


Article

Assessment of Terrorism Risk to Critical Infrastructures: The Case of a Power-Supply Substation

Xijun Yao ¹, Hsi-Hsien Wei ^{2,*}, Igal M. Shohet ^{3,4}  and Miroslaw J. Skibniewski ^{1,4,5,6}

¹ Department of Civil and Environmental Engineering, University of Maryland, 4298 Campus Dr., College Park, MD 20742, USA; miracl@hotmai.com (X.Y.); mirek@umd.edu (M.J.S.)

² Department of Building and Real Estate, Hong Kong Polytechnic University, 7/F, South Tower, Block Z, Kowloon ZS725, Hong Kong

³ Department of Structural Engineering, Ben-Gurion University of the Negev, P.O. Box 653, Beer Sheva 84105, Israel; igals@bgu.ac.il

⁴ Department of Construction Engineering, ChaoYang University of Technology, 168, Jifong E. Rd., Wufong District, Taichung City 41349, Taiwan

⁵ Institute for Theoretical and Applied Informatics, Polish Academy of Sciences, Bałtycka 5, 44-100 Gliwice, Poland

⁶ Department of Civil and Environmental Engineering and Architecture, University of Science and Technology Bydgoszcz, Al. Prof. S. Kaliskiego 7, Building 2.4, 85-796 Bydgoszcz, Poland

* Correspondence: hhwei@polyu.edu.hk; Tel.: +852-3400-8194

Received: 23 August 2020; Accepted: 12 October 2020; Published: 14 October 2020



Abstract: This paper presents a novel approach for estimating the vulnerability level of critical infrastructure confronting potential terrorist threats and assessing the usefulness of various protection strategies for critical infrastructure (CI). A methodology, utilizing a combination of topological network analysis and game theory, is presented to evaluate the effectiveness of protection strategies for certain components in the infrastructure under various attack scenarios. This paper focuses on protective strategies that are based on different attack scenarios as well as on the connectivity of the critical infrastructure components. The methodology proposed allows optimization of protection strategies in terms of investment in critical infrastructure protection in order to reduce expenditures on local infrastructure protection or on a single critical infrastructure for small projects. A case study of a power-supply substation is included to validate the analytical framework. The results indicate that the framework is highly applicable to other types of critical infrastructures facing similar threats. The results suggest that when only terrorist attacks are considered, improving the robustness of CI has a much higher effectiveness and efficiency than improving CI redundancy. The research methodology in this paper can be applied to a wide range of critical infrastructures and systems that may be at risk from manmade extreme events.

Keywords: critical infrastructure; risk assessment; terrorism

1. Introduction

The security of critical infrastructures (CIs)—“The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security”, examples of which include power supply, transportation, communication, energy and water, governance infrastructures and more [1]—has been the subject of increased governmental attention due to the expanding threat of terrorism [2]. Following the September 11

attacks in the United States, the list of CIs was expanded to 17, including energy and power systems; food, water supply and health care systems; and other service systems [3]. Since CIs are integral to the normal functioning of society, their failure is associated with immense risk. CIs are complex systems comprising various subsystem components, and their functionalities are based on the operations of the subsystems within the CIs. The complexity of CIs make them vulnerable, with minor failures sometimes resulting in significant losses [4]. For example, the unexpected and unalarmed shutdown of one high-voltage power line in northern Ohio in 2004 resulted in up to two days of blackout to 50 million people, costing an estimated \$6 billion and leading to 11 fatalities [5]. As compared to random infrastructure failures, terrorist attacks specifically targeting the most vulnerable components in CIs can result in much higher losses. The terrorist attack on the World Trade Center (WTC) in 2001, for example, resulted in an estimated total loss of \$123 billion, a larger amount than most natural disasters for which such figures are available [6]. Additionally, the collapse of the WTC also caused the failure of the water-supply system beneath it, which resulted in serious flooding to nearby places and the flood-related loss of 200,000 voice lines, 100,000 private branch exchange lines and 4.4 million data circuits [3]. Apart from such major high-profile terrorist attacks, a large number of terrorist attacks against CIs occur in various countries, with great frequency and significant consequences. On average, nearly eight terrorist attacks take place per day, causing up to 18,000 fatalities worldwide yearly [7,8]. The substation studied in this paper, which is a first degree strategic facility in Israel and the central electric power supplier of a regional town, has experienced continuous terror threats, and losses as high as \$600,000 per year due to terrorist attacks [9].

Considering the high levels of damage that CI failures may cause to human life, the economy, national security, and the normal functioning of society, accurate estimation of the vulnerability of CIs to terrorism hazards is of profound importance, as is the development of strategies that could protect CIs from such hazards, or reduce losses. Many models and methods have been developed for these purposes. Rinaldi et al. [10] proposed a method for identifying and classifying different types of interdependencies between infrastructural elements, and for recognizing rippling effects caused by interruptions based on such interdependencies. Dudenhofer et al. [11] devised mathematical definitions for each type of interdependency between infrastructure and the problem space, and modeled the potential effects on a community caused by the loss of power to an electrical-distribution substation. A variety of novel methodologies—for instance, using network theory, rating matrices, and system dynamics methods—have been used in recent years to estimate the vulnerability of infrastructure systems, especially power-supply systems [12]. However, there has hitherto been little research on vulnerability within a specific infrastructure during specific critical events, particularly terrorist attacks, and the potential risk due to the interactions between subsystems and components within that infrastructure.

In this paper, a network approach is used to model the vulnerability of a CI confronting component failure upon the occurrence of a given terrorist attack, and to evaluate the interactions between subsystems and components within the infrastructure based on system connectivity. In order to simulate strategies used to protect the CI against terrorist attacks, as well as the authorities' reactions to such attacks, a game-theory approach is selected as the basis for a vulnerability assessment in this study. This assessment aims to provide effective protective strategies in light of particular budgetary limits and the known attack scenario. Lastly, we present a case study of a power-supply substation in Israel that is under periodic attack, and determine the optimal protection strategy for it within various levels of budget limits.

2. Literature Review

2.1. Vulnerability Assessment of Critical Infrastructures

Modeling risk to CIs requires knowledge in two distinct fields: assessing the vulnerability of the infrastructure per se, and assessing the potential external threats to it [13]. The definition of vulnerability varies in the literature, but can be expressed as the magnitude of consequences that

follow the occurrence of a specific extreme event for the purposes of this paper [14]. More specifically, vulnerability can be analyzed by (1) modeling the responses of various components of the infrastructure confronting a threat and (2) assessing the risk to the entire infrastructure in light of the consequences of an attack on each component, the interactions between components, and the combined impact of direct and indirect damages on the overall functionality of the infrastructure. Vulnerability assessment of CIs can be complex, as their components are likely to exhibit different reactions to the same event. However, hazard effects on CIs can be broken down into two basic types: (1) direct losses on functionality of the components in the system, and (2) indirect effects arising from interactions between or among multiple components [15]. While the direct effects can be estimated straightforwardly based on the level of damage to the components and the costs of repair, estimating the indirect effects is relatively more difficult. Various models have been proposed to evaluate the vulnerability of CIs. Oh and Hastak [16] developed a two-degree model involving functional and social interactions between critical infrastructures and associated industries, which can be used to determine the impact of natural hazards on complex infrastructure systems. The resilience of subterranean infrastructure has been evaluated in research focused on decision-making processes, which resulted in better management [17]. A novel comprehensive model of vulnerability assessment, based on the liabilities and capabilities of the environment vis-à-vis disasters, was also investigated by McEntire et al. [18].

The system dynamics (SD) method is a useful approach to researching interdependency within a system, representing it using flows and feedback loops. The SD model enables researchers to study the functionalities of different components and provide optimization results according to different measuring criteria. Min et al. [19] used this model in an outstanding investigation of the interdependencies of the CIs of an entire country, while Rehan et al. [20] used SD to develop a wastewater system for a medium-sized city that was both financially sustainable and satisfactory in performance. Despite being primarily for evaluating interdependencies within a system, the SD method has also been used in modeling the vulnerability and resilience of CIs: for instance, by Cavallini et al. [21], who proposed an SD-based methodology called CRISADMIN to assist decision making in response to CI-related crises.

The topological approach, like network analysis, has been one of the most widely used methods of modeling complex infrastructure components and systems. Bompard et al. [22] used it to assess the vulnerability of a power-supply system, using the topological features of the network to model the interactions between busses and lines in the system. Wang et al. [23] proposed a more efficient methodology for vulnerability analysis of power-supply systems, specifically, to edge failures. This approach simplifies system-vulnerability analysis by abstracting all components of the system into interconnected nodes and edges, and models the relationship between components with topological approach. Yet, this simplification has weakened the differences between the characteristics of each component, as well as the possible relationships between them and the consideration of the physical parameters of the system. Though Hines et al. [24] have demonstrated the potential for drawing misleading conclusions from topological approaches to power-system analysis (under certain conditions), the use of such an approach has been an effective means of modeling connectivity in other types of systems [25–27] as well as a means for resilience assessment of MicroGrids electric distribution systems [28]. In this paper, the vulnerability of infrastructure confronting physical damage and operating failures was assessed in light of the varying functionality that would result from connectivity between different components and the protection level, respectively.

2.2. Strategies for Protecting Critical Infrastructures against Terrorist Attacks

Unlike natural hazards, terrorist attacks are not simply randomized events with a probability of occurrence that can be relatively well estimated (e.g., the return period of floods or earthquakes). In the case of risk analysis of terrorist attacks, the most challenging issue is to determine the probability of their occurrence, which (in contrast to natural disasters) may be related not only to the historical record of prior occurrences, but also to the current protection level of the CI. Such attacks are planned

in light of knowledge about their targets, knowledge that is often quite comprehensive; according to a captured al Qaeda training manual, “Using public sources openly and without resorting to illegal means, it is possible to gather at least 80% of information about the enemy” [29]. By considering the changes in intentions to attack in the wake of the adoption of new protective measures, Elkabets and Shohet [30] built a dynamic model to calculate the probability of terrorist attacks occurring at different levels of protection applied to a power-supply substation. The model integrates the protection level of the CI, the vulnerability, visibility, attack consequences, and the history of events for the assessment of the likelihood of a successful attack. Another way to estimate attackers’ intentions is to model scenarios using a game-theory framework. Working from an assumption that terrorists may be able to obtain and utilize up to 100% of the relevant information about the targeted CI, Brown et al. [31] studied the infrastructure-defense problem via a two-person, zero-sum framework and proposed new bi-level and tri-level models. Their later research [32] compared vulnerability analysis and defense strategies in several cases; the results assigned the weight of each component used in protecting various infrastructures, and indicated a much higher risk potential for terrorist attacks as compared to natural hazards. Jenelius et al. [33] also utilized game theory in estimating the terrorism risk to CIs and devising protection strategies, but based their calculations on an assumption that the attackers may not have complete information about their targets. As a result of this change in approach, the authors identified a protective strategy that differed markedly from those developed under Brown et al.’s complete information assumption. This review elucidates that the probability of terrorist attacks on critical infrastructures is a significant source of risk that is becoming significantly larger than that of natural events, and it is affected by factors such as the vulnerability of the CI, protection of the CI, visibility of the CI, the consequences of an event, the capabilities of the attacker, and the history of attacks. The review indicates that reducing the likelihood of an attack and improving deterrence can be achieved by higher robustness (increasing the cost of an attack) and higher resilience (reducing the consequences of an attack).

Measuring the consequences of terrorist attacks for certain infrastructure components can also differ strongly based on the nature of the components selected for analysis. In prior research on the vulnerability of power-supply systems, the functionality status of each component—which are generally speaking either busses or transmission lines—has usually been expressed as a binary parameter: either working or failed [34,35]. On the other hand, components with more distinctive characteristics in relatively more complex infrastructures may require more detailed analysis that considers the type of attack, a wider range of component types, and progressive deterioration in the condition of some or all components that may result from multiple stages of an attack. For instance, in their study of a bomb attack on an airport, Mueller and Stewart [6] analyzed the impact of the position of the attack and the severity of the explosion when modeling the potential risk.

2.3. Game Theory and Terrorism Risk Assessment in Critical Infrastructures

There is increasing research using game theory as a decision tool in counterterrorism risk assessment and management. This paragraph reviews game-theoretic models focused on the optimization of protective strategies in critical facilities using game-theoretic models. Cox [36] reviewed the problem of vulnerability of critical facilities to terrorist attacks with a focus on the probability of attack. The review proposed four alternative techniques: decision tree analysis, probabilistic activity AND-OR networks, project planning models of terrorist attacks, and hierarchical optimization. Regardless of which technical alternatives are used, treating attackers as intelligent opportunists, rather than as random-variable decision makers, appears promising for reliable prediction of the probability of event. The research concluded that focusing the resilience of critical infrastructures on optimizing protective solutions, assuming that attackers will then optimize their strategies accordingly, is a promising topic. However, this approach does not consider the information known to the attackers that can affect their strategy.

Bier and Kosanoglu [37] developed a model of attacker deterrence using target-oriented utility theory—Weibull, Rayleigh, and Exponential functions were used to express the protective investment as a function of loss due to successful attack. The results provide the optimal levels of investment in protective structures, taking into account the possibility of deterring an attack. Cost-effective protective solutions contribute to optimal allocation of resources (less investment in protective solution) or by improving protection when the cost effectiveness of defense is low. Critical facilities with higher priorities will receive supplementary protective resources, causing attackers to consider lower value targets. The model presumes that in well-protected critical facilities, few, if any, successful attacks will be on large targets, and more events on small targets—this was observed in Israel during the period of 2000–2012.

A multimodal game-theoretic model for the allocation of protective strategies to allocate security resources within a chemical supply chain with different transport modes was developed by Talarico et al. [38]. For a limited number of protective strategies, the model yields the adoption of strategies that can balance the adversary efforts. The latter can force the attacker to increase the attack; or to reduce the attack, if no strategy is profitable. The latter stresses the need for optimal solutions at the single facility as a measure to optimize the protection of critical facilities.

Feng et al. [39] developed a game theory based on the Nash equilibrium with complete information, static and a zero-sum game. The method was developed and implemented for optimizing the allocation of limited defensive resources to mitigate terrorism risk on multiple chemical plants. A case study to test the applicability and reliability of the method tested eight chemical explosive storage materials plants in China. Chemical plants with high initial intrinsic risks received priority of limited protective resources, and their initial intrinsic risks could be mitigated to the same level; the level depends on the total amount of defense resources. In contrast, plants with low initial intrinsic risks received no additional protective resources, and their initial intrinsic risks remained the same. The main deficiency in this model is a lack of analysis of the optimal allocation at the single plant level. Hausken and He [40] developed a game-theoretic model for the protection of N targets with given inherent protection against terrorist threats with a given initial strategy. The threat payout in this model considers the protection level and investment; however, it does not consider the fatalities, injuries and direct as well as indirect loss.

Napolitano et al. [41] developed a threats and security analysis model for critical infrastructure protection. A payout function is composed of four key factors: deterrence measures index, the number of fatalities, number if injured, and the level of economic loss. This model is highly dependent on the optimal design of protective solution. Jaspersen and Montibeller [42] developed a behavioral model predicting terrorists' objectives as a stochastic learning process using a reinforced learning process. The model was implemented on a sample of business, military, governmental, private and infrastructure facilities. The model showed that terrorist behavior is adaptive to the target environment at an early stage of life, and less adaptive as infrastructure activities continue over time. The latter means that protective activities should be adapted to the changing surrounding environment. The model was implemented to predict the attacks by Liberation Tigers of Tamil Eelam (LTTE) in their active time of operation after 2004 and was found to predict the probabilities of attacks at levels between 0–0.6. This model indicates the need for optimal protective strategy at the single facility as a key step to keep costs of mitigation under budget constraints.

This review emphasizes the importance of the optimal design of protective strategy at the single-level facility as a core component of the establishment of comprehensive protective strategy. The review further stresses the need to reduce the payoff function of the attackers as a means of attack deterrence.

3. Methodology

3.1. Analysis Framework

A follow chart of the framework for analyzing terrorism risk and devising an optimized protection strategy is shown in Figure 1. As previously mentioned, one of the major challenges associated with modeling terrorist attacks is that they do not typically have a substantial occurrence frequency or location. Rather, the choice of a CI target by terrorists is likely to be the dynamic result of a series of calculations including but not limited to the protection level of that target, its significance as a critical infrastructure, the protection levels of other potential targets, the consequences of a successful attack, and the capabilities of the attacker [30]. We proceed from an assumption that the process of choosing an attack method and target is focused on maximizing the total consequence of the attack. Game theory is then utilized to identify the optimal protection strategy based on the attacking behavior. Infrastructure is treated as a network system including various functioning components, and the consequence of the attack, defined in terms of loss of functionality, will be investigated utilizing topological methodologies that take account of the interdependencies between these components.

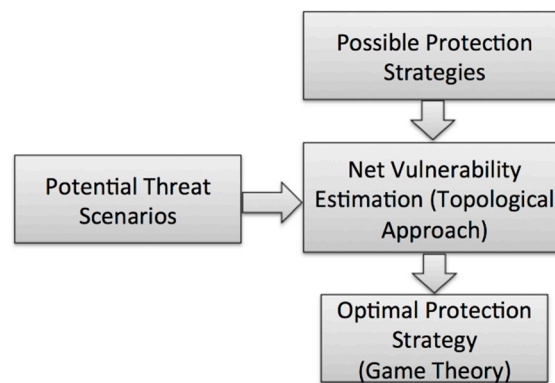


Figure 1. Protection Strategy Analysis Framework.

3.2. Critical Infrastructure Modeling

The CIs being investigated are modeled as a connected graph, in which each functioning component is considered as a node in the network, while the relationships between components in the network are defined as edges. For a network G , we define the set of nodes as V , within which each node is defined as v_i ($i = 1, \dots, n$), and the set of edges as E , where each edge is defined as e_j ($j = 1, \dots, m$). In complex network theory, for any damage D that occurs to the network G , the functionality of the network confronting this interference can be expressed as:

$$V(G, D) = \frac{\Phi(G) - \Phi(D(G))}{\Phi(G)} \tag{1}$$

where $\Phi(G)$ is defined as the betweenness of network G , and is calculated as:

$$\Phi(G) = \frac{1}{n(n-1)} \sum_{j=1}^m \frac{1}{r_j} \tag{2}$$

where (r_j) is the level of resistance in the system on edge e_j as compared to full connection. In network theory, the level of betweenness also represents the global efficiency of the network system, while the vulnerability of the network is conceived as the level of reduction in global efficiency arising from the failure of nodes and/or edges in the network [22].

Following on from the above definitions, terrorist attacks can affect the functionality of the system in two ways. First, when a functioning component (v_i) of the critical infrastructure becomes damaged,

the level of resistance of the connections in all edges that are linked to the damaged component will increase. Second, by damaging a particular connecting edge (e_j), the level of resistance to the connectivity of the damaged edge can increase. In both cases, a decrease in functionality in the whole system will occur.

For each attack strategy a_k on the critical infrastructure, the resistance level of the edges being interfered with will change; the post-attack resistance level can therefore be defined as $r_j(a_k)$. However, the changes in resistance due to attack a_k are also influenced by protective actions p_l , so the post-attack robustness level in light of such actions is expressed as $r_j(a_k, p_l)$. Thus, the vulnerability of the infrastructure given protective actions p_l and attack a_k can be calculated from Equations (1) and (2).

3.3. Terrorist Attack Loss Modeling

For each terrorist attack against a given infrastructure, losses can be divided into two major types: direct loss, which is estimated based on the cost of repairing damaged equipment and treating injured people before the infrastructure returns to its normal condition; and indirect loss, estimated based on the net economic interruption caused by the target's lack of functionality.

3.3.1. Direct Loss Estimation

For a given component i , the direct loss $L_i^D(a_k, p_l)$ caused by attack strategy a_k as mitigated by protection strategy p_l is calculated as:

$$L_i^D(a_k, p_l) = L_i^T \cdot \eta_i(a_k, p_l) \tag{3}$$

where L_i^T is the total value of the component i , and $\eta_i(a_k, p_l)$ is the level of damage to component i based on the given attack strategy a_k and protection strategy p_l .

3.3.2. Indirect Loss Estimation

The level of functionality of an infrastructure system in the wake of a terrorist attack can be conceived of as the $V(G, D)$ of the infrastructure, where $D(a_k, p_l)$ expresses the effects of attack strategy a_k and protection strategy p_l . The indirect loss based on the loss of functionality L^I of the infrastructure is calculated as:

$$L^I = L^V \cdot (1 - V(G, D)) \tag{4}$$

where L^V is the total value the infrastructure should provide during the repair period if no damage occurred.

Thus, the total loss $L(a_k, p_l)$ caused by terrorist attack a_k for the infrastructure under protection strategy p_l can be modeled as:

$$L = \sum_i L_i^D + L^I \tag{5}$$

4. Strategy Analysis

Optimizing Protection Strategy Using Game Theory

In the game-theory phase of our analysis, we assume that both defenders and attackers have full knowledge of the critical infrastructure. The protection process is modeled as a zero-sum game, which means that while the defenders try to minimize the potential loss L after the attack, the attackers aim to maximize L by allocating limited resources. Given budget constraints for protection and attack of Bg_P and Bg_A , respectively, the problem can be modeled as shown in Equation (6), and the protection strategy P calculated from this model will be the most effective one in light of the budgets available.

$$\min_P \max_A L(p_l, a_k) \tag{6}$$

$$s.t. C_{p_l} \leq Bg_P \ \& \ C_{a_k} \leq Bg_A \quad (7)$$

The strategies used by each of the parties involved are evaluated based on their effectiveness and costs. For attackers, the set of attacking methods a_k is defined as A ; each attacking method a_k includes both the equipment used and the attack's position/direction; and the cost of conducting a_k is defined as C_{a_k} .

For defenders, the set of protection strategies p_l is defined as P , with each strategy p_l comprising the target and the specific method used in protecting it, resulting in a cost for conducting p_l defined as C_{p_l} . Specifically, two protection methods for each of the components in the infrastructure were considered. The first consists of improving the robustness of certain components, e.g., by building concrete walls or shelters surrounding the component that will tend to reduce the level of damage to the component if an attack occurs. When a particular robustness level Ro_l is added to the target component of the infrastructure, a damage reduction factor ΔRo_l will be applied to the original attack consequence associated with that component, and reduces the level of damage to related edges in the attack so that the potential loss $L(p_l, a_k)$ can be reduced.

The second protection method consists of improving redundancy, meaning that the given infrastructural component will be replicated, for the specific purpose of allowing that component to maintain functionality despite being damaged in an attack. When a certain level of redundancy Re_l is applied to a target component, the damage to that target component within the redundancy level will have only minor (ignorable) consequences to its functionality, and also maintain its level of reliance to the other relative components in the network during the attack, resulting in a reduction in total potential loss $L(p_l, a_k)$.

5. Case Study

As previously discussed, our methodology was tested using the case of an electric substation in Israel. The power-plant systems in the research region are widely dispersed and exposed to terror events, while an increasing local demand for electricity—combined with lack of access to backup power from neighboring countries—has created an urgent need for an effective protection strategy for this critical infrastructure. The case substation has been deemed a First Degree Strategic Facility by the Israel government, being the main and almost only electric power supplier to this region, and it is under constant terror threat in the form of steep-path shooting with projectiles containing up to 20 kg of TNT each [9].

5.1. Substation Network Modeling

The electric substation in this case study can be conceived of as divided into nine interrelated components, joined by eight connecting edges, as shown in Figure 2. The nine components are: (A) current transformers, (B) power transformers, (C) insulators, (D) earthing systems, (E) isolation switches, (F) circuit breakers, (G) surge arrestors, (H) distribution busses and (I) the control building. Each of these components, with the exception of the control building, consists of several identical functioning units, the number of which and the number of parallel transmission lines in each connecting edge are set forth in Table 1.

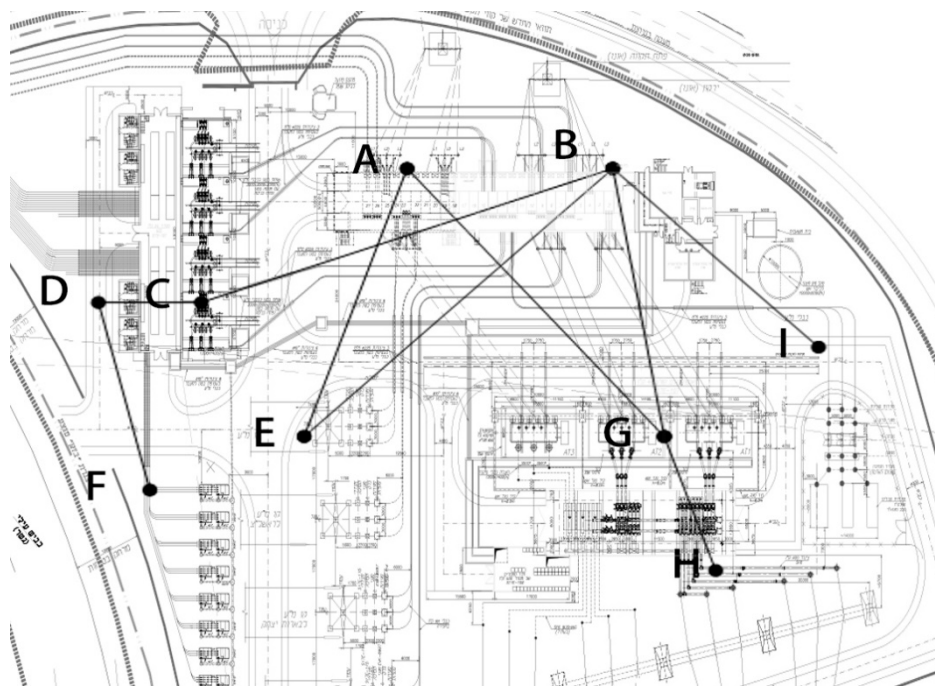


Figure 2. Network Model of Electric Substation.

Table 1. Electric Substation Functioning Unit Layout (according to site layout map).

Component Type	Number of Functioning Units
A	10
B	17
C	4
D	4
E	4
F	8
G	3
H	2
I	1
Connecting Edge	Number of Transmission Lines
AE	2
AG	1
BC	4
BE	2
BG	2
BI	1
CD	2
DF	1
GH	2

5.2. Terrorist Attack Damage Estimation

5.2.1. Attacking Weapon Used

Historically, weapons used in terrorist attacks on the substation case have been TNT explosives weighing not more than 20 kg. For the purposes of this analysis, we assumed that each new attack would utilize the same type and maximum historical size of projectile. Uncertainty in the explosive weight affects the model results by the scaled distance expressed by [43]:

$$Z = R/W^{1/3} \tag{8}$$

where Z is the scaled distance, R is the stand-off distance [m], and W is the weight of the charge [kg].

Thus, the threshold distance at which the structures will suffer severe damage varies linearly with the scaled distance Z .

5.2.2. Estimating Damage

In Kingery-Bulmash equations, the measuring criterion for damage is known as level incident overpressure under explosion, which can be calculated based on the weight of TNT explosives and the distance to the explosion’s center [44]. According to the explosive blast study conducted by the U.S. Federal Emergency Management Agency [45], the level of overpressure that causes severe damage to metal structures, and which therefore affects the functionality of the substation components, is 7 psi. Given the case-study projectile size, the threshold radius for explosive damage affecting component functionality is approximately 12 m. Calculated from the data above, Table 2 lists the number of functioning units and transmission lines that are predicted to fail after each attack. The threshold distance is subject to uncertainty in the charge weight and may be reduced up to 10.5 and 8.8 m in case of larger explosive warhead of 30 and 50 kg TNT, respectively. Larger scenarios will require increased protection of the facility at the direct vicinity of the substation.

Table 2. Failure of Substation Units under Terrorist Attack.

Component Type	Number of Failed Units
A	10
B	10
C	2
D	2
E	1
F	4
G	1
H	1
I	1
Connecting Edge	Number of Failed Transmission Lines
AE	2
AG	1
BC	2
BE	2
BG	2
BI	1
CD	1
DF	1
GH	1

5.3. Terrorist Attack Loss Estimation

5.3.1. Direct Loss Estimation

Table 3 presents the total estimated potential loss to the same substation’s equipment and staff, according to expert estimation.

Table 3. Total Direct Loss to Substation.

Loss Factor	Amount of Loss (N.I.S.)
Damage to Equipment and Facility	11,000,000 (2,773,613 USD)
Casualties	19,803,000 (5,000,000 USD)
Total Direct Loss	30,803,000 (7,773,613 USD)

5.3.2. Indirect Loss Estimation

The repair times and costs for this substation, as determined by expert estimation, are set forth in Table 4.

Table 4. Total Indirect Loss to Substation.

Loss Causing Factor	Quantity
Total indirect loss of the substation	25,000 N.I.S./h (6,304 USD/h)
Interruption to the power-supply network	75,000 N.I.S./h (18,911 USD/h)
Estimated time to recovery	10 d
Total indirect loss	24,000,000 N.I.S. (6,059,688 USD)

5.4. Protection Method Specifications

5.4.1. Improving Substation Component Robustness

Based on past research on this substation [30], five levels of protection aimed at improving the robustness of the substation have been proposed and are listed in Table 5 below. The effectiveness of each protection method is also provided, expressed as the percentage by which terror attack damage to a given component would be reduced if this type of protection were provided.

Table 5. Protection Methods for Improving Robustness.

Level of Protection	Protective Solution	Effectiveness (ΔRo_I)
I	Steel construction	99%
II	Reinforced concrete construction	90%
III	Burial of critical components	65%
IV	Partitioning reinforced concrete walls	55%
V	Secured space	35%

The costs of providing each level of protection to the whole substation were calculated in prior research [29], as 350,000 N.I.S. for complete Level V protection, 650,000 N.I.S. for Level IV protection, 1 million N.I.S. for Level III protection, 1.5 million N.I.S. for Level II protection, and 3 million N.I.S. for Level I protection. In the present research, the estimated costs for each level of protection have been further refined based on the amount of equipment requiring protection.

5.4.2. Improving Substation Component Redundancy

The level of redundancy for the substation is considered to be a continuous parameter between 0 and 1, with 0 representing no redundancy and 1 representing full redundancy. The amount of direct loss from a terrorist attack is not affected by improvement in redundancy, since explosions are still expected to result in the same amount or slightly more of damage and casualties to the substation as they would if no redundant systems were provided. On the other hand, redundancy has the potential to entirely prevent indirect loss, i.e., in cases where the percentage of failed units does not exceed the level of redundancy to the component. The estimated costs of providing redundancy to the substation have been adopted from previous research on the substation by Elkabets and Shohet [9].

5.5. Protection Strategy Analysis

As illustrated in the Methodology section, our analyses of protective strategies were conducted using a network-assisted game-theory approach, and considered protection methodologies aimed at improving both the redundancy and robustness of the substation under varied terrorist attack threats from TNT explosives of 10 to 20 kg. The losses presented here are based on an assumption that both the critical infrastructure defenders and the attackers are using optimized strategies; as such, the losses from real attacks may be lower than these projections.

5.5.1. Protection Strategy Analysis: Improving Robustness

The optimized protection strategy for improving the robustness of the substation on a component-by-component basis is presented in Table 6, below. A mixed strategy of protection allocation to each of the components in the substation is also included, under the assumption that the protection budget will only cover for one full protection for one component in the infrastructure.

Table 6. Protection Strategy Arrangements Aimed at Improving Robustness

Level of Protection	Protection Allocation to Each Component									Expected Total Loss (N.I.S.)	Percentage Reduction in Loss	
	A	B	C	D	E	F	G	H	I			
None	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	14,291,300	0%
I	0.42	0.58	0	0	0	0	0	0	0	0	6,153,747	59%
II	0.41	0.59	0	0	0	0	0	0	0	0	6,702,103	53%
III	0.35	0.65	0	0	0	0	0	0	0	0	8,103,435	43%
IV	0.31	0.69	0	0	0	0	0	0	0	0	8,834,589	38%
V	0.15	0.85	0	0	0	0	0	0	0	0	10,053,180	30%

It should be noted that components A and B are the most vulnerable components in the critical infrastructure system. The high value of these two components can be inferred from the large number of other components that are supported by one or both of them, as well as their relatively compact size, which renders it easier for a single attack on these components to result in high levels of damage. It also worth noting that, when the overall level of protection is reduced, a higher proportion of protection is required for component B; this indicates the paramount importance of protecting component B when seeking to reduce losses from terrorist attacks, especially under restrictive budgetary conditions.

We calculated the return of investment (ROI) associated with the installation of each level of protection confronting a 20 kg TNT attack under a game-theory assumption—the ROI is calculated based on an estimated lifespan of 20 years for the infrastructure with a successful terrorist attack occurring rate of 5.78% annually (General Security Service, 2015). ROI is the Internal Rate of Return of each alternative, where the investment is the cost of the protection alternative and the return is the reduction in the risk assessment in present value. The lowest-budget loss reduction, which is defined as the expected amount by which losses are reduced (ΔL) at the baseline protection budget B_{gp} (a protection investment of 105,000 N.I.S according to expert estimation), is presented along with the protection ROI in Figure 3.

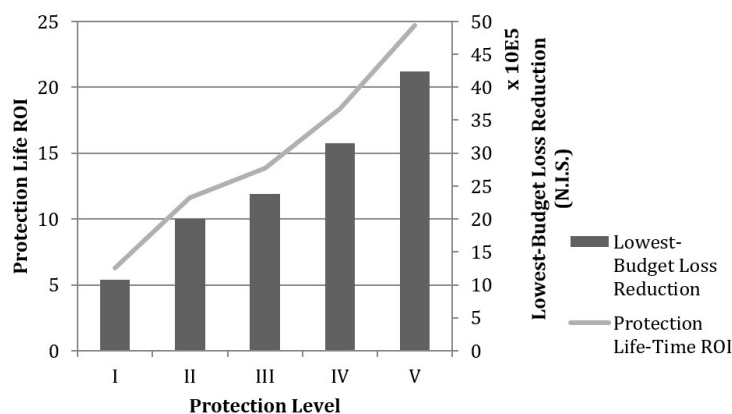


Figure 3. Comparison of ROI between Alternative Protection Levels.

It is clear from Figure 3 that the cost effectiveness of protection methods decreases when installing higher levels of protections. To achieve the most cost-effective protection strategy, lower levels of protection methods should be applied specifically to (in order of importance) components B and A.

Analysis of protective arrangements in response to less severe attacking strategies, i.e., using TNT projectiles as small as 5 kg, was conducted using the same methodology described above. We found that

the most cost-effective strategy for each case was still Level V protection, and the optimized allocation of protection to each component is listed in Table 7. Our estimates for the ROI and loss-reduction proportion for each type of attack and protection method are also presented in Figure 4.

Table 7. Robustness Improvement Strategy for Varied Attacking Scenarios (Protection Level V).

Intensity of Terrorist Attack (kg TNT)	Protection Allocation to Each Component								
	A	B	C	D	E	F	G	H	I
5	0.15	0.85	0	0	0	0	0	0	0
7.5	0.15	0.85	0	0	0	0	0	0	0
10	0.15	0.85	0	0	0	0	0	0	0
12.5	0.15	0.85	0	0	0	0	0	0	0
15	0.15	0.85	0	0	0	0	0	0	0
20	0.15	0.86	0	0	0	0	0	0	0

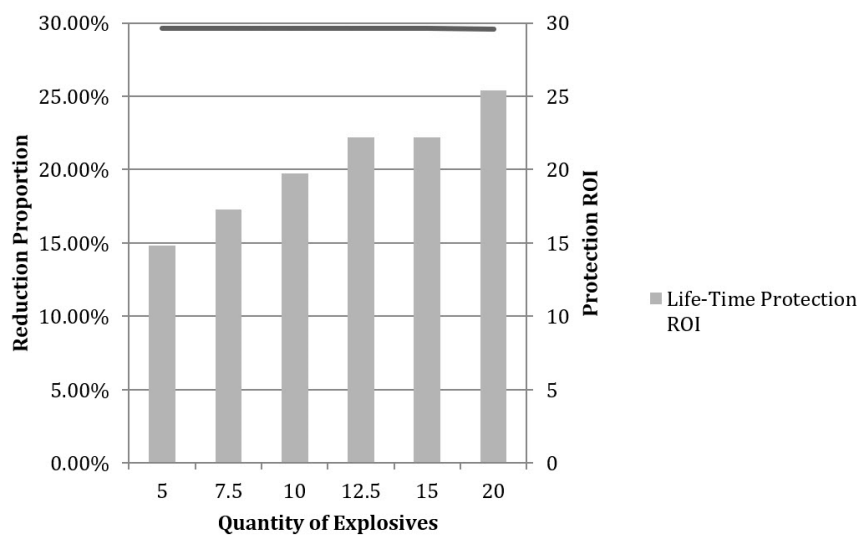


Figure 4. Effectiveness of Protection at Varied Attack Levels.

It can be seen that the optimized protection strategy is not sensitive to the quantity of explosives used in the terrorist attack, with the effectiveness of protection remaining within a very narrow range of approximately 30% of loss reduction. As the strength of attack increases, the ROI of the protection method increases from 23 to 40 due to greater damage reduction. Thus, it is reasonable to consider that Level V protection, as presented in Table 6, is the optimized robustness-improvement strategy, with highest cost efficiency, in response to the terrorist attacks on the substation that are most likely to occur.

5.5.2. Protection Strategy: Improving Redundancy

Our analysis of the optimized protection strategy based on redundancy was conducted assuming that the same amount of budget is used for each protection strategy as installing the Level I protection method. The result suggests that a mixed strategy of providing 64% redundancy to component B and 36% redundancy to component A would be optimal, resulting in a total loss of 8,884,618 N.I.S. after a given terrorist attack using 20 kg of TNT. These improvements to the redundancy of these two key substation components would reduce the total loss from such an attack by 38%. However, it should be remembered that the loss reduction associated with a robustness-improvement strategy at the same level of investment could be as high as 56%. The ROI for redundancy improvement is presented below in Figure 5, alongside robustness-improvement methods.

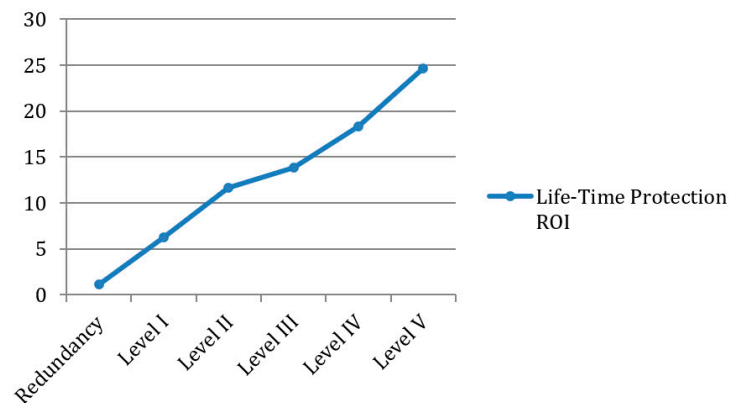


Figure 5. Comparison of ROI between Protection Methodologies.

It is clear that, compared to improving robustness, improving redundancy has a much lower effectiveness in improving infrastructural resilience to terrorist attacks. This may result from the fact that redundancy improvements do not reduce (and may slightly increase) losses from damaged facility equipment and injured staff during terrorist attacks, which together represent a large proportion of total losses caused (79% in this case study). Therefore, full redundancy of the entire substation was not considered in this case, but may be considered in CIs with significantly higher importance and indirect loss.

6. Conclusions

A zero-sum complete information game-theory methodology for the protection of CI was developed. The novelty of the model focuses on integration between the vulnerability of the CIs using topological network analysis, various threat scenarios, and comprehensive consequences considering direct and indirect loss. The cost effectiveness of the optimal solution considers ROI along the lifetime of the CI. Topological network analysis provides an effective tool for identifying the cascading effects and resilience of the CIs particularly in electric power stations. The limitation of topological network analysis in considering physical parameters and capacity of the components is complemented in the methodology by the vulnerability analysis. The results of the case study strongly suggest that, when only terrorist attacks are considered, protective strategies aimed at improving the robustness of CI have a much higher effectiveness and efficiency than those aimed at improving CI redundancy. Nevertheless, in CIs with lower direct loss and high indirect loss and importance, full redundancy should also be considered. Moreover, components with more connections to other components tend to be designed in a compact, space-efficient manner that may unintentionally result in their higher vulnerability to potential attacks, and demand higher priority in protection strategy. In other words, it can be inferred that a relatively loose arrangement of the critical components of the infrastructure could help to decrease its overall vulnerability to physical attacks. Particularly, in this case, an overcompact arrangement of the cardinal components may be responsible for the fact that reductions in the severity of a given attack scenario did *not* translate into reductions in the severity of damage to essential components.

As most research in CI protections focuses on the macro scale, such as the interaction of multiple infrastructures or even multiple systems, this paper has provided a potential approach to protection strategy analysis within a relative micro scale, considering the complexity of the interdependencies between the components of the critical infrastructure. The methodology proposed makes it possible to optimize the investment to critical infrastructure protections at lower levels, which can help to reduce expenditures on local infrastructure protection or on a single critical infrastructure for small projects. This paper also provides a complementary method to estimating terrorism risk. As research has been conducted on the changing occurrence of terrorist attacks over time [46], this research provides a

possible approach to estimating the occurrence of terrorist attacks in space, specifically within the infrastructure, with the help of network modeling based on the connectivity within the infrastructure.

In future research, it would be useful to include a wider variety of protection methods as well as possible response operations (e.g., buried in an underground cavern [47]) in order to present a more accurate estimation of potential damage and optimal protection strategies. The sensitivity of the methodology to various potential attack strategies can also be further developed through the examination of additional cases with diverse arrangements of functioning components.

Author Contributions: Conceptualization, H.-H.W., I.M.S., and M.J.S.; methodology, X.Y.; formal analysis, X.Y.; data curation, I.M.S.; writing—original draft preparation, X.Y.; writing—review and editing, H.-H.W.; visualization, X.Y.; supervision, I.M.S. and M.J.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

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

References

1. Mifflin, H. *The American Heritage Dictionary*; Turtleback School & Library Binding: San Diego, CA, USA, 2001.
2. Moteff, J.; Parfomak, P. *Critical Infrastructure and Key Assets: Definition and Identification*; The Library of Congress, Congressional Research Service: Washington, DC, USA, 2004.
3. O'Rourke, T.D. *Critical Infrastructure, Interdependencies, and Resilience*; National Emergency Training Center: Emmitsburg, MD, USA, 2007.
4. Zimmerman, R. Social implications of infrastructure network interactions. *J. Urban Technol.* **2001**, *8*, 97–119. [[CrossRef](#)]
5. Minkel, J.R. The 2003 Northeast Blackout—Five years later. *Scientific American*, 13 August 2008.
6. Mueller, J.; Stewart, M.G. *Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Homeland Security*; Oxford University Press: Oxford, UK, 2011.
7. IEP. *2014 Global Terrorism Index Report—Vision of Humanity*; Institute of Economics & Peace (IEP): Sydney, Australia, 2014.
8. University of Maryland. *Global Terrorism Database*; University of Maryland: College Park, MD, USA, 2014.
9. Elkabets, S.M.; Shohet, I.M. “Triple R”—A quantitative model for critical infrastructures to withstand extreme events. In Proceedings of the Creative Construction Conference, Prague, Czech Republic, 21–24 June 2014.
10. Rinaldi, S.M.; Peerenboom, J.P.; Kelly, T.K. Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Syst. Mag.* **2001**, *21*, 11–25.
11. Dudenhofer, D.D.; Permann, M.R.; Manic, M. CIMS: A framework for infrastructure interdependency modeling and analysis. In Proceedings of the 2006 Winter Simulation Conference, Monterey, CA, USA, 3–6 December 2006; pp. 478–485.
12. Yusta, J.M.; Correa, G.J.; Lacal-Arántegui, R. Methodologies and applications for critical infrastructure protection: State-of-the-art. *Energy Policy* **2011**, *39*, 6100–6119. [[CrossRef](#)]
13. Haimes, Y.Y. Systems-based guiding principles for risk modeling, planning, assessment, management, and communication. *Risk Anal. Int. J.* **2012**, *32*, 1451–1467. [[CrossRef](#)] [[PubMed](#)]
14. Eusgeld, I.; Nan, C.; Dietz, S. “System-of-systems” approach for interdependent critical infrastructures. *Reliab. Eng. Syst. Saf.* **2011**, *96*, 679–686. [[CrossRef](#)]
15. Trucco, P.; Cagno, E.; De Ambroggi, M. Dynamic functional modelling of vulnerability and interoperability of Critical Infrastructures. *Reliab. Eng. Syst. Saf.* **2012**, *105*, 51–63. [[CrossRef](#)]
16. Oh, E.H.; Deshmukh, A.; Hastak, M. Disaster impact analysis based on inter-relationship of critical infrastructure and associated industries. *Int. J. Disaster Resil. Built Environ.* **2010**. [[CrossRef](#)]
17. White, T.; Ariaratnam, S.T.; Michael, J. Subterranean infrastructure reconnaissance for manmade and natural hazards and disasters. *Int. J. Disaster Resil. Built Environ.* **2012**. [[CrossRef](#)]
18. McEntire, D.; Crocker, C.G.; Peters, E. Addressing vulnerability through an integrated approach. *Int. J. Disaster Resil. Built Environ.* **2010**. [[CrossRef](#)]
19. Min, H.-S.J.; Beyeler, W.; Brown, T.; Son, Y.J.; Jones, A.T. Toward modeling and simulation of critical national infrastructure interdependencies. *IIE Trans.* **2007**, *39*, 57–71. [[CrossRef](#)]

20. Rehan, R.; Unger, A.J.; Knight, M.A.; Haas, C.T. Financially sustainable management strategies for urban wastewater collection infrastructure—Implementation of a system dynamics model. *Tunn. Undergr. Space Technol.* **2014**, *39*, 102–115. [[CrossRef](#)]
21. Cavallini, S.; D'Alessandro, C.; Volpe, M.; Armenia, S.; Carlini, C.; Brein, E.; Assogna, P. A system dynamics framework for modeling critical infrastructure resilience. In Proceedings of the International Conference on Critical Infrastructure Protection, Arlington, VA, USA, 17–19 March 2014; pp. 141–154.
22. Bompard, E.; Wu, D.; Xue, F. Structural vulnerability of power systems: A topological approach. *Electr. Power Syst. Res.* **2011**, *81*, 1334–1340. [[CrossRef](#)]
23. Wang, S.; Hong, L.; Ouyang, M.; Zhang, J.; Chen, X. Vulnerability analysis of interdependent infrastructure systems under edge attack strategies. *Saf. Sci.* **2013**, *51*, 328–337. [[CrossRef](#)]
24. Hines, P.; Cotilla-Sanchez, E.; Blumsack, S. Do topological models provide good information about electricity infrastructure vulnerability? *Chaos Interdiscip. J. Nonlinear Sci.* **2010**, *20*, 033122. [[CrossRef](#)]
25. Bentes, I.; Afonso, L.; Varum, H.; Pinto, J.; Varajão, J.; Duarte, A.; Agarwal, J. A new tool to assess water pipe networks vulnerability and robustness. *Eng. Fail. Anal.* **2011**, *18*, 1637–1644. [[CrossRef](#)]
26. Bono, F.; Gutiérrez, E. A network-based analysis of the impact of structural damage on urban accessibility following a disaster: The case of the seismically damaged Port Au Prince and Carrefour urban road networks. *J. Transp. Geogr.* **2011**, *19*, 1443–1455. [[CrossRef](#)]
27. Wang, S.; Hong, L.; Chen, X. Vulnerability analysis of interdependent infrastructure systems: A methodological framework. *Phys. A Stat. Mech. Appl.* **2012**, *391*, 3323–3335. [[CrossRef](#)]
28. Mousavizadeha, S.; Ghanizadeh Bolandi, T.; Haghifama, M.R.; Moghimic, M.; Luc, J. Resiliency analysis of electric distribution networks: A new approach based on modularity concept. *Electr. Power Syst. Res.* **2020**, *117*, 105669. [[CrossRef](#)]
29. Federation of American Scientists. *Al Qaeda Training Manual*; Federation of American Scientists: Washington, DC, USA, 2006.
30. Elkabets, S.M.; Shohet, I.M. Resilience Modeling (TRA) for critical infrastructures to withstand extreme events-sensitivity analyses. In Proceedings of the Creative Construction Conference, Krakow, Poland, 21–24 June 2015.
31. Brown, G.G.; Carlyle, W.M.; Salmeron, J.; Wood, K. Analyzing the vulnerability of critical infrastructure to attack and planning defenses. In *Emerging Theory, Methods, and Applications*; Informs: Catonsville, MD, USA, 2005; pp. 102–123.
32. Brown, G.; Carlyle, M.; Salmerón, J.; Wood, K. Defending critical infrastructure. *Interfaces* **2006**, *36*, 530–544. [[CrossRef](#)]
33. Jenelius, E.; Westin, J.; Holmgren, Å.J. Critical infrastructure protection under imperfect attacker perception. *Int. J. Crit. Infrastruct. Prot.* **2010**, *3*, 16–26. [[CrossRef](#)]
34. Dwivedi, A.; Yu, X. A maximum-flow-based complex network approach for power system vulnerability analysis. *IEEE Trans. Ind. Inform.* **2011**, *9*, 81–88. [[CrossRef](#)]
35. Schneider, C.M.; Moreira, A.A.; Andrade, J.S.; Havlin, S.; Herrmann, H.J. Mitigation of malicious attacks on networks. *Proc. Natl. Acad. Sci. USA* **2011**, *108*, 3838–3841. [[CrossRef](#)]
36. Cox, L.A., Jr. Some Limitations of “Risk = Threat × Vulnerability × Consequence” for Risk Analysis of Terrorist Attacks. *Risk Anal.* **2008**, *28*, 1749–1761. [[CrossRef](#)] [[PubMed](#)]
37. Bier, V.M.; Kosanoglu, F. Target-oriented utility theory for modeling the deterrent effects of counterterrorism. *Reliab. Eng. Syst. Saf.* **2015**, *136*, 35–46. [[CrossRef](#)]
38. Talarico, L.; Reniers, G.; Sörensen, K.; Springael, J. MISTRAL: A game-theoretical model to allocate security measures in a multi-modal chemical transportation network with adaptive adversaries. *Reliab. Eng. Syst. Saf.* **2015**, *138*, 105–114. [[CrossRef](#)]
39. Feng, Q.; Cai, H.; Chen, Z.; Zhao, X.; Chen, Y. Using game theory to optimize allocation of defensive resources to protect multiple chemical facilities in a city against terrorist attacks. *J. Loss Prev. Process Ind.* **2016**, *43*, 614–628. [[CrossRef](#)]
40. Hausken, K.; He, F. On the Effectiveness of Security Countermeasures for Critical Infrastructures. *Risk Anal.* **2016**, *36*, 711–726. [[CrossRef](#)]

41. Napolitano, P.; Rossi, G.; Lombardi, M.; Garzia, F.; Ilariucci, M.; Forino, G. Threats Analysis and Security Analysis for Critical Infrastructures: Risk Analysis vs. Game Theory. In Proceedings of the IEEE 2018 International Carnahan Conference on Security Technology, Montreal, QC, Canada, 22–25 October 2018; pp. 1–5. [[CrossRef](#)]
42. Jaspersen, J.G.; Montibeller, G. On the learning patterns and adaptive behavior of terrorist organizations. *Eur. J. Oper. Res.* **2020**, *282*, 221–234. [[CrossRef](#)]
43. Jeon, D.; Kim, K.; Han, S. Modified equation of shock wave parameters. *Computation* **2017**, *5*, 41. [[CrossRef](#)]
44. Remennikov, A.M. A review of methods for predicting bomb blast effects on buildings. *J. Battlef. Technol.* **2003**, *6*, 5.
45. Federal Emergency Management Agency. *Risk Management Series: Primer to Design Safe School Projects in Case of Terrorist Attacks*; Federal Emergency Management Agency: Washington, DC, USA, 2003.
46. Haimes, Y.Y. On the complex quantification of risk: Systems-based perspective on terrorism. *Risk Anal.* **2011**, *31*, 1175–1186. [[CrossRef](#)] [[PubMed](#)]
47. Shohet, I.M.; Elkabets, S.M.; Ornai, D.; Kivity, Y.; Gilad, E.; Levy, R.; Shany, G.; Levi-Tzedek, M.; Tavron, B.; Ben-Dor, G. A methodology for risk assessment and management for nuclear power plant SMR hit by high explosive warheads. In Proceedings of the Creative Construction Conference, 28 June–1 July 2020; pp. 50–55. [[CrossRef](#)]

Publisher’s Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).