managed [32].

To bridge this gap, this paper contributes by providing a cyber-physical risk assessment approach for IoT enabled transportation infrastructure subjected to cyber-physical attacks at the sensing area that can be applied by stakeholders who act as assessors (i.e., operators, civil and security engineers). The approach aims to enable stakeholders to manage the cyber-physical risk in the sensing area in a proactive manner. In our approach, cyber-physical risk is computed as the product of three main aspects: (i) the vulnerabilities of IoT devices; (ii) the threat source who can exploit the vulnerabilities; and (iii) the physical impact resulting from the successful exploitation of the vulnerabilities. Vulnerabilities and threats are assessed based on combined cyber and physical characteristics, while physical impacts are assessed considering previous related work in the security and civil engineering domain. Quantitative scores are employed to assess the level and importance of the cyber-physical characteristics. An illustrative, yet realistic, case study of an IoT enabled bridge, being subjected to cyber-physical attack (i.e., energy depletion attack) against its IoT based WSN is used to demonstrate the application and usefulness of the approach. The cyber-physical attack is composed of four scenarios, based on the application of different control barriers, which can prevent and detect cyber-physical attacks. Control barriers can operate in the cyber (e.g., intrusion detection systems) and physical space (e.g., motion detectors), separately or at the same time (i.e., integrated control barriers). Monte Carlo simulations are performed to vary the quantitative scores assigned to vulnerabilities, threat sources and physical impacts, and conduct a sensitivity analysis to illustrate the impact of the scores on the cyber-physical risk.

This paper contributes to existing knowledge in the following ways. First, cyber-physical characteristics, that have not been previously considered in the aspect of threat source profile (e.g., terrorism experience), all associated with an IoT enabled transportation infrastructure, are integrated in the cyber-physical risk assessment approach, minimizing the knowledge gap between civil and security engineering domain. Second, this paper describes and uses a realistic case study of a cyber-physical attack scenario that takes place in the sensing area of an IoT enabled transportation infrastructure. Third, the role of control barriers, which could be activated in the sensing layer, is introduced, and considered in the approach, to inform assessors towards the cyber-physical risk reduction. The remainder of the paper is as follows: Section 2 presents the related work; Section 3 describes the proposed cyber-physical risk assessment approach; Section 4 illustrates the case study and presents the results; Section 5 includes a description of the results and limitations of the approach; and Section 6 concludes the paper.

2. Related Work

A review of related work within the areas of security risk and critical infrastructure, mainly focusing on the transportation sector, is presented in this section. The related work is divided into two domains, namely, international standards or frameworks, used by organizations and research studies.

International Standards. International standards or frameworks exist in cyber domain and have been widely used in critical infrastructure risk domain, due to the increasing severity of cyberattacks. As mentioned in Section 1, NIST has released standards that assist organizations towards the cyber risk management such as the qualitative impact-likelihood matrix in NIST SP800-30 [25]. NIST's Cyber Security Framework for Critical Infrastructure [33], targets to assist stakeholders within critical infrastructure domain, into management of cybersecurity related risk and cyber resilience. It builds on three core structures, namely, framework core (i.e., discuss the management of cyber risk), implementation tiers (i.e., discuss the standards that more effectively suit organizations cybersecurity program), and framework profile (i.e., discuss identified opportunities for improving organizations cybersecurity). NIST standards are mainly applicable to manage risks arising from remote attacks (i.e., through the Internet) and insider attacks. Additionally, the standards provide guidance on how to protect valuable assets in cyber space (e.g., sensitive data) by performing activities at the level of an organization (e.g., employees training). Contrary to this, this approach presented in this paper rigorously focusses on cyber-attacks at the sensing area (i.e., sensing layer), which result in physical impacts (i.e., cyber-physical attacks) and emerge from the exposure of IoT devices at physical space. Furthermore, the discussed control barriers originate from the engineering domain (e.g., motion detectors) and aim to protect the IoT enabled transportation infrastructure. NIST 8228 internal report [34], aims to inform federal agencies and organizations on how to manage IoT cybersecurity and privacy risks. The report identifies high level considerations that may affect the management of cybersecurity and privacy risks for IoT devices (e.g., interaction with physical systems) as compared to conventional IT devices. Although the report provides valuable information about cyber security risks determined by the use of IoT devices, it does not provide a method to assess these risks. Common Vulnerability Scoring System (CVSS) [35], is an open framework that assists organizations to assess and prioritize their vulnerability management processes.. Although it focuses on measuring the severity of security vulnerabilities, it has been widely integrated in risk assessment procedures [36]. For example, the exploitability metrics of Base Score (e.g., Attack vector), which are considered in this approach, represent the intrinsic characteristics of a vulnerability that are constant over time and across user environments. The Base metric produces a score that ranges from zero to ten to measure the severity of vulnerability, based on human judgement. CVSS [35] is only applicable for measuring the severity of vulnerabilities, rather than assessing the risks that emerge from their exploitation.

Research Studies. Studies in the transportation sector have focused on security issues of advanced transportation elements (e.g., vehicles) that communicate wirelessly (i.e., vehicle-to-vehicle and vehicle-to-infrastructure communication), rather than considering harm that these elements can cause to the transportation infrastructure [37–39]. A risk assessment process for policymakers and engineers was presented by Kelarestaghi et al. [40], to raise security awareness of exploitable in-vehicle network security vulnerabilities. Due to the lack of statistical data in cyber-attacks, a qualitative impact-likelihood matrix, that follows the guidelines of NIST SP800-30 standards [25] was applied. The process synthesizes security incidents from the current literature and real-world cyber events, to visualize a risk matrix, related to safety, operation, reliability, and security issues that emerged from in-vehicle network security vulnerabilities. The maritime transportation sector includes crucial activities (export and import of goods) that face security threats. Gunes et al. [41] applied previously proposed cyber security risk assessment approaches (i.e., [42]) to a real case study of a container port. Stakeholders (e.g., port staff, IT managers) were actively involved in the approach by participating in interviews and questionnaires to assess cyber risk under different attack scenarios. Cyber risk was calculated as a summation of likelihood and impact, based on stakeholders' answers, while mitigation strategies (e.g., use of stronger passwords) were briefly discussed when risk values were not acceptable. ENISA released a report [43] to outline good practices for cybersecurity in the maritime sector, providing a list of security threats (e.g., social engineering) and measures (e.g., security awareness raising program) in relation to critical operations. Kandasamy et al. [44] highlight that existing cyber risk frameworks alone, are unable to address new threats that are arising in IoT-based systems. Indeed, current cybersecurity assessment methods alone cannot directly address the needs of IoT-based smart environments [45]. To address this gap, Stellios et al. [46] proposed an approach that enables decision makers in critical systems (e.g., healthcare sector), to identify and assess cyber-physical attack paths, rather than the risks that emerge from them, due to the existence of IoT devices. The method, which was tested in the healthcare sector, relies on qualitative and quantitative scales and builds on attack trees topologies [47], a recursive algorithm and exploitability metrics of CVSS [35]. The enablement of cyber-physical attack paths due to the existence of IoT devices was highlighted by Agadakos et al. [48]. They proposed an approach to identify unexpected chains of events and subsequent potential impacts due to addition or removal of a device to/from an existing network, mainly applicable for industrial IoT applications (i.e., smart homes). The application of the approach was demonstrated, using a language and tool for relational models (i.e., Alloy [49]) in realistic IoT use cases (i.e., smart home devices).

Although research studies succeed in raising security awareness in the transportation sector, they have certain limitations. Firstly, they focus on the protection of interactive transportation elements (i.e., vehicles) from cyber-attacks, rather than the critical transportation infrastructure itself [40]. Existing research studies have not considered cyber-attacks that take place in the sensing area of a critical transportation infrastructure and impact physical space, but rather focus on remote cyber-attacks. Additionally, studies that ground their risk calculation on attacker profiles have only considered a limited number of profile characteristics. For example, in [41,46] only a limited numbers of profile characteristics (e.g., skills of an attacker) were considered to calculate the likelihood of an attack. However, as critical transportation infrastructure can also be the target of terrorist activities, other characteristics should also be considered. For example, attacker motives (e.g., ideology, political) could substantially affect the targets of an attack and the effort that the attacker will put to achieve their objectives. In the approach presented in this paper, a detailed attacker (also referred to as threat source) profile is considered based on the literature (i.e., latent content analysis) and the cyber-physical perspective of an IoT enabled transportation infrastructure. Finally, in comparison with previous studies that treat all threat source profile characteristic equally, we weigh the characteristics using importance indexes determined using expert judgement.

3. Cyber-Physical Risk Assessment Approach

Due to the complex nature of critical infrastructure domain, risk assessment methods should be adapted to each sector (e.g., maritime, transportation) individually [41]. Thus, the cyber-physical risk assessment approach presented in this paper focuses on critical transportation infrastructure and can be performed by stakeholders who act as assessors (i.e., operators, security, and civil engineers). Similarly to existing risk assessment methods, this approach is based on the identification and assessment of vulnerability, threat, and impact [50]. As shown in Figure 1, this approach incudes six activities.

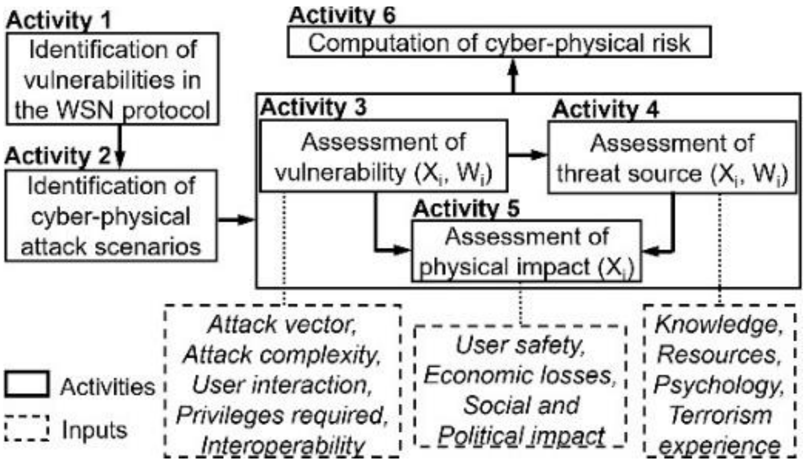
Activity 1
Identification of vulnerabilities in the WSN protocol
Activity 2
Identification of cyber-physical attack scenarios
Activity 6
Computation of cyber-physical risk
Activity 3
Assessment of vulnerability (X_i, W_i)
Activity 4
Assessment of threat source (X_i, W_i)
Activity 5
Assessment of physical impact (X_i)
Attack vector, Attack complexity, User interaction, Privileges required, Interoperability
User safety, Economic losses, Social and Political impact
Knowledge, Resources, Psychology, Terrorism experience
Activities
Inputs

Figure 1. Overview of cyber-physical risk assessment approach.

The first activity, as shown in Figure 1 (*Identification of vulnerabilities in the wireless sensor network protocol*), includes the identification of vulnerabilities that are present in the wireless network protocol used by the IoT devices to communicate. This activity can be facilitated by the use of public vulnerability databases (e.g., Common Vulnerabilities and Exposures [51]) as well as research [52] and experimental studies [53]. The identified vulnerabilities are used in the second activity to identify potential cyber-physical attack scenarios (*Identification of cyber-physical attack scenarios*), that enable their exploitation. Identification of cyber-physical attack scenarios necessitates the role of stakeholders who have bespoke knowledge of their system [42]. Indeed, the preparation of cyber-physical attack scenarios requires the consideration of weaknesses not only in cyber space but also in the physical space (e.g., deficient physical protection). The main attack scenarios against IoT devices (e.g., battery drainage, eavesdropping etc) that can be used in this approach, have been discussed in detail in the literature [54]. The second activity (refer to Figure 1) can be further facilitated with the use of publicly available catalogues of common attack patterns (e.g., CAPEC [55]) that describes how specific parts of an attack are designed and executed based on real world examples, as well as experimental studies [56].

Cyber-physical attack scenarios identify how vulnerability in the IoT network can be exploited by a threat source to damage physical space. The third, fourth and fifth activities revolve on the assessment of the vulnerabilities that can be exploited in a cyber-physical attack scenario, the threat source who attempts to exploit them, and the adversarial physical impact that can be caused by the successful exploitation of vulnerability. As shown in Table 1, the assessment of vulnerabilities and threat source requires assessors to assign a numerical score: (i) in the decision scale (X_i), that describes the level of their characteristics with respect to the considered IoT based WSN; and (ii) in the importance index (W_i), that describe the importance of their characteristics with respect to their effect on the completion of cyber-physical attack scenario. More precisely, in Activity 3 assessors define the level of vulnerability characteristics and their importance: *Attack vector* (X_{AV}, W_{AV}), *Attack complexity* (X_{AC}, W_{AC}), *User interaction* (X_{UI}, W_{UI}), *Privileges required* (X_{PR}, W_{PR}), and *Interoperability* (X_{IO}, W_{IO}). These characteristics are similar to those considered in CVSS [35]. The overall assessment of vulnerability is computed as the weighted average of the level of vulnerability characteristics. In Activity 4 assessors define the level of threat source characteristics and their importance: *Knowledge* (X_{KN}, W_{KN}), *Resources* (X_{RE}, W_{RE}), *Psychology* (X_{PS}, W_{PS}), *and Terrorism experience* (X_{Te}, W_{Te}). These characteristics reflect the potential of a threat source to exploit the vulnerabilities considered in the cyber-physical attack scenarios generated in Activity 2. The overall assessment of a threat source is computed as the weighted average of the level of threat source characteristics. In Activity 5 the types of physical impact (X_{PI}) are assessed: *User safety, Economic losses, Social and Political impact*, which can arise from the attack scenarios generated in Activity 2. Assessment of physical impact can be accomplished by considering each type of physical impact individually, resulting in a different risk level for each type of physical impact. Alternatively, physical impacts can be assessed jointly, for example, when a successful attack scenario can lead to both casualties and economic losses [32]. Activity 4 depends on the outcome of Activity 3. For example, if the exploitation of a cyber vulnerability has high attack complexity (X_{AC}) then the importance of the knowledge of the threat source (W_{KN}) should also be high. Activity 5 also depends on the outcomes of Activities 3–4. For example, if a vulnerability has a higher attack vector and it is exploited by a threat source that has high knowledge (X_{KN}) and terrorism experience (X_{Te}), it can potentially lead to a high physical impact (X_{PI}).

Table 1. Levels and scores of decision scale and importance index.

Level	Decision Scale Scores, X_i	Importance Index Scores, W_i
Very Low	0–1	0–0.20
Low	2–4	0.21–0.40
Medium	5–7	0.41–0.60
High	8–9	0.61–0.80
Very High	10	0.81–1.0

In Activity 6 assessors compute the cyber-physical risk following Equation (1), based on the outcomes of Activities 3–5. The cyber-physical risk is computed as the product of the overall assessment of vulnerability, threat source and impact. The numerical result of Equation (1) allows identifying a corresponding risk level as shown in Table 2.

Table 2. Cyber-physical risk levels.

Cyber-Physical Risk Level	Quantitative Ranges	Description
High	344–1000	Failure of IoT enabled transportation infrastructure. Control barriers need to be enabled immediately.
Medium	65–343	Partial operation of IoT enabled transportation infrastructure. Control barriers need to be enabled as soon as possible.
Low	0–64	Operation of IoT enabled transportation infrastructure will continue. Control barriers to be determined as proactive measures.

The use of different ranges of levels and scores enables a qualitative (i.e., Low) and quantitative (i.e., 0–1) guide for stakeholders to aid the computation of risk, following the structure of NIST SP800-30 [25], which has been widely used by security engineers.

$$\begin{aligned} \text{Risk} = {} & \frac{W_{AV}\times X_{AV}+W_{AC}\times X_{AC}+W_{UI}\times X_{UI}+W_{PR}\times X_{PR}+W_{IO}\times X_{IO}}{W_{AV}+W_{AC}+W_{UI}+W_{PR}+W_{IO}} \\ & \times \frac{W_{KN}\times X_{KN}+W_{RE}\times X_{RE}+W_{PS}\times X_{PS}+W_{Te}\times X_{Te}}{W_{KN}+W_{RE}+W_{PS}+W_{Te}} \times X_{PI} \end{aligned} \tag{1}$$

The symbols of X_i, W_i in Equation (1), indicate the level and the importance of *Attack vector* (X_{AV}, W_{AV}), *Attack complexity* (X_{AC}, W_{AC}), *User interaction* (X_{UI}, W_{UI}), *Privileges required* (X_{PR}, W_{PR}), *Interoperability* (X_{IO}, W_{IO}), *Knowledge* (X_{KN}, W_{KN}), *Resources* (X_{RE}, W_{RE}), *Psychology* (X_{PS}, W_{PS}), *and Terrorism experience* (X_{Te}, W_{Te}) and type of physical impact (X_{PI}). In order to expand the established calculation of risk from the assessment of generic terms such as vulnerability, threat source and impact [50], Equation (1) was developed. This equation includes the assessment of particular characteristics in vulnerability, threat source and impact that assist stakeholders to achieve a more detailed and realistic risk computation. Risk assessment approaches suggest that risk levels have to be determined prior to the risk assessment based on stakeholders needs [41]. As indicated by NIST SP800-30 [25], the determined risk levels can be used as a starting point with appropriate tailoring to adjust for any specific conditions. Specifically, it divides the risk scales (i.e., Low, Medium etc.) based on the product of the individual levels of likelihood and impact. For example, a Low risk level is a product of a Low level likelihood and impact. Appropriate control barriers should be implemented depending on the level of cyber-physical risk [42]. Therefore, for the purpose of this paper, the following cyber-physical risk levels have been determined, based on NIST SP800-30 guidelines, as described in Table 2, namely Low (0–64) when the overall assessment of vulnerability, threat source and physical impact does not exceed 4, High (344–1000) when the overall assessment of vulnerability, threat source and physical impact is at least equal to 7 and Medium (65–343), otherwise.

3.1. Vulnerability Characteristics

The vulnerability characteristics that are considered in this approach are based on the exploitability metrics of CVSS 3.1 framework [35] and the access points brought by different IoT devices [57,58]. The vulnerability characteristics are namely *Attack vector, Attack complexity, User interaction Privileges required* and *Interoperability. Attack vector* describes the context in terms of level of access, by which vulnerability exploitation is possible (i.e., Network, Adjacent, Local, Physical). Differently from CVSS where the more remote the attacker (i.e., Network) the greater the vulnerability metric, this is not always the case for an IoT based WSN. The exposure of IoT devices to physical space (i.e., sensing layer) offer the opportunity to a threat source to exploit vulnerabilities in the WSN protocol, that can be accomplished by gaining physical access or through local network of the IoT based WSN [59]. Thus, X_{AV}, should be assigned a High or a Very high level not only when a vulnerability can be exploited remotely, but also when the conditions of IoT based WSN (e.g., absence of physical control barriers) facilitates the required access. X_{AV} should be determined case by case, depending on the cyber-physical attack scenario. *Attack complexity* reflects how many steps a threat source should perform to exploit the vulnerability, which can depend on the presence of advanced control barriers. Attacks with low complexity should be reflected in a greater X_{AC}, while attacks having high complexity should result in a lower X_{AC}. *User interaction* describes whether a user other than the threat source is required (i.e., the more interaction required, the lower X_{UI}) to exploit the vulnerability, such as an administrator who clicks a specially crafted link provided by the attacker and discloses sensitive information (e.g., WSN encryption password). *Privileges required* describes the level of privileges (i.e., No privileges, Low or High) the threat source should have before being able to exploit the vulnerability successfully. If the exploitation requires no or low privileges (i.e., vulnerability can be exploited by unauthorized attacker) then the level of X_{PR} will be high or very high. As outlined by Nawaratne et al. [60] and Desai et al. [58], *Interoperability* in IoT environments is a key characteristic of IoT technology. It describes the ability of an IoT system to effectively communicate with other IoT systems. An IoT enabled transportation infrastructure has a high level of *Interoperability* when it is connected with other heterogenous IoT devices. Interoperability can increase the access points to IoT devices and can be seen as a more appealing target for a threat source who seeks for extended disruption to more than one IoT system. For example, IoT devices of two IoT applications can operate in the same IoT based WSN providing different services (e.g., traffic and structural integrity monitoring) and share data between them. Thus, assessors should assign a high or very high level to X_{IO} when the IoT WSN has high *Interoperability*.

3.2. Threat Source Characteristics

The threat source characteristics that are considered in this approach are based on attacker's attributes proposed in the literature and by considering that an IoT based WSN operates in both cyber and physical space. The broader lack of access to organizational information related to cyber-attacks, has led to the adoption of a generic threat source description that cannot sufficiently describe an attacker profile and affect risk assessment [61]. The lack of detailed characteristics and knowledge gap with respect to the threat source profile has been highlighted by Rocchetto et al. [62]. Therefore, a latent content analysis of the existing literature was performed in this paper to identify the fundamental characteristics of threat sources. The identified characteristics are mainly based on the outcomes of the detailed research by Rocchetto et al. [62], which describes a set of attacker profiles based on different dimensions, namely *Knowledge*, *Resources* and *Psychology*. *Knowledge* describes the level of expertise, related to cyber skills (e.g., attack methods, attack patterns) and of understanding of the exploitable vulnerability that is under attack. The more complex the exploitation of a vulnerability, the more expertise the threat source needs to have, thus W_{KN} should be greater. The higher the level of *Knowledge* determined by the assessors, the greater the level of X_{KN}. *Resources* describe the level of: (i) manpower, indicating whether the threat source acts alone, in small or larger groups; (ii) tools/ability, indicating whether the threat source has access to the means necessary for the attack; and (iii) financial support, indicating the budget available to the threat source. A cyber-physical attack scenario that requires access to manpower, tools and financial support should be assigned a high importance index (W_{RE}). Assessors should determine at what level a threat source has manpower, tools/ability and financial support to assign a level to X_{RE}. *Psychology* describes the motivation of the threat source. Motivation indicates the motives (e.g., ideology, religious) that drive the threat source to accomplish their goal and affect the effort put in the performed attack. A cyber-physical attack scenario that requires strong motives and effort to be accomplished, should be assigned a greater W_{PS} importance index. Assessors should determine the level motivation of the threat source to assign a score to $X_{PS.}$

However, all the aforementioned characteristics described originate from cyber-attacks. In this risk assessment approach, *Terrorism experience* originating from the physical space is also considered. This characteristic has not been considered in previous work. Critical transportation infrastructure has always been an appealing target due its value to terrorist organizations [63]. However, a significant number of remote cyber-attacks have been conducted against critical infrastructure by terrorist organizations, indicating an expansion of malicious activities to cyber space [64,65]. The exposure of IoT devices in the sensing area of an IoT enabled transportation infrastructure will offer them new opportunities to impact the physical space by exploiting cyber vulnerability (i.e., cyber-physical attack). Terrorism experience refers to the experience of threat source to remain undetected in public secured areas (e.g., where the IoT based WSN is located) and the ability of the threat source to access valuable information (e.g., sensitive national data) to detect critical targets related to highly exploitable vulnerabilities that can harm the physical transportation infrastructure. A level should be assigned to X_{Te} by the assessors depending on these aforementioned characteristics. The value of W_{Te} will be high or very high if performing a cyber-physical attack requires the ability of the threat source to detect critical targets and remain undetected during the infiltration to a physical area.

3.3. Types of Physical Impact

Physical impacts caused by disruption of a critical infrastructure are hard to quantify due to their inherent unmeasurable nature (e.g., social impact) and to different terminologies, in terms of risk, used by critical infrastructure stakeholders [32]. The problem is amplified when security issues of data breach and their impacts are considered, which are mainly based on economic losses [66,67]. However, a disruption of an IoT enabled transportation infrastructure due to vulnerability exploitation, will result in identical types of physical impacts as for a critical transportation infrastructure due to natural hazards or man-made attacks. Therefore, the following types of physical impact are considered: *User safety*, *Economic losses*, *Social and political impact* as suggested by risk assessment policies within EU member states [32], individual national risk guidelines [68] and physical impacts from previous cyber events (e.g., casualties, economic losses) [11,12]. *User safety* describes the number of casualties. Assessors should consider the occupancy capacity of their transportation infrastructure during the cyber-physical attack scenario. *Economic losses* (monetary loss) describe the economic losses. Assessors should consider direct and indirect losses coming from the construction and repair/replacement costs of IoT application, disruption of primary services for hours or days, and due to business disruption. *Social and political impact* describes the number of people affected by the cyber-physical attack, due to violation of public security, sense of fear and outrage within people, unstable environment etc. The assessment of physical impact (X_{PI}) should be accomplished based on the sets of criteria established by stakeholders [68]. For the purposes of this approach, Table 3 presents the criteria, according to which physical impacts can be assessed following the suggestions of Canadian risk guidelines applicable for Critical Infrastructure Protection and Emergency Preparedness [69].

Table 3. Types of physical impacts (adapted to this study from [69]).

Type of Impacts Level/Score (X_{PI})	User Safety	Economic Losses	Social and Political Impact
Very Low/ 0–1	Slight injuries	No losses	No impact
Low/ 2–4	Less than 100 people	Under $10 million, Closure for hours	Public perceives low impact

Table 3. *Cont.*

Type of Impacts Level/Score (X_{PI})	User Safety	Economic Losses	Social and Political Impact
Medium/ 5–7	Between 100 and 1000 people	Between $10 to $100 million, Closure for days, weeks	Public perceives moderate impact
High/ 8–9	Between 1000 and 10,000	Between $100 million to $1 billion, Closure for months	Public perceives high national risk
Very High/ 10	More than 10,000 people	More than $1 billion, Closure for more than a year	Public perceives very high national risk

The criteria, according to which physical impacts can be assessed, as shown in Table 3, can be modified according to the guidelines of individual national risk guidelines, as adapted in this study following the suggestions of Canadian risk guidelines applicable for Critical Infrastructure Protection and Emergency Preparedness [69].

4. Case Study of an IoT Enabled Bridge

An illustrative and realistic case study of an IoT enabled bridge with wireless structural monitoring capabilities is presented in this section, as shown in Figure 2. The IoT enabled bridge is deployed into three layers. The sensing layer includes the IoT based WSN, which comprises IoT devices responsible for collecting and transmitting sensed data. Zigbee is a wireless technology used as a communication protocol among the IoT devices. It is based on the based on IEEE 802.15.4 standard [52,53] and has been demonstrated to be a reliable technology for monitoring purposes in civil engineering infrastructure [70]. Indeed, previous experimental studies [43,44,71,72], have successfully instrumented a wireless monitoring system for bridges, demonstrating the capabilities of ZigBee technology. ZigBee protocol stack includes the following layers: application (i.e., data transmission and security services); network (i.e., routing, security, and configuration of new devices); MAC (i.e., interface between physical and network layer); and physical (i.e., functions related to ZigBee hardware). The ZigBee mesh topology is based on a coordinator that governs the network, routers that establish connection from the coordinator to other routers or from a router to end devices, and end devices that collect information. In this case study we assume that the IoT enabled bridge is the target of an energy depletion attack, which is a cyber-physical attack targeting the IoT based WSN.

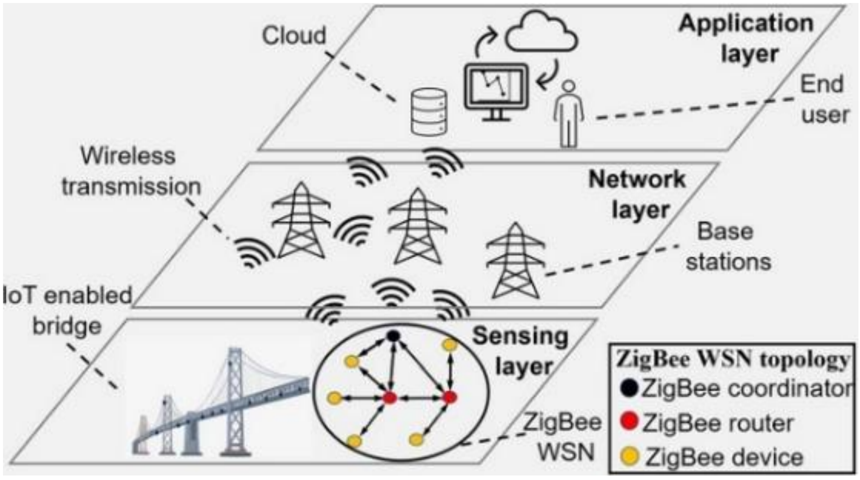

Figure 2. IoT enabled bridge case study.

4.1. Cyber-Physical Attack Scenarios against the IoT Based WSN

ZigBee devices are prone to cyber-physical attacks, due to inherent vulnerabilities of their protocol stack. A common cyber-physical attack against ZigBee technology is the energy depletion attack [56,73]. If the threat source has sufficient physical proximity to the end devices in the ZigBee WSN, it can exploit vulnerability in the MAC layer to victimize such devices by sending them bogus messages until their energy is depleted. The cyber-physical attack scenario identified during Activity 2 in Figure 1 should include the following steps of: (a) Reconnaissance; (b) Infiltration; and (c) Conclusion, as shown in Figure 3.

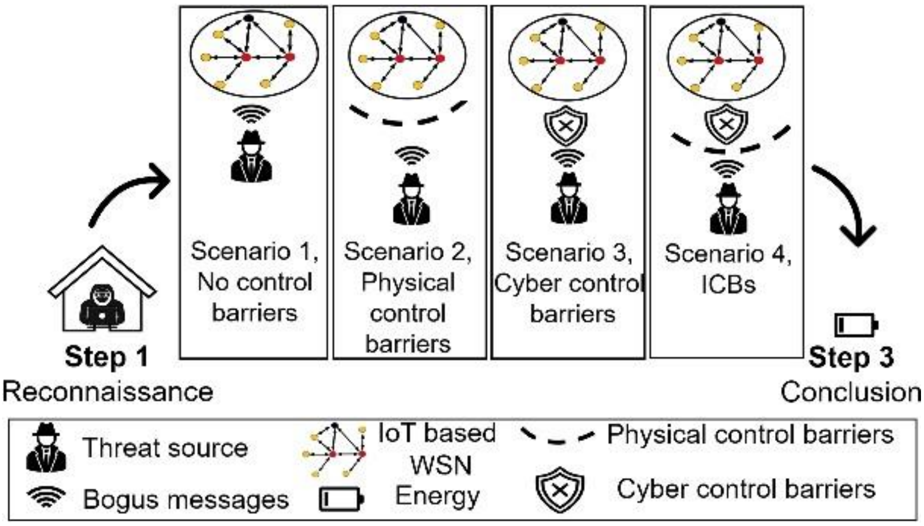

Figure 3. Four scenarios of energy depletion attack against IoT based WSN.

Reconnaissance. This step is performed before an attack takes place. The threat source is motivated to launch a cyber-physical attack against the IoT based WSN. The gathering of information is accomplished by performing physical and remote activities. The threat source can physically visit the IoT based WSN to evaluate the level of physical security, in terms of existence of physical control barriers that could restrict their moves (e.g., cameras) and collect information of the integrated IoT technology. The threat source can also remotely use their laptop to gather information about the ZigBee technology. Information about ZigBee and IoT technology allows a threat source to identify exploitable vulnerabilities in order to instrument the attack methods and supply the necessary tools to conduct the attack. Public databases and criminal cyber communities (e.g., Dark Web) provide information on exploitable vulnerabilities [51,74]. The threat source can act alone or increase the manpower by acting as part of larger groups.

Infiltration. The threat source infiltrates the physical area of the IoT based WSN to broadcast bogus signals. To achieve this aim, the threat source should use module with sufficient storage and computation capabilities. The threat source crafts bogus messages that do not pass the integrity check (i.e., a message integrity code verification standard in MAC layer) of the ZigBee protocol stack. The admission process of messages performed in the ZigBee devices consume an amount of energy. However, the victimized ZigBee devices, are unable to develop blacklists (i.e., a protocol stack vulnerability) and inform the network or the operator about unidentified malicious devices, attempting to join the network, and therefore prevent threat source from sending bogus messages. The threat source exploits this vulnerability and sends a significant number of bogus messages to enforce victim ZigBee devices running unforeseen computations and therefore consuming a significant amount of energy. The threat source sends the bogus messages either at different times or by victimizing other IoT devices to avoid being caught. In this case study, the IoT based WSN operates under one IoT system.

Conclusion. Finally, the threat source consumes the energy of ZigBee devices and can fully disrupt the IoT based WSN through a DoS attack and unavailability of data or loss of data packets due to network congestion.

The abovementioned cyber-physical attack is composed of four scenarios, that reflect the application of different control barriers in cyber and physical space in the IoT enabled bridge sensing area. The existence of control barriers reduces the decision score of Attack vector (X_{AV}) and Attack complexity (X_{AC}). The control barriers are applied to prevent, detect or respond to the energy depletion attack.

Scenario 1—No control barriers. The threat source infiltrates the physical area of the IoT based WSN, launching the attack against the victim ZigBee devices. Physical accessibility to the IoT WSN increases the score of X_{AV}. Due to the lack of control barriers in cyber space, the threat source can consume the energy of ZigBee devices without carrying out additional steps. This increases the score of X_{AC}.

Scenario 2—Physical control barriers only. Physical control barriers, such as intelligent video-surveillance systems, motion detectors or line crossing [75,76], can detect or prevent physical access of the threat source to the IoT based WSN. The presence of such control barriers should reduce the score assigned to X_{AV}. However, if the threat source has sufficient knowledge, motivation, resources, and terrorism experience to overcome the physical control barriers, energy of IoT devices can still be depleted.

Scenario 3—Cyber control barriers only. The threat source can infiltrate the physical area of the IoT based WSN, as discussed in Scenario 1. Cyber control barriers increase the steps that should be carried out by the threat source to exploit the vulnerability and reduce the level of Attack complexity (X_{AC}). An example of the cyber control barrier that could prevent the threat source from sending bogus messages is the development of a blacklist of misbehaving devices [56]. A cyber control barrier that could detect the energy depletion attack is the application called Intrusion Detection Systems, which could detect known and new types of attacks against ZigBee devices and alert operators when malicious actions are detected [77].

Scenario 4—Integrated Control barriers (ICBs). These control barriers are a combination of the physical and cyber control barriers described in Scenarios 2 and 3, respectively.

4.2. Assessment of Vulnerability, Threat Source and Physical Impact

The assessment of the individual characteristics of vulnerability (i.e., *Attack vector* (X_{AV}, W_{AV}), *Attack complexity* (X_{AC}, W_{AC}), *User interaction* (X_{UI}, W_{UI}), *Privileges required* (X_{PR}, W_{PR}), *Interoperability* (X_{IO}, W_{IO})), threat source (i.e., *Knowledge* (X_{KN}, W_{KN}), *Resources* (X_{RE}, W_{RE}), *Psychology* (X_{PS}, W_{PS}), *and Terrorism experience* (X_{Te}, W_{Te})) and type of physical impact (X_{PI}) are based on the description of the experimental study as presented in [56].

Concerning the assessment of the MAC layer vulnerability, the exploitation of this vulnerability based on the identified cyber-physical attack scenario, does not require the threat source to interact with any other user (*User interaction*), to have any privileges (*Privileges required*), or to gain access to other interacting IoT devices (*Interoperability*). Thus, assessors can assign W_{UI}, W_{PR}, W_{IO} a score in [0–0.20] corresponding to a Very low level. The threat source exploits the MAC layer vulnerability without the need to interact with other users, without requiring additional privileges, and without the need to gain entry point through another IoT device, since the IoT based WSN operates under one IoT application. Thus, assessors can assign X_{UI} and X_{PR} a score corresponding to a High or Very High level (i.e., 8–10). They can also assign X_{IO} a score corresponding to a Very low level (0–1). To perpetrate the energy depletion attack successfully, the threat source needs to have a sufficient level of physical proximity with the IoT devices and act without being identified as a malicious sender, in order to send bogus messages targeting the Zigbee protocol. Thus, assessors should assign both W_{AV}, W_{AC} values corresponding to a Very High level in [0.81, 1]. In Scenario 1 (i.e., *No control barriers*), the threat source can be in close proximity to the ZigBee device without performing any additional step to communicate with them. Thus, assessors can assign X_{AV}, X_{AC} scores corresponding to High or Very high levels. In Scenario 2, the existence of control barriers in physical space only and the lack of control barriers in cyber space reduce X_{AV} that should be assigned a score ranging from Very low to Low level. In Scenario 3, the existence of control barriers in cyber space only, can eliminate the MAC layer vulnerability and thus reduces X_{AC} that now should be assigned a score corresponding to a Very low level. As Scenario 4 combines control barriers in both cyber and physical spaces, X_{AV} should be assigned a score ranging from Very Low to Low level and X_{AC} should be assigned a score corresponding to a Low level.

Regarding assessment of the threat source, the exploitation of the MAC layer vulnerability does require a moderate level of knowledge in the three steps, although it does not necessitate resources (e.g., advanced computational modules) or manpower. Thus, assessors should assign W_{KN} a value in [0.61, 1.0] corresponding to a High to Very high level. They should also assign W_{RE} a value in [0, 0.4] corresponding to a Very low or Low level. Additionally, the exploitation of the MAC layer vulnerability requires strong motives and terrorism experience. Thus, assessors should assign W_{PS} and W_{Te} a value in [0.81, 1.0] corresponding to a Very high level. While critical transportation infrastructure has always been a target for attackers involved into terrorism activities, we assume that the threat source has a sufficient level of knowledge, access to resources, strong motives and terrorism experience. Thus, we assign $X_{KN,}$ $X_{RE,}$ $X_{PS,}$ X_{Te} a decision score corresponding at least to a Medium level (between 5 and 10).

Regarding the assessment of physical impact for the four scenarios, successful exploitation of the vulnerability can result in closure of the IoT enabled bridge for days or weeks (i.e., economic losses) until restoration services take place. Thus, assessors should assign X_{PI} a decision score comprised between five and seven corresponding to a Medium level (i.e., 5–7). The scores assigned to the characteristics and weights of the vulnerability and threat source and the physical impact are shown in Table 4.

Table 4. Assigned scores to vulnerability, threat source and physical impact per scenario.

Scenarios	Vulnerability $(W_i)/(X_i)$	Threat Source $(W_i)/(X_i)$	Physical Impact (X_{PI})
1. No control barriers	**AV, AC:** (VH)/(H to VH) **UI, PR:** (VL)/(H to VH) **IO:** (VL)/(VL)	**KN**: (H-VH)/(M-VH) **RE**: (VL-L)/(M-VH) **PS**: (VH)/(M-VH) **Te**: (VH)/(M-VH)	**Economic losses** M
2. Physical control barriers only	**AV:** (VH)/(VL TO L) **AC:** (VH)/(H to VH) **UI, PR:** (VL)/(H to VH) **IO:** (VL)/(VL)		
3. Cyber control barriers only	**AV:** (VH)/(H to VH) **AC:** (VH)/(VL) **UI, PR:** (VL)/(H to VH) **IO:** (VL)/(VL)		
4. ICBs (both cyber and physical control barriers)	**AV:** (VH)/(VL TO L) **AC:** (VH)/(VL) **UI, PR:** (VL)/(H to VH) **IO:** (VL)/(VL)		

AV: *Attack vector*, **AC**: *Attack complexity*, **UI**: *User Interaction*, **PR**: *Privileges required*, **IO**: *Interoperability*, **KN:** *Knowledge*, **RE:** *Resources*, **PS:** *Psychology*, **Te**: *Terrorism experience*; X_i:VL: Very Low (0–1), L: Low (2–4), M: Medium (5–7), H: High (8–9), VH: Very High (10); Wi: VL: (0–0.20), L: (0.21–0.40), M: (0.41–0.60), H: (0.61–0.80), VH: (0.81–1.0).

The assigned ranges of scores as presented in Table 4, following the description of the experimental study in [56], will be used as the parameters for the Monte Carlo simulations (see Section 4.3).

4.3. Analysis and Results

This section provides the results obtained performing Monte Carlo simulations and a sensitivity analysis, using as variables the values in the ranges shown in Table 4. Five thousand Monte Carlo simulations were performed for each scenario using random number generators uniformly distributed. For the output (i.e., cyber-physical risk), the basic statistical measures of mean, maximum, minimum and coefficient of variation were considered [78]. Simulation results that represent the cyber-physical risk for each scenario using the inputs from Table 4 are presented in Figure 4. It can be seen in Figure 4 that a significant reduction occurs in the cyber-physical risk when ICBs operate together (Scenario 4). Comparing Scenario 1 (i.e., No barriers) and Scenario 4 (i.e., ICBs), it was possible to obtain a decrease in risk of 62.16% in maximum values and of 71.8% in mean values.

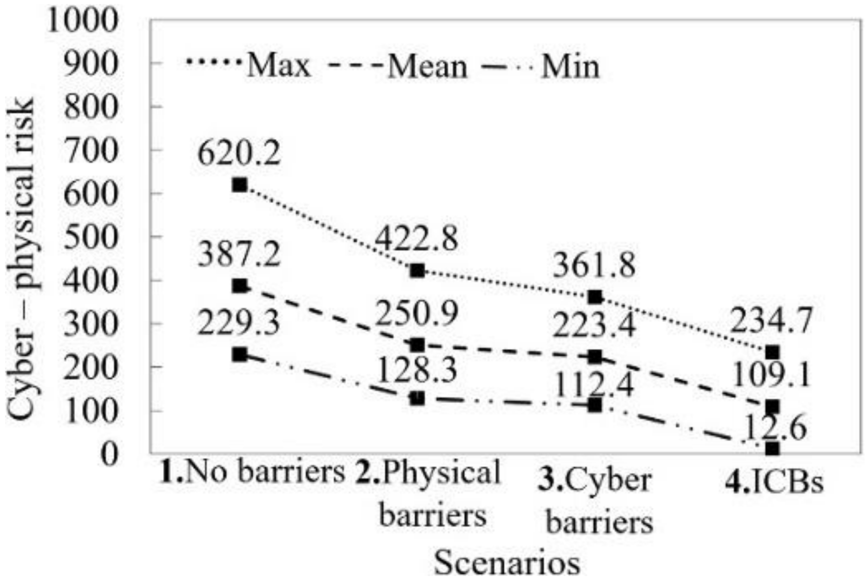

Figure 4. Cyber-physical risk per scenario.

The coefficient of variation, as the relative dispersion of data points around the mean values, ranges from 15% to 18.7% for Scenarios 1, 2 and 3 indicating a smaller dispersion and greater reliability of the mean as statistical measure, as compared to 30.6% for Scenario 4. The Monte Carlo outputs in Figure 5 demonstrate the frequency of occurrence in the determined risk boundaries (see Table 2) for each scenario. Results from Figure 5 illustrate that the cyber-physical attack against the IoT based WSN can result in conditions of High Risk (i.e., risk greater than 343) occurring 76.6% in Scenario 1 (no barriers) whilst including any control barrier in the cyber and/or physical space completely eliminates completely the High risk (3.2% in Scenario 2 and 0% in Scenarios 3 and 4).

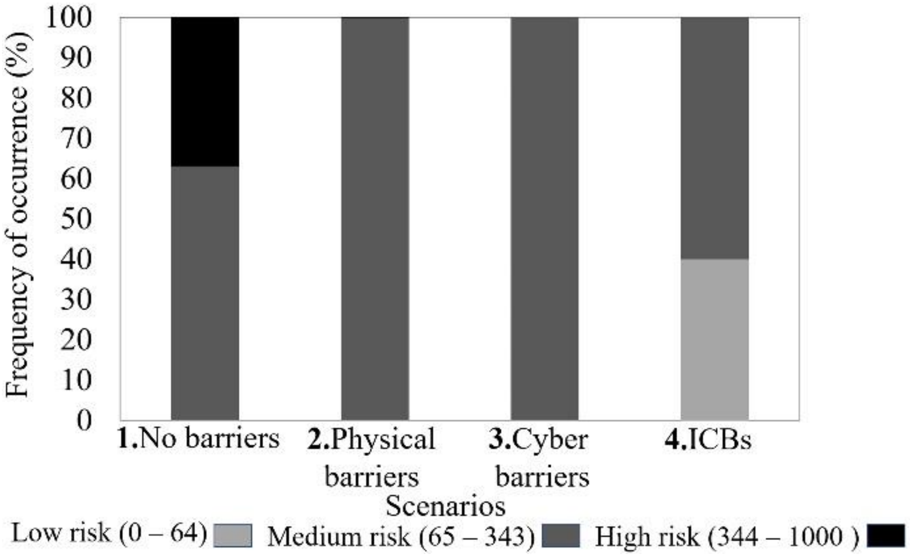

Figure 5. Frequency of occurrence of cyber-physical risk levels per scenario.

The inclusion of the importance indexes contributes towards the accurate calculation of cyber-physical risk, in terms of the importance of certain characteristics. Other studies or standards do not take the importance index into consideration. The influence of the importance index is investigated from the Monte Carlo simulations using the input scores from Table 4, when $W_i = 1$ for every characteristic. The results are illustrated in Figure 6. Results from Figure 6 demonstrate that ignoring the importance indexes, can result in a significant underestimation of cyber-physical risk. When results in Figure 4 are compared to Figure 6, the greatest deviation is depicted in Scenario 1, with an underestimation of cyber-physical risk of 15.1% in mean values (i.e., 387.2 in Figure 4 and 328.8 in Figure 6), and in Scenario 4 with an overestimation of cyber-physical risk of 73.3% in mean values (i.e., 109.1 in Figure 4 and 189.1 in Figure 6).

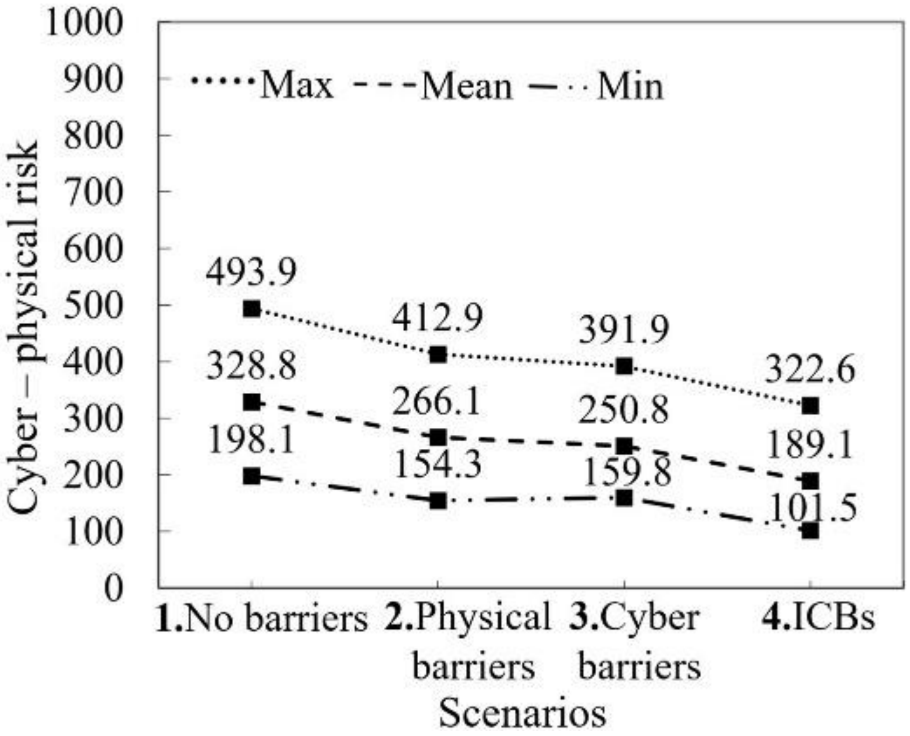

Figure 6. Cyber-physical risk when no importance index is considered (i.e., $W_i = 1$).

Finally, a sensitivity analysis for the proposed threat source characteristic of Terrorism experience, in the Monte Carlo simulations was undertaken to demonstrate the relevance of the decision score of this characteristic. By keeping constant all the inputs (i.e., X_i, W_i) from Scenario 1, as in Table 4, three categories of threat source related to intensity score of Terrorism experience are considered. The specific categories capture real examples from a threat source and its potential association with terrorist organizations that target critical infrastructure as described by Gunes et al. [38]. Specifically, the threat source could either have no terrorism experience, (X_{Te} is assigned a Low level) or being manipulated online using social media or online communities (X_{Te} is assigned a Medium level), or is a terrorist organization (X_{Te} is assigned a Very high level). Results for the cyber-physical attack, as shown in Figure 7, indicate an increase of 58.05% in mean values of cyber-physical risk, when they are undertaken by a terrorist organization in comparison to threat sources with no previous terrorism experience.

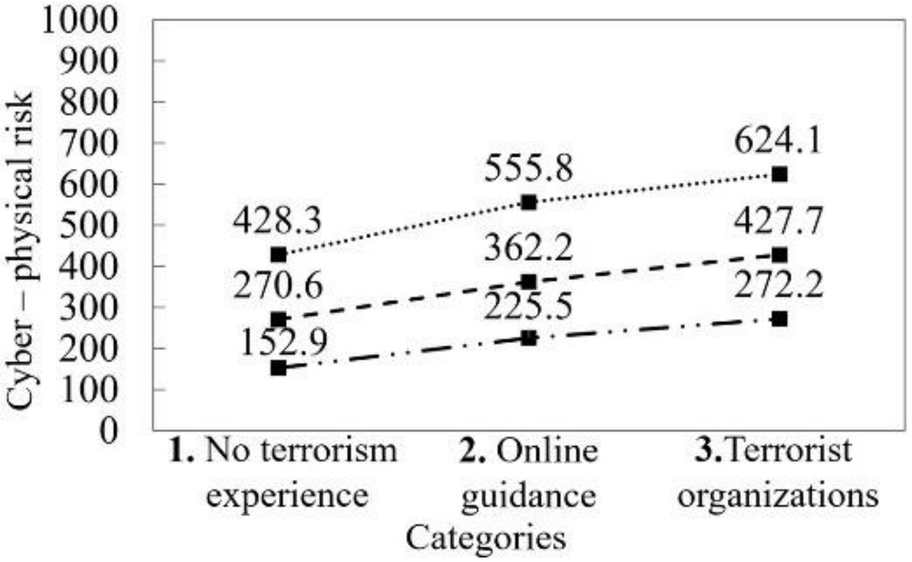

Figure 7. Sensitivity analysis considering Terrorism experience characteristic.

5. Discussion

The results of the cyber-physical risk assessment of the illustrative attack on the IoT based WSN, indicate that IoT enabled transportation infrastructure is susceptible to cyber-physical attacks that can be conducted on the sensing area. The proposed cyber-physical risk assessment approach was developed to assist stakeholders who act as assessors towards the assessment of their own system against cyber-physical attacks, but also improve existing risk assessment approaches by incorporating fundamental characteristics of vulnerability and threat source from cyber and physical space. The identification and proposal of cyber-physical characteristics associated with the security and civil engineering domain (i.e., Terrorism experience) and the inclusion of types of physical impacts, target to bridge the gap between cyber and physical space. To the best of the author's knowledge, while most studies focus on different aspects of IoT applications in transportation domain (e.g., reliability of data), this is the first study that considers a cyber-physical attack against an IoT based WSN as a part of an IoT enabled transportation infrastructure. The proposed approach contributes to existing studies (see Section 2) that mainly focus on remote attacks against infrastructure, through the internet [20] or on other interacting smart elements (e.g., smart vehicles) [19]. The results of the risk analysis undertaken in this paper demonstrate that if the threat source enables a sufficient attack path (Attack vector) and perform a few steps (Attack complexity) then cyber-physical risk will be significant (i.e., 76.6% of attack scenarios, see Figure 5) and thus cyber-physical attacks against IoT based WSN should not be neglected. Control barriers as described in Section 4.1 should be considered to reduce cyber-physical risk (refer to Figure 4). The inclusion of integrated control barriers can eliminate High risk levels (refer to Figure 5) completely.

Additionally, the cyber-physical risk assessment approach is based on both identified and proposed cyber-physical characteristics and their importance (see Equation (1)). The risk simulations suggest that risk can be underestimated and overestimated when generic or simplistic threat profiles are used. For example, in comparison to other studies, such as [26], that adopt a more generic threat profile, or standards [31] that do not consider the importance indexes, outcomes of the approach indicate an underestimation of risk (comparison of Figure 4 with Figure 6). This can be very challenging as importance of specific characteristics can affect the risk calculations. It is acknowledged that the structure of the cyber-physical risk assessment approach (refer to Figure 1) necessitates the role of stakeholders, who act as assessors. Experts' opinion is needed as there is still significant underreporting of incidence and a lack of scientifically verified data on cyber-physical attacks. For example, as shown in Figure 7, the assignment of score in threat source characteristics (i.e., Terrorism experience) could affect the cyber-physical risk.

It is acknowledged that such challenges around the selection of certain ranges or scores could affect the risk approach, which is based on expert judgment and the rational considerations about the cyber-physical attack scenario. Therefore, an inventory of the assessment of vulnerability, threat source and physical impact in different scenarios would be beneficial to guide the expert judgement in performing the risk assessment. The latter (i.e., inventory) along with the development of datasets that include training data related to cyber-attacks against transportation infrastructure, would resolve one of the main challenges of machine learning methods (i.e., lack of training data) in the detection of cyber-attacks.

Additionally, the role of stakeholders in the assessment process should be clearly distinguished. For example, security engineers should be actively involved in the assessment of vulnerability, while they should collaboratively be involved in the assessment of threat source along with civil engineers. Operators that have bespoke knowledge of their system should be actively involved in the assessment of physical impact.

6. Conclusions

Critical transportation infrastructure implemented with IoT technology can be targeted by multiple threats due its cyber-physical nature. The knowledge gap between security and civil engineering domain, a lack of statistical data related to cyber-attacks and emerging threats from cyber and physical space make the assessment of risk more difficult. Additionally, the exposure of IoT devices in physical areas brings new opportunities for attackers, which have been previously overlooked. To address this gap, in this paper a novel cyber-physical risk assessment approach is proposed. This is based on cyber-physical characteristics of threat sources, vulnerabilities, and types of physical impacts. The approach utilizes a decision scale and importance indexes, to assist stakeholders in the assessment of the level of vulnerability, threat source and physical impact. To overcome the lack of data and the premature level of IoT adoption in transportation infrastructure, an illustrative but realistic case study of an IoT enabled bridge subjected to a cyber-physical attack in the physical space was presented. Results from Monte Carlo simulations, indicate that IoT enabled transportation infrastructure is susceptible to cyber-physical attacks when the threat source can physically access IoT devices that have limited physical and cyber control barriers, resulting in high risk levels in a significant number of cases. Control barriers that operate in both cyber and physical space, individually or combined, resulted in the reduction in cyber-physical risk. Comparison with other studies that do not thoroughly consider the importance of characteristics, led to an underestimation of cyber-physical risk. Overall, this risk assessment approach can constitute a valuable resource towards the future assessment of IoT enabled transportation infrastructure under its cyber-physical perspective.

Author Contributions: All the researchers collaborated for the main activities of the study, main contributions may be identified as follows: Conceptualization, K.N. and D.P.M. and L.P.; methodology, K.N. and D.P.M. and L.P.; software, K.N.; validation, K.N. and D.P.M. and L.P.; formal analysis, K.N. and D.P.M. and L.P.; investigation, K.N. and D.P.M. and L.P.; resources, D.P.M. and L.P.; data curation, K.N.; writing—original draft preparation, K.N.; writing—review and editing, K.N. and D.P.M. and L.P.; visualization, K.N.; supervision, D.P.M. and L.P.; project administration, D.P.M. and L.P.; funding acquisition, D.P.M. and L.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the University College of Dublin Advanced PhD Scholarship Scheme 41063.

Institutional Review Board Statement: Not applicable.

Data Availability Statement: Data is contained within the article.

Acknowledgments: This work is financially supported by a University College of Dublin Advanced PhD Scholarship Scheme.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Singh, S.K.; Jeong, Y.-S.; Park, J.H. A deep learning-based IoT-oriented infrastructure for secure smart city. *Sustain. Cities Soc.* **2020**, *60*, 102252. [CrossRef]
2. Fakhimi, A.H.; Khani, A.H.; Sardroud, J.M. Smart-city infrastructure components. In *Solving Urban Infrastructure Problems Using Smart City Technologies*; Elsevier: Amsterdam, The Netherlands, 2021; pp. 17–54.
3. Koursari, E.; Wallace, S.; Xu, Y.; Michalis, P.; Valyrakis, M. Smart bridge: Towards robust monitoring of environmental hazards. In *River Flow 2020*; CRC Press: Boca Raton, FL, USA, 2020; pp. 886–890.
4. Zhao, Z.; Gao, Y.; Hu, X.; Zhou, Y.; Zhao, L.; Qin, G.; Guo, J.; Liu, Y.; Yu, C.; Han, D. Integrating BIM and IoT for smart bridge management. In *IOP Conference Series: Earth and Environmental Science*; IOP Publishing: Bristol, UK, 2019.
5. Mishra, M.; Lourenço, P.B.; Ramana, G.V. Structural health monitoring of civil engineering structures by using the internet of things: A review. *J. Build. Eng.* **2022**, *48*, 103954. [CrossRef]
6. Tokognon, C.A.; Gao, B.; Tian, G.Y.; Yan, Y. Structural health monitoring framework based on Internet of Things: A survey. *IEEE Internet Things J.* **2017**, *4*, 619–635. [CrossRef]
7. Da Xu, L.; He, W.; Li, S. Internet of things in industries: A survey. *IEEE Trans. Ind. Inform.* **2014**, *10*, 2233–2243.
8. Mahmoud, R.; Yousuf, T.; Aloul, F.; Zualkernan, I. Internet of things (IoT) security: Current status, challenges and prospective measures. In Proceedings of the 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 14–16 December 2015.
9. Loukas, G. *Cyber-Physical Attacks: A Growing Invisible Threat*; Butterworth-Heinemann: Oxford, UK, 2015.
10. Butun, I.; Österberg, P.; Song, H. Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. *IEEE Commun. Surv. Tutor.* **2019**, *22*, 616–644. [CrossRef]
11. Templeton, S.J. Security aspects of cyber-physical device safety in assistive environments. In Proceedings of the 4th International Conference on PErvasive Technologies Related to Assistive Environments, Heraklion Crete, Greece, 25–27 May 2011.
12. ENISA. Security measures in the Railway Transport Sector. In *Railway Cybersecurity*; European Union Agency for Cybersecurity: Athens, Greece, 2020.
13. Kouicem, D.E.; Bouabdallah, A.; Lakhlef, H. Internet of things security: A top-down survey. *Comput. Netw.* **2018**, *141*, 199–221. [CrossRef]
14. Perti, A.; Singh, A.; Sinha, A.; Srivastava, P.K. Security risks and challenges in IoT-based applications. In Proceedings of the International Conference on Big Data, Machine Learning and Their Applications, Prayagraj, India, 29–31 May 2020; Springer: Singapore, 2021.
15. Tsantikidou, K.; Sklavos, N. Vulnerabilities of Internet of Things, for Healthcare Devices and Applications. In Proceedings of the 2021 8th NAFOSTED Conference on Information and Computer Science (NICS), Hanoi, Vietnam, 21–22 December 2021.
16. Lonzetta, A.M.; Cope, P.; Campbell, J.; Mohd, B.J.; Hayajneh, T. Security vulnerabilities in Bluetooth technology as used in IoT. *J. Sens. Actuator Netw.* **2018**, *7*, 28. [CrossRef]
17. Moore, S.J.; Nugent, C.D.; Zhang, S.; Cleland, I. IoT reliability: A review leading to 5 key research directions. *CCF Trans. Pervasive Comput. Interact.* **2020**, *2*, 147–163. [CrossRef]
18. Dong, Y.; Frangopol, D.M. Risk and resilience assessment of bridges under mainshock and aftershocks incorporating uncertainties. *Eng. Struct.* **2015**, *83*, 198–208. [CrossRef]
19. Thaduri, A.; Aljumaili, M.; Kour, R.; Karim, R. Cybersecurity for eMaintenance in railway infrastructure: Risks and consequences. *Int. J. Syst. Assur. Eng. Manag.* **2019**, *10*, 149–159. [CrossRef]
20. PROTECTRAIL. The Railway-Industry Partnership for Integrated Security of Rail Transport. 2014. Available online: https://www.protectrail.eu/ (accessed on 1 July 2022).
21. SECRET. Security of Railways against Electromagnetic Attacks. 2015. Available online: https://secret-project.eu/ (accessed on 1 July 2022).
22. CARONTE. Creating an Agenda for Research ON Transportation sEcuity. 2016. Available online: https://cordis.europa.eu/project/id/606967 (accessed on 1 July 2022).
23. CIPSEC. Enhancing Critical Infrastructure Protection with Innovative SECurity Framework. 2019. Available online: https://www.cipsec.eu/ (accessed on 1 July 2022).
24. CIPSEC. UPCommons. Global access to UPC knowledge. 2019. Available online: https://upcommons.upc.edu/handle/2117/106378 (accessed on 14 September 2022).
25. NIST. Guide for Conducting Risk Assessments. 2012. Available online: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf (accessed on 1 July 2022).
26. Ramotsoela, D.; Abu-Mahfouz, A.; Hancke, G. A survey of anomaly detection in industrial wireless sensor networks with critical water system infrastructure as a case study. *Sensors* **2018**, *18*, 2491. [CrossRef] [PubMed]

27. Zeadally, S.; Tsikerdekis, M. Securing Internet of Things (IoT) with machine learning. *Int. J. Commun. Syst.* **2020**, *33*, e4169. [CrossRef]
28. Wu, M.; Song, Z.; Moon, Y.B. Detecting cyber-physical attacks in CyberManufacturing systems with machine learning methods. *J. Intell. Manuf.* **2019**, *30*, 1111–1123. [CrossRef]
29. Berglund, E.Z.; Monroe, J.G.; Ahmed, I.; Noghabaei, M.; Do, J.; Pesantez, J.E.; Fasaee, M.A.K.; Bardaka, E.; Han, K.; Proestos, G.T. Smart infrastructure: A vision for the role of the civil engineering profession in smart cities. *J. Infrastruct. Syst.* **2020**, *26*, 03120001. [CrossRef]
30. Maschmeyer, L.; Deibert, R.J.; Lindsay, J.R. A tale of two cybers-how threat reporting by cybersecurity firms systematically underrepresents threats to civil society. *J. Inf. Technol. Politics* **2021**, *18*, 1–20. [CrossRef]
31. Gandhi, R.; Sharma, A.; Mahoney, W.; Sousan, W.; Zhu, Q.; Laplante, P. Dimensions of cyber-attacks: Cultural, social, economic, and political. *IEEE Technol. Soc. Mag.* **2011**, *30*, 28–38. [CrossRef]
32. Theocharidou, M.; Giannopoulos, G. *Risk Assessment Methodologies for Critical Infrastructure Protection. Part II: A New Approach*; Scientific and Technical Research Reports; Publications Office of the European Union: Luxembourg, 2015.
33. NIST. *Framework for Improving Critical Infrastructure Cybersecurity*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2018.
34. NIST. *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2019.
35. FIRST. Common Vulnerability Scoring System 2019. Available online: https://www.first.org/ (accessed on 1 July 2022).
36. Wang, Y.; Wang, Y.; Qin, H.; Ji, H.; Zhang, Y.; Wang, J. A Systematic Risk Assessment Framework of Automotive Cybersecurity. *Automot. Innov.* **2021**, *4*, 253–261. [CrossRef]
37. Ekedebe, N.; Yu, W.; Lu, C.; Song, H.; Wan, Y. Securing transportation cyber-physical systems. In *Securing Cyber-Physical Systems*; CRC Press: Boca Raton, FL, USA, 2015; pp. 163–196.
38. Škorput, P.; Vojvodić, H.; Mandžuka, S. Cyber security in cooperative intelligent transportation systems. In Proceedings of the 2017 International Symposium ELMAR, Zadar, Croatia, 18–20 September 2017.
39. Sun, Y.; Song, H. *Secure and Trustworthy Transportation Cyber-Physical Systems*; Springer: Berlin/Heidelberg, Germany, 2017.
40. Kelarestaghi, K.B.; Foruhandeh, M.; Heaslip, K.; Gerdes, R. Intelligent transportation system security: Impact-oriented risk assessment of in-vehicle networks. *IEEE Intell. Transp. Syst. Mag.* **2019**, *13*, 91–104. [CrossRef]
41. Gunes, B.; Kayisoglu, G.; Bolat, P. Cyber security risk assessment for seaports: A case study of a container port. *Comput. Secur.* **2021**, *103*, 102196. [CrossRef]
42. Kure, H.I.; Islam, S.; Razzaque, M.A. An integrated cyber security risk management approach for a cyber-physical system. *Appl. Sci.* **2018**, *8*, 898. [CrossRef]
43. ENISA. Port Cybersecurity—Good Practices for Cybersecurity in the Maritime Sector. 2019. Available online: https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector (accessed on 1 July 2022).
44. Kandasamy, K.; Srinivas, S.; Achuthan, K.; Rangan, V.P. IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP J. Inf. Secur.* **2020**, *2020*, 8. [CrossRef]
45. Karie, N.M.; Sahri, N.M.; Yang, W.; Valli, C.; Kebande, V.R. A review of security standards and frameworks for IoT-based smart environments. *IEEE Access* **2021**, *9*, 121975–121995. [CrossRef]
46. Stellios, I.; Kotzanikolaou, P.; Grigoriadis, C. Assessing IoT enabled cyber-physical attack paths against critical systems. *Comput. Secur.* **2021**, *107*, 102316. [CrossRef]
47. Gallon, L.; Bascou, J.J. Using CVSS in attack graphs. In Proceedings of the 2011 Sixth International Conference on Availability, Reliability and Security, Vienna, Austria, 22–26 August 2011.
48. Agadakos, I.; Chen, C.-Y.; Campanelli, M.; Anantharaman, P.; Hasan, M.; Copos, B.; Lepoint, T.; Locasto, M.; Ciocarlie, G.F.; Lindqvist, U. Jumping the air gap: Modeling cyber-physical attack paths in the Internet-of-Things. In Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy, Dallas, TX, USA, 3 November 2017.
49. Jackson, D. Alloy: A lightweight object modelling notation. *ACM Trans. Softw. Eng. Methodol. TOSEM* **2002**, *11*, 256–290. [CrossRef]
50. Zambon, E.; Etalle, S.; Wieringa, R.J.; Hartel, P. Model-based qualitative risk assessment for availability of IT infrastructures. *Softw. Syst. Modeling* **2011**, *10*, 553–580. [CrossRef]
51. CVE. Common Vulnerabilities and Exposures. 2022. Available online: https://cve.mitre.org/cve/search_cve_list.html (accessed on 1 July 2022).
52. Meneghello, F.; Calore, M.; Zucchetto, D.; Polese, M.; Zanella, A. IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices. *IEEE Internet Things J.* **2019**, *6*, 8182–8201. [CrossRef]
53. Olawumi, O.; Haataja, K.; Asikainen, M.; Vidgren, N.; Toivanen, P. Three practical attacks against ZigBee security: Attack scenario definitions, practical experiments, countermeasures, and lessons learned. In Proceedings of the 2014 14th International Conference on Hybrid Intelligent Systems, Kuwait, Kuwait, 14–16 December 2014.
54. Krishna, R.R.; Priyadarshini, A.; Jha, A.V.; Appasani, B.; Srinivasulu, A.; Bizon, N. State-of-the-art review on IoT threats and attacks: Taxonomy, challenges and solutions. *Sustainability* **2021**, *13*, 9463. [CrossRef]
55. CAPEC. Common Attack Pattern Enumeration and Classification. 2022. Available online: https://capec.mitre.org/ (accessed on 1 July 2022).

56. Cao, X.; Shila, D.M.; Cheng, Y.; Yang, Z.; Zhou, Y.; Chen, J. Ghost-in-zigbee: Energy depletion attack on zigbee-based wireless networks. *IEEE Internet Things J.* **2016**, *3*, 816–829. [CrossRef]
57. Hossain, M.M.; Fotouhi, M.; Hasan, R. Towards an analysis of security issues, challenges, and open problems in the internet of things. In Proceedings of the 2015 IEEE World Congress on Services, New York, NY, USA, 27 June–2 July 2015.
58. Desai, P.; Sheth, A.; Anantharam, P. Semantic gateway as a service architecture for iot interoperability. In Proceedings of the 2015 IEEE International Conference on Mobile Services, New York, NY, USA, 27 June–2 July 2015.
59. Mrabet, H.; Belguith, S.; Alhomoud, A.; Jemai, A. A survey of IoT security based on a layered architecture of sensing and data analysis. *Sensors* **2020**, *20*, 3625. [CrossRef]
60. Nawaratne, R.; Alahakoon, D.; de Silva, D.; Chhetri, P.; Chilamkurti, N. Self-evolving intelligent algorithms for facilitating data interoperability in IoT environments. *Future Gener. Comput. Syst.* **2018**, *86*, 421–432. [CrossRef]
61. Doynikova, E.; Novikova, E.; Gaifulina, D.; Kotenko, I. Towards Attacker Attribution for Risk Analysis. In Proceedings of the International Conference on Risks and Security of Internet and Systems, Paris, France, 4–6 November 2020; Springer: Berlin/Heidelberg, Germany, 2020.
62. Rocchetto, M.; Tippenhauer, N.O. On attacker models and profiles for cyber-physical systems. In Proceedings of the European Symposium on Research in Computer Security, Heraklion, Greece, 26–30 September 2016; Springer: Berlin/Heidelberg, Germany, 2016.
63. Williamson, E.B.; Winget, D.G. Risk management and design of critical bridges for terrorist attacks. *J. Bridge Eng.* **2005**, *10*, 96–106. [CrossRef]
64. Malin, C.H.; Gudaitis, T.; Holt, T.; Kilger, M. *Deception in the Digital Age: Exploiting and Defending Human Targets through Computer-Mediated Communications*; Elsevier: Amsterdam, The Netherlands, 2017.
65. From Terrorism to Cyber-Terrorism: The Case of ISIS. 2018. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3135927 (accessed on 14 September 2022).
66. Radanliev, P.; de Roure, D.C.; Nicolescu, R.; Huth, M.; Montalvo, R.M.; Cannady, S.; Burnap, P. Future developments in cyber risk assessment for the internet of things. *Comput. Ind.* **2018**, *102*, 14–22. [CrossRef]
67. Scala, N.M.; Reilly, A.C.; Goethals, P.L.; Cukier, M. Risk and the five hard problems of cybersecurity. *Risk Anal.* **2019**, *39*, 2119–2126. [CrossRef] [PubMed]
68. Doty, P. US homeland security and risk assessment. *Gov. Inf. Q.* **2015**, *32*, 342–352. [CrossRef]
69. Esposito, S.; Stojadinovic, B.; Mignan, A.; Dolšek, M.; Babič, A.; Selva, J.; Iqbal, S.; Cotton, F.; Iervolino, I. *Report on the Proposed Engineering Risk Assessment Methodology for Stress Tests of Non-Nuclear CIs*; ETH Zurich: Zurich, Switzerland, 2016.
70. Dang, G.; Cheng, X. Application of wireless sensor network in monitoring system based on Zigbee. In Proceedings of the 2014 IEEE Workshop on Advanced Research and Technology in Industry Applications (WARTIA), Ottawa, ON, Canada, 29–30 September 2014.
71. Chae, M.; Yoo, H.; Kim, J.; Cho, M.-Y. Development of a wireless sensor network system for suspension bridge health monitoring. *Autom. Constr.* **2012**, *21*, 237–252. [CrossRef]
72. Harms, T.; Sedigh, S.; Bastianini, F. Structural health monitoring of bridges using wireless sensor networks. *IEEE Instrum. Meas. Mag.* **2010**, *13*, 14–18. [CrossRef]
73. Vidgren, N.; Haataja, K.; Patino-Andres, J.L.; Ramirez-Sanchis, J.J.; Toivanen, P. Security threats in ZigBee-enabled systems: Vulnerability evaluation, practical experiments, countermeasures, and lessons learned. In Proceedings of the 2013 46th Hawaii International Conference on System Sciences, Wailea, HI, USA, 7–10 January 2013.
74. Schäfer, M.; Fuchs, M.; Strohmeier, M.; Engel, M.; Liechti, M.; Lenders, V. BlackWidow: Monitoring the dark web for cyber security information. In Proceedings of the 2019 11th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, 28–31 May 2019.
75. Bocchetti, G.; Flammini, F.; Pragliola, C.; Pappalardo, A. Dependable integrated surveillance systems for the physical security of metro railways. In Proceedings of the 2009 Third ACM/IEEE International Conference on Distributed Smart Cameras (ICDSC), Como, Italy, 30 August–2 September 2009.
76. Fausto, A.; Gaggero, G.B.; Patrone, F.; Girdinio, P.; Marchese, M. Toward the Integration of Cyber and Physical Security Monitoring Systems for Critical Infrastructures. *Sensors* **2021**, *21*, 6970. [CrossRef]
77. Sadikin, F.; van Deursen, T.; Kumar, S. A ZigBee intrusion detection system for IoT using secure and efficient data collection. *Internet Things* **2020**, *12*, 100306. [CrossRef]
78. Raychaudhuri, S. Introduction to Monte Carlo simulation. In Proceedings of the 2008 Winter Simulation Conference, Miami, FL, USA, 7–10 December 2008.