Eur. Phys. J. Plus (2024) 139:669
https://doi.org/10.1140/epjp/s13360-024-05422-6

THE EUROPEAN
PHYSICAL JOURNAL PLUS

Regular Article

Building risk assessment methodology for explosive and non-conventional terrorist attacks

Marco Carbonelli[1], **Riccardo Quaranta**[5,2,a], **Pasquale Gaudio**[2], **Daniele Di Giovanni**[2,4], **Grace P. Xerri**[2], **Andrea Malizia**[3], **Laura Gratta**[6]

[1] Presidency of the Council of Ministers, Rome, Italy
[2] Department of Industrial Engineering, University of Rome Tor Vergata, Rome, Italy
[3] Department of Biomedicine and Prevention, University of Rome Tor Vergata, Rome, Italy
[4] Unicamillus-Saint Camillus International University of Health Sciences, Rome, Italy
[5] The American University of Rome, Rome, Italy
[6] Italian Risk Management Expert, Rome, Italy

Received: 26 March 2024 / Accepted: 2 July 2024

Abstract An original methodology suitable for the assessment of the risk of a terrorist attack in a given site/building is proposed and illustrated for the case of an explosive or non-conventional (Chemical, Biological, Radiological, Nuclear and explosive—CBRNe) attack. The Building Risk Assessment Methodology discussed in this paper represents the arrival point of a detailed analysis and research carried out during the past 5 years and provides the synthesis of different results obtained for the assessment of Building Threats and Building Vulnerabilities. These two assessments were discussed in detail in other already published papers. The effort presented in this work is to deploy a risk and impact assessment technique for buildings that can be adopted in any operating scenario in the presence of explosive or non-conventional threats. The main target of the methodology is to provide a sufficiently accurate estimate of the risk in a simple fashion. The methodology allows to manage the different kinds of risk related to the explosive and non-conventional threats, and it is useful for identifying a ranking of risks for different buildings in different portions of territory and for prioritizing actions and investments in preparedness, protection and resilience of critical areas and critical infrastructures. In the paper, the results of two different case studies for three different threats will be considered, analyzed and compared.

1 Introduction

Risk assessment is a widely discussed and implemented methodology across various fields of human activities, spanning, for example, from finance to civil protection and personal data protection.

One critical area where risk assessment techniques are vital is the protection of buildings, particularly in reference to terrorist attack scenarios. The events of September 11, 2001, i.e., the attacks to the New York World Trade Center and to the Pentagon also known as 9/11, have significantly increased awareness and stimulated extensive attention to this issue over the past decades. As highlighted by many scholars, this event and its profound impacts and consequences have marked a key shift in the approach of terrorist threats against buildings [1], raising the attention of both the general public and the specialists in this field.

Recent trends in terrorist activities show this shift from targeting exclusively institutional or high-value buildings to an increased frequency of attacks on more accessible targets. In fact, prior to 9/11, terrorist actions were typically logistically complex, often involving hostage situations or mass casualties at high-value sites. However, following the 9/11 events, terrorist strategies evolved toward easier-to-execute attacks, although the lethality of such incidents remains significantly high [2].

It is evident that buildings have begun the preferred targets for terrorists, as they serve as central hubs of a country's economic activity and symbolize its wealth and culture. Thus, safeguarding buildings from terrorist attacks has become a crucial element of the defense strategy adopted by Western countries. This strategy entails a comprehensive approach to building risk assessment, aiming to mitigate vulnerabilities and introduce technical methods and measures fitted for building protection design with the objective of protecting both individuals and properties by enhancing the security of the site's exterior, the building perimeter and its internal functions.

In this paper, a well-established approach to building risk assessment [3] is used, recalling the two foundational methods outlined by the authors in the previous published works: the Building Threat Assessment Method (BTAM) [4] and the Building Vulnerability Assessment Method (BVAM) [5]. Additionally, a method for conducting a Building Exposure Assessment Method (BEAM) is

[a] e-mail: quaranta@ing.uniroma2.it (corresponding author)

Published online: 01 August 2024

Table 1 Characterization of the threats for the considered attacks

Parameter	Type of attack		
	Explosion of a van bomb	Explosion of a suicide belt bomb	Explosion of a Cesium-137 dirty bomb
Type of material or explosive employed	TNT	TNT	TNT and Cesium-137
Type of vector	Van	Belt bomb	Pick-up truck
Maximum amount of the material employed	800 kg	5 kg	400-kg TNT and 90-g Cesium-137
Specific location relative to the structure suitable for the application of the threat	Area of entry for shipping/delivery vehicles	Access part of the building, corresponding to the main entrance	External main parking area of the building

introduced. These three methods are integrated into a comprehensive Building Risk Assessment Methodology (BRAM), which is then applied to two case studies involving different building typologies.

To conduct a complete building risk assessment, the application of this methodology should be assigned to a specialized Assessment Team (AT) [4, 5]. This team should consist of engineers, architects and subject matter experts with the expertise to conduct an accurate analysis of Chemical, Biological, Radiological, Nuclear and explosive (CBRNe) threats. Additionally, the involvement of intelligence experts and direct access to intelligence information could be crucial for accurately estimating the final risk levels, beginning with the assessment of threats, vulnerabilities and exposure levels.

2 Case studies

This study examines three threats proposed in a previous paper of the authors [4]. These threats include the detonation of a suicide belt bomb, the detonation of a van bomb and the detonation of a Cesium-137 Radiation Dispersal Device (RDD), commonly called dirty bomb. This approach follows a similar methodology described in [4, 5], providing a concrete basis for the analysis.

For each selected threat, the AT specified the parameters below:

- Type of material or explosive employed,
- Type of vector for the material or explosive employed,
- Possible maximum amount of the material employed,
- Possible specific location relative to the structure suitable for the application of the threat.

In this paper, the scenarios will be evaluated assuming the absence of wind at the time of the attacks.

Table 1 summarizes all the information assumed by the AT, for the three considered threats.

Two different sites, whose essential characteristics are described in the following sections, will be analyzed as case studies under the abovementioned three attack scenarios: a Shopping Center and a Public Administrative Building in an Italian town.

2.1 Shopping center

The small Shopping Center, built in the late 1980s and lacking significant symbolic value, primarily serves the local neighborhood residents in a prominent town. The Shopping Center is in an area with a park and various private residential constructions, housing approximately 3000 inhabitants within a 0.3-km radius. The average daytime occupancy, including both customers and employees, amounts to 500 individuals. Currently, the building's value is estimated at 5 million euros, with a weekly business turnover of approximately 0.4 million euros.

The Shopping Center does not have a dedicated internal security monitoring and operation center, and the policies for protecting critical and essential services—such as energy, Information and Communication Technology (ICT) and Heating, Ventilation and Air Conditioning (HVAC)—are minimal. The external parking area of the Shopping Center is freely accessible by the public, featuring unprotected air and consumable intake. Vehicles are parked without following any specific security policy. Access to the building is unrestricted for visitors and for suppliers. Furthermore, the majority of shops within the Shopping Center lack a specific business/operation continuity plan.

2.2 Public administrative building

The Public Administrative Building, which was constructed recently and has important architectural value, has an average daytime occupancy of 2000 individuals daily, including public workers, advisors and political figures. The building is in an area with wide streets and public spaces, along with stores and some private residential constructions, resulting in a typical presence of 1500

Table 2 Characterization of the sites

Parameter	Shopping Center	Public Administrative Building
Site visitors	500	2000
Surrounding population (0.3 km)	3000	1500
Building relevance	Low	Very high
Relevance of the occupants	Medium low	Very high
Total economic value	5.4 M euro	53 M euro

individuals within a 0.3-km radius. Currently, the building's value is estimated at 50 million euros, with the surrounding weekly business activity exceeding 3 million euros.

The access area is video-monitored, and the internal security monitoring center operates continuously, supported by specific and updated policies for protecting essential and critical services, such as energy, ICT and HVAC. Furthermore, an updated and comprehensive operational continuity plan is implemented for the building. The external parking area is controlled with access limited to pass holders only. Vehicle parking is prohibited within 50 m of the building. The entry points for air and consumables are fenced, guarded and protected. Strict access control is enforced at the two main entrances, requiring identification for visitors and non-staff personnel, whereas personnel identification and registration are guaranteed by access badges.

A summary of the essential data for evaluating asset attractiveness for both case studies is reported in Table 2.

3 Background

The technical literature presents various definitions of risk [3, 6–10]. In every definition, risk is consistently related to future events and their uncertainties. Supporting this perspective, ISO provided a simple definition of risk as "*the effect of uncertainty on objectives*" [11]. In practical terms, risk is often described as a combination of the consequences of an event and the probability of its occurrence [3, 12, 13]. Therefore, the quantification of risk typically involves multiplying the probability of occurrence of an event by the consequence of its occurrence [6].

Other widely accepted methodologies [14] quantify risk by considering not only the consequences of an event, but rather also the vulnerability and exposure, as described by the following fundamental equation:

$$R = f(T, V, E) \tag{1}$$

For the application of the method presented in this study, the above fundamental quantities Threat Probability (T), Vulnerability (V) and Exposure (E) are defined as follows [14, 15]:

- Threat (T) represents the probability of occurrence of a specific event within a specified time period, determined by the AT. For the purpose of this research, in the context of terrorist attacks, T depends on factors such as the *attractiveness of the target or asset*, the *criticality attractiveness* of the target, the *capabilities of the terrorists* and the available intelligence and law enforcement information. A detailed description of the evaluation of the parameter T can be found in [4].
- Vulnerability (V) represents a potential weakness in structures, systems, individuals or territories that can be exploited by a threat to cause damage. V is expressed as a number between 0 and 1, where 0 means completely invulnerable and 1 completely vulnerable. The value V depends upon the specific threat and the type of damage being analyzed [5].
- The European Commission defines Exposure (E) as the "*totality of people, property, systems, or other elements present in hazard zones that are thereby subject to potential losses*" [13]. E, which sometimes is referred to as asset, can be considered the total value of all elements at risk. Practical assessment of E may include objective parameters, such as the number of people or other types of assets in the area affected by the event [16].

The quantities T, V and E, as defined above, have been rigorously analyzed by the authors in the previous studies [4, 5], with a particular emphasis on the context of terrorist attacks involving CBRNe agents targeting sites and buildings. Each of these values must be evaluated within the specific framework of the risk analysis being conducted.

3.1 Threat assessment (BTAM)

A Building Threat Assessment Method (BTAM) for addressing terrorist attacks involving CBRNe agents is introduced in [4, 17]. This method provides an organized approach beneficial to the AT responsible for evaluating potential terrorist threats to a given site or building. The method [4, 17] introduces two novel indices: the general *Attractiveness of the Target*, characterized by eight parameters, and the *Capability of the Terrorists*, characterized by three parameters. These indices provide an objective basis for evaluating perspectives from both law enforcement and intelligence agencies [4, 17].

The objective of the BTAM is to assess the probability level of specific threats for each site or building considered. This evaluation is conducted by the AT, putting together results from their analyses along with evaluations from intelligence and law enforcement

Table 3 Threat probability scale

Threat probability level	Qualitative definition	Quantitative definition (probability over a given interval of time)	Description of the level's significance
7	Very high	From 3^{-1} to 3^{0} (from 1/3 to 1)	The threat to the site or building is impending. According to intelligence information, the threat is credible
6	High	From 3^{-2} to 3^{-1} (from 1/9 to 1/3)	The threat to the site or building is to be expected. According to intelligence information, the threat is credible
5	Medium to high	From 3^{-3} to 3^{-2} (from 1/27 to 1/9)	The threat to the site or building is likely. According to intelligence information, the threat is credible
4	Medium	From 3^{-4} to 3^{-3} (from 1/81 to 1/27)	The threat to the site or building is possible. According to intelligence information, the threat is recognized but unverified
3	Low to medium	From 3^{-5} to 3^{-4} (from 1/243 to 1/81)	The threat in the region is likely. According to intelligence information, the threat is recognized but deemed unlikely
2	Low	From 3^{-6} to 3^{-5} (from 1/729 to 1/243)	The threat in the region is possible. According to intelligence information, the threat is present but deem unlikely
1	Very low	$< 3^{-6}$ ($<$ 1/729)	The threat to the region or the site/building is insignificant. According to intelligence information, the threat is either non-existent or highly improbable

experts. This comprehensive approach ensures that each threat is assessed not only for its applicability to the specific site or building but also from the perspectives of law enforcement and intelligence.

Upon completing the analysis of the specific site and the relative intelligence information, the AT designates a *Threat Probability Level* through a 7-level Threat Probability Scale based on a logarithm base 3 approach, as depicted in Table 3. The table specifies qualitative and quantitative definitions for each level, along with a description of each level's significance. The proposed scale shares some principles with the scale discussed in [18, 19], although it also presents significant differences as detailed in [4].

3.2 Vulnerability assessment (BVAM)

In the previous publications by the authors, an innovative Building Vulnerability Assessment Method (BVAM) is described and applied to thoroughly analyze the characteristics of a facility and its associated elements. This process identifies flaws in the building and poor redundancy, enabling the determination of protective or corrective measures to mitigate these vulnerabilities [5, 17]. This method aims to categorize the vulnerabilities that significantly affect the risk level of a building when a specific CBRNe threat arises. The proposed method is structured around the analysis of 76 different items relative to the building or site, organized into nine general topics. These topics include both physical and organizational aspects, as well as structural, economic, social and institutional factors, with the objective of assessing critical vulnerabilities of the building. The outcome of the BVAM can be expressed using the 7-level vulnerability scale shown in Table 4 [5].

The numerical value of the assessed Vulnerability level (V) can be employed, along with the values of Threat level (T) and Exposure level ®—described in detail in the following section—to calculate the overall Risk level ® associated with a building.

Table 4 Vulnerability scale

Vulnerability level	Qualitative definition	Quantitative definition (# of successes/total # of attempts)	Description of the level's significance
7	Very high	From 3^{-1} to 3^{0} (from 1/3 to 1)	Major vulnerabilities identified. Asset extremely vulnerable to the specific threat The building lacks necessary protection systems and resilience The entire building would take a very long time to become functional again after an event
6	High	From 3^{-2} to 3^{-1} (from 1/9 to 1/3)	Major vulnerabilities identified. Asset highly vulnerable to the specific threat The building has poor protection systems and low resilience Most sections of the building would take a long time to become functional again after an event
5	Medium to high	From 3^{-3} to 3^{-2} (from 1/27 to 1/9)	One key vulnerability identified. Asset very vulnerable to the specific threat The building has inadequate protection systems and resilience Most critical functions of the building would take a long time to become operational again after an event
4	Medium	From 3^{-4} to 3^{-3} (from 1/81 to 1/27)	One vulnerability identified. Asset fairly vulnerable to the specific threat The building has insufficient protection systems and resilience Most sections of the building would take considerable time to become functional again after an event
3	Low to medium	From 3^{-5} to 3^{-4} (from 1/243 to 1/81)	One vulnerability identified. Asset somewhat vulnerable to the specific threat The building has fair protection systems and resilience Most critical functions of the building would take considerable time to become operational again after an event
2	Low	From 3^{-6} to 3^{-5} (from 1/729 to 1/243)	One minor vulnerability identified. Asset has a slightly increased vulnerability to the specific threat The building has good protection systems and resilience The building would take a short time to become operational again after an event
1	Very low	$<3^{-6}$ (< 1/729)	No relevant vulnerability identified. Asset not vulnerable to the specific threat The building has excellent protection systems and resilience The building would be operational immediately after an event

4 Building exposure assessment method—BEAM

The third critical aspect in risk evaluation is the assessment of Exposure I. It is important to note that the exposure of a building constitutes objective information, independent of the probability of a successful attack. Instead, it provides a factual representation of the valuable assets within the building. This means that the analysis provides information on the presence, attributes and values of any assets potentially affected by a threat, along with criteria or categories chosen for evaluating the consequences, such as economic losses, impacts on people and public confidence [3, 20].

The following section describes the application of the Building Exposure Assessment Method (BEAM) to evaluate the values of the assets. To accurately identify the building's assets, the AT should conduct interviews with individuals most familiar with them. Input from building owners, facility staff, tenants and other relevant parties should be sought by the team to identify the most valuable assets.

Table 5 Exposure scale of the site and surrounding population specific capacity (representing only people subjected to potential losses)

Exposure level	Site population		Surrounding population	
	Qualitative	Quantitative (number of people)	Qualitative	Quantitative (number of people)
7	Very high	>2430	Very high	>24,300
6	High	811–2430	High	8101–24,300
5	Medium to high	271–810	Medium high	2701–8100
4	Medium	91–270	Medium	901–2700
3	Low to medium	31–90	Medium low	301–900
2	Low	11–30	Low	101–300
1	Very low	0–10	Very low	0–100

In this analysis, an asset is defined as a valuable resource that requires protection. An asset can be either tangible—as for people, tenants, structures, equipment, facilities and information—or intangible—as for reputation of an institution or company, a work process organization and a building's symbolic/historical value.

The identification of the more relevant assets and, consequently, the assessment of the Exposure, is carried out with the aim of evaluating the possible consequence of a terrorist attack. Consequences refer to as the adverse effects of a terrorist attack, reflecting the nature and severity of the damages sustained from such an event [17]. Consequences are typically expressed in terms of direct effects, such as property damage, economic costs, fatalities, injuries or other adverse effects such as psychological or social impacts on the victims. Following certain incidents, immediate losses can cascade through society, leading to indirect or secondary losses that may be far-reaching and, at times, even more devastating than the direct ones. This is particularly evident when large areas or sites with critical functions or significance are affected. For instance, terrorist attacks like the 9/11 Twin Towers attack impact society as a whole, requiring a comprehensive analysis of the potential assets characterizing the building.

The approach here proposed for the BEAM focuses on direct and tangible effects. The characterization of the Exposure of a building is divided into the following two categories:

- *Population capacity* of the building or in the surrounding area, for protecting public health and safety avoiding effects on human life and physical well-being (e.g., deaths and injuries).
- *Economic* value of the building and business related to the building and surrounding area. This category implies the potential direct economic effects related to the building and its functions, such as the cost to rebuild the asset, the expenses associated with responding to and recovering from the attack, downstream costs resulting from operational or service disruptions and the economic impact on surrounding infrastructures and facilities.

The scales presented below adopt similar numerical values and approach to that discussed for the BTAM in [4]. However, a fundamental distinction exists: The scales proposed for BEAM only assess the portion of the asset vulnerable to potential losses specific to the considered threat. In contrast, in BTAM [4], the provided tables are applied universally across threats, assessing the total potential value associated with the considered asset for the specific building. This is a relevant distinction and must always be considered in the analysis conducted by the AT.

Three specific Exposure scales for the assessment of the assets subjected to potential losses are provided in this paper:

- *Scale for site population specific capacity* (Table 5). This scale characterizes the population of the specific point of the site or building attacked with a specific threat.
- *Scale for surrounding population specific capacity* (Table 5). This scale characterizes the population of the specific surrounding area (for example, within a radius of 0.3 km), considering the specific point of the building attacked with a specific threat.
- *Scale for the economic specific value of the site* (Table 6). This scale characterizes the intrinsic economic value of the building, along with the business and revenue generated weekly by activities managed at the specific point of attack and its surrounding area (e.g., within a 0.3-km radius around the primary target [21]).

These Exposure scales are applied in the risk assessment method described below, where the results obtained for each individual asset are not combined into a single risk value but are assessed independently. In fact, it is a common concern that comparing different types of assets involves subjective value judgments. Stakeholders and decision-makers may have different perspectives and standards when assessing, for instance, the trade-off between a specific number of fatalities and economic damages. Nevertheless, the fundamental criterion for assigning the risk rating remains the losses associated with human lives (i.e., fatalities and casualties). Other potential losses of assets should only marginally influence this primary rating.

Examples of the three scales are provided in the following tables. The AT is responsible for checking and fixing, in the initial phase of the context analysis, the ranges of the quantitative values in the scales and can decide to modify the proposed ranges based on the specific context to be analyzed. The ranges here proposed have been designed for a general application to a building located in an Italian important city.

Table 6 Exposure scale of the economic specific value of the building (representing only economic specific assets subjected to potential losses)

Exposure level (Economic value)	Qualitative	Quantitative range (Euro) Revenue per week
7	Very high	>97.2 M
6	High	32.4–97.2 M
5	Medium to high	10.8–32.4 M
4	Medium	3.6–10.8 M
3	Low to medium	1.2–3.6 M
2	Low	400 k–1.2 M
1	Very low	1–400 k

5 Building risk assessment methodology—BRAM

This section describes the *Building risk assessment methodology* (BRAM) based on the three assessment methods introduced in the previous sections and the Multi-Risk Assessment approach presented by the authors in [14]. BRAM is designed to evaluate and rank different risk scenarios using a multi-threat approach for the case of terrorist attacks on buildings. The proposed BRAM is characterized by the following design choices:

- Use of 7-point rating scales for all fundamental Threat, Vulnerability and Exposure quantities, represented with logarithmic scales as previously introduced.
- Adoption of logarithm base 3 in the definition of the scales.
- Selection of the observation time interval for the Threat definition proposed above, chosen from one of these possible values: 1, 3, 6 or 12 months, depending on the available information and the AT indications.
- Application of the tripling criterion, which involves quantitatively incrementing values and ranges as one progresses from one level to the next in a scale. This criterion is a direct consequence of adopting logarithm base 3.

It should be noted that the first two design choices, i.e., the use of 7 levels in the scales and the adoption of logarithm base 3, enable an efficient and compact design of the scales for building risk analysis. Furthermore, all the results obtained in BTAM, BVAM and BEAM, as discussed above are applied in this risk assessment method for buildings.

Summarizing these main points in case of terrorist attacks, we can highlight that:

1. The value of the Threat T is related to, as discussed in [4], the Attractiveness of Asset Att_{A} and to the Criticality Attractiveness Att_{C}, other than to the Terrorist capabilities Ter_{C} and Intelligence Information (Int_{I}), i.e.:

$$T = f(\mathrm{Att_A}, \mathrm{Att_C},\ \mathrm{Ter_C},\ \mathrm{Int_I}) \tag{2}$$

   The BTAM provides a possible approach for the estimation of the quantity T, and Table 3 represents a useful tool for the final assessment of threat probability rating values.

2. The value of the Vulnerability V is related, as discussed in [5], to the Criticalities of the building (Cri_{B}) but also to the Threat Type (Thr_{T}) selected by the terrorist for the attack and to the Exposure Specific characteristics (Exp_{S}) (in terms of the asset considered: people, economy and so on), i.e.:

$$V = f\big(\mathrm{Cri_B},\ \mathrm{Thr_T},\ \mathrm{Exp_S}\big) \tag{3}$$

   The BVAM provides a possible approach for the estimation of the quantity V, and Table 4 represents a useful tool for the final assessment of vulnerability rating values.

3. The value of the Exposure E is related to different assets to be protected, as discussed in the previous section. These assets are typically independent of one another, and each asset type requires a separate risk analysis. The analysis below focuses on the asset indicated as *Site Population Specific Capacity* for the building, introduced in Table 5, with the risk assessed in terms of potential deaths and injuries following a terrorist event. It is important to note that the risk assessment could be similarly evaluated for the *Surrounding Population Specific Capacity* (Table 5) and *Economic Specific Value* (Table 6) assets, as discussed in Sect. 4.

Under the hypothesis summarized above for the three variables T, V and E, and taking into account, the results published by the authors in [14], along with the application of logarithm base 3 in the "level" definitions of the scales, the following risk and impact formulas are applied in the BRAM approach:

$$L_{\mathrm{R}} = \ \log_3(R)\ = \text{Risk level} \tag{4}$$

$$L_{\mathrm{T}} = \ \log_3(T)\ = \text{Threat level} \tag{5}$$

Table 7 BRAM semi-quantitative threat scale (over a given time interval)

Threat level	Qualitative scale	From >	To < =	Threat probability Min	Threat probability Max
7	Very high	0.33	1	1/3	1
6	High	0.11	0.33	1/9	1/3
5	Medium to high	0.037	0.11	1/27	1/9
4	Medium	0.012	0.037	1/81	1/27
3	Low to medium	0.0041	0.012	1/243	1/81
2	Low	0.0014	0.0041	1/729	1/243
1	Very low	< 0.0014		< 1/729	

Table 8 BRAM semi-quantitative and qualitative vulnerability scale

Vulnerability level	Qualitative scale	From >	To < =	Vulnerability Min	Vulnerability Max
7	Very high	0.33	1	1/3	1
6	High	0.11	0.33	1/9	1/3
5	Medium to high	0.037	0.11	1/27	1/9
4	Medium	0.012	0.037	1/81	1/27
3	Low to medium	0.0041	0.012	1/243	1/81
2	Low	0.0014	0.0041	1/729	1/243
1	Very low	< 0.0014		< 1/729	

$$L_{\mathrm{V}} = \log_3(V) = \text{Vulnerability level} \tag{6}$$

$$L_{\mathrm{E}} = \log_3(E) = \text{Exposure level} \tag{7}$$

$$L_{\mathrm{I}} = \log_3(I) = \text{Impact level} \tag{8}$$

wherein the Impact I represents the actual damage caused by the exploitation of the considered vulnerability over the exposed assets. Then, due to logarithm properties, the risk and impact formulas discussed in [14] can be re-written as risk and impact level formulas, i.e.:

$$L_{\mathrm{R}} = L_{\mathrm{T}} + L_{\mathrm{V}} + L_{\mathrm{E}} \tag{9}$$

$$L_{\mathrm{I}} = L_{\mathrm{V}} + L_{\mathrm{E}} \tag{10}$$

In this way, risk can be expressed in a more compact form as follows:

$$L_{\mathrm{R}} = L_{\mathrm{T}} + L_{\mathrm{I}} \tag{11}$$

The next step is to adopt appropriate scales for all the fundamental quantities discussed. As a general rule, the range of the first level in the scale is typically set based on the minimal desired granularity for the analysis. The choice of a 7-level rating scale, combined with a logarithm base 3 approach, guarantees that the fundamental quantities cover an adequate range over the entire interval of interest, as will be evident in the following proposed scales.

The BRAM method introduces a semi-quantitative threat scale (Table 7), which revisits the threat probability scale initially presented in Table 3. It reasonably assumes the minimum probability for threat T to be approximately 1 out of 1000 observation intervals. As previously discussed in the threat definitions of Sect. 3, the time interval must be set by the AT, choosing either 1, 3, 6 or 12 months.

The BRAM method proposes a semi-quantitative vulnerability scale (Table 8) with 7 rating values, revisiting the vulnerability scale introduced in Table 4. It reasonably assumes the minimum vulnerability V to be approximately 1 out of 1000 attempts.

For the Exposure scale, as discussed in Sect. 4, the BRAM can focus on different assets, such as the number of people in the building, the number of people in the nearby external area of the building, the economic amount of business per week generated by building activities and the intrinsic value of the building.

Exclusively the first asset mentioned in Sect. 4 is considered in this section: the number of people at the specific point of the building under attack, as shown in the first three columns of Table 5. The scale comprises 7 rating values, reasonably assuming a maximum number of people in the building to be approximately 3000.

Based on the previously described rating tables, a 7-level vulnerability scale (Table 8) and a 7-level exposure scale are found in the first three columns of Table 5. Using these two tables, a semi-quantitative Impact Matrix can be created, as shown in Table 9.

Table 9 Example of BRAM semi-quantitative impact I matrix (*E* is Exposure, and *V* is Vulnerability)

	7	8	9	10	11	12	13	14
	6	7	8	9	10	11	12	13
	5	6	7	8	9	10	11	12
V	*4*	5	6	7	8	9	10	11
	3	4	5	6	7	8	9	10
	2	3	4	5	6	7	8	9
	1	2	3	4	5	6	7	8
		1	*2*	*3*	*4*	*5*	*6*	*7*
					E			

Table 10 BRAM qualitative impact scale

Impact rating	Qualitative Impact	Meaning
from 13 to 14	Very high	Exceptionally grave effect on public health and safety (thousands of deaths and serious injuries possible).
from 11 to 12	High	Grave effect on public health and safety (hundreds of dead and serious injured possible).
from 9 to 10	Medium to High	Serious effect on public health and safety (some tens of cases of deaths and serious injuries possible).
from 7 to 8	Medium	Moderate to serious effect on public health and safety (some cases of death and serious injury possible).
from 5 to 6	Low to Medium	Moderate effect on public health and safety (some cases of non-serious consequences for human health possible).
from 3 to 4	Low	Minor effect on public health and safety (no deaths or serious injuries, unlikelihood of non-serious injuries).
2	Very low	Negligible effect on public health and safety (no significant consequence on human health).

Table 11 BRAM semi-quantitative risk R matrix (*I* is Impact, and *T* is Threat)

	7	9	10	11	12	13	14	15	16	17	18	19	20	21
	6	8	9	10	11	12	13	14	15	16	17	18	19	20
	5	7	8	9	10	11	12	13	14	15	16	17	18	19
T	*4*	6	7	8	9	10	11	12	13	14	15	16	17	18
	3	5	6	7	8	9	10	11	12	13	14	15	16	17
	2	4	5	6	7	8	9	10	11	12	13	14	15	16
	1	3	4	5	6	7	8	9	10	11	12	13	14	15
		2	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*
							I							

As discussed above, this matrix applies the tripling criterion for each increase of 1 in the rating value. The impact rating values represented by the matrix elements are calculated by simply adding the row and column indices, as indicated by formula (10).

The use of colors and the definition of an appropriate scale allows to represent both a semi-quantitative scale with 13 rating values and a qualitative 7-level scale within a single matrix, as shown in Table 10. For each level, these definitions can also be verified by evaluating the quantitative impact value by using formula (10) and the corresponding V and E numerical values available for each element of the matrix.

For a qualitative and semi-quantitative estimation of risk, using the 7-level threat scale (Table 3), the results obtained in Table 9 for the Impact rating of 13 distinct semi-quantitative values, and formula (11), it is possible to create a semi-quantitative risk matrix of 19 levels of risk (Table 11). Similar to the impact case, in this new matrix (Table 11), the tripling criterion applies for each increment of 1 in the rating value, and the matrix elements representing the risk rating values are simply calculated by adding the row and column indices, as suggested by formula (11).

Table 12 BRAM qualitative risk scale

Risk rating values	Qualitative Risk	Meaning
from 20 to 21	Very high	In the short term, an exceptionally severe disaster with exceptionally severe impacts on public health and safety is very likely.
from 18 to 19	High	In the short-medium term, a severe disaster with severe impacts on public health and safety is likely.
from 16 to 17	Medium to High	In the short-medium term, a serious disaster with serious impacts on public health and safety is probable.
from 13 to 15	Medium	In the medium term, a moderate to serious event with moderate to serious impacts on public health and safety is possible.
from 10 to 12	Low to Medium	In the medium-long term, an event with a low impact on public health and safety is possible.
from 7 to 9	Low	Even in the medium-long term, an event with impacts on public health and safety is unlikely.
from 3 to 6	Very low	Even in the long term, an event with impacts on human health is very unlikely.

Table 13 Evaluation of the general attractiveness

Attractiveness index	Shopping Center	Public Administrative Building
Attractiveness of the target	19	30
Criticality attractiveness	19	4
General attractiveness	38	34

Table 14 Evaluation of the terrorist capability

Rank	Threats	Terrorist capability index
1	Suicide belt bomb	18
2	Van bomb	16
3	Cesium-137 dirty bomb	11

Again, the use of colors and the definition of an appropriate scale allow the transition from a semi-quantitative scale of 19 levels to a qualitative scale of 7 levels of risk, as shown in Table 12. The BRAM described here for the Site Population Specific Capacity asset shows the fundamental characteristics of the method and provides a guideline for its application to other specific assets.

6 Results of the case studies

In this section, the focus is on the application of BRAM to the two case studies, whose characteristics are described in Sect. 2: a Shopping Center and a Public Administrative Building in an important Italian town.

Following the steps outlined in Sect. 5, the first parameter to be obtained is the general Attractiveness index for the two sites. This index includes both the Asset attractiveness and the Criticality attractiveness, as described in detail in [17]. For the case studies analyzed in this paper, considering the *Attractiveness of the Target* and the *Criticality Attractiveness* indices discussed in Sect. 5 and detailed in [4, 17], Table 13 shows the results obtained from analyzing the characteristics of the target.

As a further step, Table 14 shows the assessment of the *Terrorist capability* index, discussed in Sect. 5 of this paper and in [17], for the three attacks considered here, based on the approach described in [4]. This assessment is independent on the site. As shown in Table 13, both buildings exhibit a similar General Attractiveness. According to this assessment, the suicide belt bomb requires significantly less capability, indicating a higher likelihood of use by terrorists, whereas the dirty bomb, due to the high cost and skills required, is the least probable attack method. At this stage of the BTAM analysis, it is assumed that intelligence information is available to estimate the general probability of an unspecified terroristic attack in the area. In this scenario, it is assumed that intelligence suggests a *credible threat to a non-specified target in the area.*

By merging the results from Tables 13 and 14, together with intelligence data, Table 3 can be used to obtain a ranking of the Threat probabilities for the two targets and three threats as outlined in Table 15.

As evident from the ranking in Table 15, the most likely attack is the suicide belt bomb in the Shopping Center. This accounts for the high general attractiveness of the target, due to the large number of people present, and the relatively simple execution of this type of attack.

Table 15 Ranking of the threat level

Threat Level L_T (over 12 months)	Suicide belt bomb	Van bomb	Cesium-137 dirty bomb
Shopping Center	5	3	2
Public Administrative Building	3	2	1

Table 16 Ranking of the vulnerability level

Vulnerability level L_V	Suicide belt bomb	Van bomb	Cesium-137 dirty bomb
Shopping Center	7	7	7
Public Administrative Building	1	1	1

Table 17 Ranking of the exposure level

Exposure level L_E	Suicide belt bomb	Van bomb	Cesium-137 dirty bomb
Shopping Center	3	4	5
Public Administrative Building	2	5	7

Table 18 Ranking of the risk level

Risk level L_R	Suicide belt bomb	Van bomb	Cesium-137 dirty bomb
Shopping Center	15	14	14
Public Administrative Building	6	8	9

For the Vulnerability, the 7-level vulnerability scale described in [5] and presented in Table 4 is used. A comprehensive analysis of all parameters defined in the BVAM method, along with the characteristics of the sites summarized in Table 2, leads to the ranking outlined in Table 16.

As it can be observed, the Shopping Center shows a significantly higher vulnerability than the Public Administrative Building, mainly due to substantial lack of controls over people and vehicles. In contrast, the protective measures of the Public Administrative Building make it less vulnerable to attacks. Regarding the Exposure level, as stated in Sect. 5, only the number of people within the specific building is considered as a parameter for estimating the impact. Different stakeholders may include other parameters, such as economic value, in their assessment. By matching the parameters in Table 2 with the scale in the first three columns of Table 5, it is possible to estimate the Exposure levels detailed in Table 17 for the two sites across the three attack scenarios:

In this case, the most severe type of attack is unsurprisingly the dirty bomb. However, while the Public Administrative Building shows higher exposure in the cases of van bomb and dirty bomb, mainly due to its structure and location, the Shopping Center shows greater exposure to the suicide belt bomb, due to the larger concentration of people. Using formula (11), the BRAM method facilitates the evaluation of the risk levels by adding all evaluated components, i.e., Threat, Vulnerability and Exposure levels. The final risk ranking for the three attack methods and the two sites is summarized in Table 18. These quantitative values can be easily interpreted using Table 12, which translates numerical ranges into a color-coded format. As shown in the table, the Shopping Center is considered significantly more at risk than the Public Administrative Building. This assessment primarily considers the presence of people in the building and does not include, for example, the psychological impact of a possible attack. Moreover, the Shopping Center's substantial lack of stringent controls, due to its commercial nature, makes it a highly vulnerable target to various types of attacks.

However, based on the presented case studies, many other risk scenarios can be assessed by highlighting different vulnerabilities or targets, or considering alternative threat scenarios. BRAM is not just an exact numerical evaluation algorithm but could prove to be a flexible assessment tool capable of easily identifying and highlighting specific risk situations or trends based on the selected scenario.

7 Conclusions

In this research, an original Building Risk Assessment Methodology (BRAM) has been presented and applied to various case studies. The BRAM comprises a set of tools and methods designed to assess threats, vulnerabilities and exposure in a chosen scenario. These tools can be customized and configured according to the specific aspect under investigation or emphasis in the risk assessment. Moreover, the analysis can be focused on particular aspects depending on available information. For example, if intelligence information suggests that a specific type of attack is imminent, the analysis can concentrate on the identification of the building most vulnerable to attacks. Conversely, when designing a new public building, the BRAM can be used to assess possible vulnerabilities to different types of attacks.

The great value of this methodology resides in its flexibility and adaptability to different environments and perspectives: It can prioritize safeguarding a specific asset or emphasize the preparation for a specific imminent threat, while giving the proper weight to each individual parameter.

Author's contribution All authors contributed to the study conceptualization and design. Material preparation, data collection and analysis were performed by Marco Carbonelli, Laura Gratta, Riccardo Quaranta and Daniele Di Giovanni. Pasquale Gaudio and Andrea Malizia supervised the work. Marco Carbonelli and Laura Gratta wrote the first draft of the manuscript. All authors commented, edited and reviewed the previous versions of the manuscript. Riccardo Quaranta and Grace P. Xerri edited the final version of the manuscript. All authors read and approved the final manuscript.

Funding Open access funding provided by Università degli Studi di Roma Tor Vergata within the CRUI-CARE Agreement.

Data availability The methodology developed in this work stems from the previously published works of the authors on [3–5, 14, 17]. Information relative to the location, infrastructure, operations and safety procedures of the buildings used as case studies, i.e., the Shopping Center and the Public Administrative Building, cannot be disclosed for safety reason, given the sensitive topic discussed in this manuscript.

Declarations

Conflict of interest The authors have no competing interests to declare that are relevant to the content of this article.

References

1. N.K. Ersun, The "new terrorism" and its critics. Stud. Confl. Terror. **34**(6), 476–500 (2011). https://doi.org/10.1080/1057610X.2011.571194
2. W. Enders, T. Sandler, After 9/11: Is it all different now? J. Confl. Resolut. **49**(2), 259–277 (2005)
3. M. Carbonelli, *Terrorist attacks and natural/anthropic disasters: risk analysis methodologies for supporting security decision making actors* (Aracne CBRN Series, Rome, 2019)
4. M. Carbonelli, M. Carestia, R. Quaranta, Threat assessment method for buildings in case of terrorist attacks. Int. J. Saf. Secur. Eng. **11**(4), 285–294 (2021). https://doi.org/10.18280/ijsse.110401
5. M. Carbonelli, R. Quaranta, A. Malizia, P. Gaudio, D. Di Giovanni, G.P. Xerri, "Building vulnerability assessment for explosive and CBR terrorist attacks", WIT transactions on the built environment, Volume 214, 2022, Risk safe 2022, pp.97-111, edition 2022WIT Press, www.witpress.com, (2022), https://doi.org/10.2495/SSR220081
6. B.M. Ayyub, *Risk analysis in engineering and economics* (University of Maryland, Chapman & Hall/CRC, New York, 2003), pp.35–38
7. B.E. Biringer, R.V. Matalucci, S.L. O'Connor, *Security risk assessment and management: a professional practice guide for protecting buildings and infrastructures* (John Wiley & Son Inc., Hoboken, 2007)
8. S. Bouchon, "The vulnerability of interdependent critical infrastructures systems: epistemological and conceptual state of-the-art", (2006)
9. M. Modarres, *Risk analysis in engineering: techniques, tools and trends* (Taylor & Francis Group, Boca Raton, 2006)
10. A. Sotic, R Radjic, 'The review of the definition of risk', online journal of applied knowledge management, Vol.3, special issue (2015)—Paper selected from international conference in applied protection and its trends, http://www.iiakm.org/ojakm/articles/2015/volume3_3/OJAKM_Volume3_3pp17-26.pdf
11. ISO 31000, Risk management—Principles and guidelines, International Organization for Standardization, last edition (2018)
12. ISO 31010, Risk management—Risk assessment techniques. International Organization for Standardization (2009)
13. European commission staff working paper, Risk assessment and mapping guidelines for disaster management, Brussels (2010), https://ec.europa.eu/echo/files/about/COMM_PDF_SEC_2010_1626_F_staff_working_document_en.pdf
14. M. Carbonelli, L. Gratta, A general multi-risk assessment method for natural disasters and CBRNe attacks. Int. J. Saf. Secur. Eng. **11**(4), 345–352 (2021). https://doi.org/10.18280/ijsse.110407
15. M. Carbonelli et al., "Risk Assessment institutional approaches for disaster management: US, UN and EU cases", 2nd scientific international conference on CBRNe - SICC series conference (2020), Rome, https://www.sicc-series.com/book-of-abstract/
16. United Nations, "Terminology on disaster risk reduction, United Nations international strategy for disaster reduction (UNISDR)", Geneva (2009), https://www.unisdr.org/files/7817_UNISDRTerminologyEnglish.pdf
17. M. Carbonelli, *Attacks against* buildings*: threat, vulnerability and risk assessment*, e-book CISINT, Sect.4, Rome, 30 December (2023), ISBN: 979–12–210–4808–7, https://www.cisint.org/cms/wp-content/uploads/Attacks-against-buildings-M.Carbonelli-CISINT-2023.pdf
18. USA Federal Emergency Management Agency, Risk assessment: a how-to guide to mitigate potential terrorist attacks against buildings, Risk management series, FEMA 452, January (2005), https://www.fema.gov/sites/default/files/2020-08/fema452_01_05.pdf
19. USA Federal Emergency Management Agency, Reference manual to mitigate potential terrorist attacks against buildings, Fema 426/BIPS06 October (2011), Edition 2, https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf
20. UNISDR, "Open-ended intergovernmental expert working group on indicators and terminology relating to disaster risk reduction: report of the second session (informal and formal)", The United Nations office for disaster risk reduction, Geneva, Switzerland (2016), https://www.preventionweb.net/files/50683_oiewgreportenglish.pdf
21. USA Federal Emergency Management Agency, Handbook for rapid visual screening of buildings to evaluate terrorism risks, FEMA 455 / March (2009), https://www.fema.gov/sites/default/files/2020-08/fema_455_handbook_rapid_visual_screening.pdf.