IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

International Journal of Safety and Security Engineering
Vol. 11, No. 4, August, 2021, pp. 285-294
Journal homepage: http://iieta.org/journals/ijsse

Threat Assessment Method for Buildings in Case of Terrorist Attacks

Marco Carbonelli*, Mariachiara Carestia, Riccardo Quaranta

Industrial Engineering Department, University of Rome 'Tor Vergata', 00133 Roma RM, Italy

Corresponding Author Email: marcocarbonelli62@gmail.com

https://doi.org/10.18280/ijsse.110401

Received: 28 December 2020
Accepted: 20 July 2021

Keywords:
building asset attractiveness, building vulnerability attractiveness, building threat, CBRNe threat, hazard material, risk management, terrorist attack, threat assessment

ABSTRACT

The objective of this paper is to outline the essential features of an original Threat Assessment Method for sites and buildings for the case of terrorist attacks with Explosive/CBR agents. The proposed method, based on an approach in six Steps, provides a structured guide useful to the Assessment Team in charge to evaluate the terrorist risks in a site/building. The method introduces two indexes, the general Attractiveness of a target and the Terrorist Capability. Using these indexes, it is possible to evaluate for a wide area a first rank for the sites/buildings that shows a potentially higher Attractiveness for the terrorists and, in a similar way, the Terrorist Capability index that provides a criterion for determining the easily applicable threats in a wide list of proposed Explosive/CBR weapons. Finally, the proposed method is applied to three practical Case Studies and obtained results are discussed.

1. INTRODUCTION

In the last two decades, several different possible approaches have been proposed in the technical literature [1-9] to face the problem of the Risk Assessment for buildings and sites in the case of terrorist attacks.

In particular, in the USA the Federal Emergency Management Agency (FEMA) with the 'How-to Guide' 452/2005 [4] and the 'Reference Manual' 426/BIP06/2011 [5] has provided a technical model widely applied in the United States (US) professional market.

Nevertheless, many aspects of these US approaches have been changed over the time, starting from the 2003 [3], and even the concepts and the practical evaluations of *threats*, *vulnerabilities*, *consequences* and *assets*, fundamental for the risk management process even in the case of terrorist attack, maintain some critical unresolved points.

The objective of this paper is to outline the essential features of an original *Threat Assessment Method* for sites and buildings for the case of terrorist attacks with Explosive/CBR (Chemical, Biological, Radiological) agents. The proposed method, based on six logical Steps, provides a structured approach useful to the *Assessment Team* in charge to evaluate the possible terrorist threats applicable in a site/building. The method, overcoming some critical points of existing methodologies, introduces two original indexes, the general *Attractiveness* of a target and the *Terrorist Capability*. The general Attractiveness index is, in its turn, composed by two other sub-indexes: the *Asset Attractiveness* and the *Vulnerability Attractiveness* of the site/building. Using these indexes it is possible, as shown in the work for three considered Case Studies, to assess the level of magnitude of the assets present in a site/building. The method proposed is applicable in a geographical wide area - for example a district, a town or a region - and allows to generate a *first rank* for the sites/buildings that shows the attractiveness potential higher for the terrorists. In a similar way, the *Terrorist Capability* index provides a basic criterion for determining the easily applicable threats in a wide list here presented of attacks based on Explosive/CBR weapons. The capability of the terrorist to access the weapons and the CBR agents are evaluated, threat by threat, and the analysis in this case focuses the attention on the capability to manage arms and not-conventional weapons and to organize an attack exploiting weakness in the service infrastructure and in the control/security systems of the target. Even these aspects will be analyzed in the considered Case Studies. Finally, the method proposes the evaluation of the Threat Probability Level, adopting a scale of 7-levels based on logarithm ranges [10].

2. THREAT ASSESSMENT METHOD AND CASE STUDIES

In the institutional literature of US on disaster management, the concept of *threat* is often defined [3, 4] *as any circumstance or event with the potential to cause loss of, or damage to an asset*. In the European (EU) documents on the same issue, the concept of *threat* is defined [10, 11] as *a potentially damaging physical event, phenomenon or activity of an intentional/ malicious character*. Within the military services, the intelligence community, and law enforcement, the term threat is typically used to describe the possible contest for a terrorist action or manmade disaster.

It is important to observe that, in a more extended technical arena [3, 10-13], other than the term *threat*, is often used in several different situations the term *hazard*, intending natural or man-made source or cause of harm or difficulty. A hazard differs [11, 12] from a threat in *that a threat is intentionally directed at an entity, asset, system, network, or geographic area, while a hazard is not directed*.

In this work we focus our attention only on *terrorist threats*, taking clear in mind that imagine and identify an ex-ante specific threat can be a complex task.

In fact, the *terrorist threat* is very difficult to predict because it directly depends on human will, historical data are generally insufficient and, for their intrinsic intentional nature, the occurrence and possible recurrence of terrorist attacks are very difficult to predict. This makes the determination of a particular threat, for any particular site or building as focused on this work, a topic very difficult to face.

In general terms, we can state that terrorists select targets that have a *well recognized* value for the enemy. A selected target could be an iconic commercial property, a symbolic administrative building or government center, or a similar structure to inflict significant emotional, economical and political damage to the enemy.

Furthermore, terrorists usually choose their targets to maximize the impact of their attack and minimize the effort. Statistical data on past attacks [3, 4] show that terrorists more rarely attack *hard targets*, denoting with 'hard target' those buildings that are fortified or defended with care, for example, government, military or intelligence buildings/sites. They often prefer to attack *soft targets*, such as commercial shopping malls, theatres, cinemas, where a successful attack might produce the researched relevant effect.

In other words, the probability of occurrence of a terrorist event in a specific site (*threat probability*), is greatly influenced by the general *Attractiveness* - denoted in the following with *Att* - of the site.

With the term *Attractiveness* we describe two different aspects:

- the *value* of the *assets* characterizing the site, for example, number of people in the building, economic and symbolic value of the building. In the following this component will be referred as *Asset Attractiveness* Att_A sub-index;
- the potential *vulnerabilities* exploitable in the site, for example: possibility to attack easily, minimizing the effort and exploiting some weaknesses of the structure/organization. In the following this second component will be referred as *Vulnerability Attractiveness* Att_V sub-index.

For the scope of this work, the following relation holds for the general *Attractiveness Att* index:

$$Att = Att_A + Att_V \qquad (1)$$

This last index can be usefully adopted in the process of evaluation and selection of *sites and buildings potentially interested by terroristic threats*. Such a process is of interest for threat *Assessment Teams* at institutional/government level where, at federal, national, regional and sub-regional level, it's necessary to conduct a preventive analysis of the potential terrorist targets, in order to determine on large territory (*wide area*) a rank of sites and buildings on which to implement risk mitigation policy to reduce the impact of a potential attack. At the same time, this Attractiveness index can result of interest even for the private *Assessment Teams* that operate in specific fields, for example for commercial centers, productive sites or financial buildings, where, in cooperation with the private building stakeholders, it is necessary to identify which buildings and sites, among many, are to protect against potential terrorist threats.

Starting from several different possible methodologies proposed in the last two decades in the technical literature [1-9, 14-16] and introducing some original aspects in the approach, a *Threat Assessment Method for buildings/sites* is here proposed to support the Assessment Teams to select and identify the sites characterized by an high general Attractiveness index, and, for each of these sites, investigate the *primary threats applicable* and a *possible rank of the threats*, finally determining the threat probability. The *Threat Assessment Method for buildings/sites* here discussed aims to provide a linear approach in *six Steps*, where the first five steps can be carried out by the Assessment Teams even without a direct *intelligence* information contribution, on the base of skill and experience. The last Step, on the contrary, results well addressed if the Assessment Team can access intelligence information for the final evaluation of the threat probability level. The proposed Steps for the method are visually represented in Figure 1 and are listed and analyzed in detail in the following.

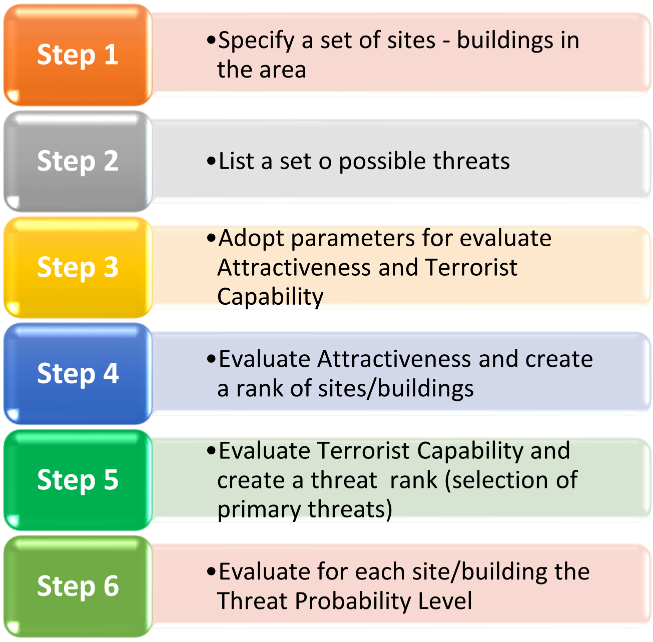
Step 1
•Specify a set of sites - buildings in the area
Step 2
•List a set o possible threats
Step 3
•Adopt parameters for evaluate Attractiveness and Terrorist Capability
Step 4
•Evaluate Attractiveness and create a rank of sites/buildings
Step 5
•Evaluate Terrorist Capability and create a threat rank (selection of primary threats)
Step 6
•Evaluate for each site/building the Threat Probability Level

Figure 1. Threat assessment method for site/building in six steps

Step 1. Specify the set of sites/buildings in the area – typically wide - on which the method here presented is applied. The wide area can be a district, a town, a region or, conversely at a limit condition, a small area reduced to a single site/building.

Step 2. List a large set of possible threats in the field of Explosive and CBR attacks for residential/administrative and commercial buildings/sites.

Step 3. Adopt an adequate number of parameters in order to characterize the *Attractiveness* index (depending on asset values and exploitable vulnerabilities in the buildings/sites) and the *Terrorist Capability* index (depending on the easy for terrorist to access the agents/weapons for the attack and on the expertise/skill to conduct the attack).

Step 4. Evaluate the general Attractiveness Att index of the targets for the different sites/buildings specified in Step 1. On the basis of this index, create a *first rank of sites* showing an higher attractiveness for the terrorists (independently of the attack type).

Step 5. Evaluate the Terrorist Capability Ter_C index for every threat of the list determined in Step 2, applying the parameters introduced in Step 3. On the basis of this index, produce a first possible *selection of the primary threats* to be expected in the wide area analyzed (independently of the specific site/building).

Step 6. Evaluate for each site/building the final rating of the probability of a specific threat, taking into account the results obtained in Steps 4 and 5, together with the fundamental evaluations of *intelligence* and *law-enforcing institutional experts* and of *reliable intelligence information*. This means that all the threats considered in the analysis, and in particular the selected primary threats of Step 5, are further analyzed both for evaluating the applicability in the specific site/building considered (site and threat dependent analysis) and from a law-enforcing perspective and intelligence information viewpoints. At the end of these 'site and threat based' and 'intelligence' analyses, a final *Threat Probability Rating* can be assigned using a *threat scale of 7 levels* proposed in the method. In absence of institutional intelligence experts and of direct intelligence information for the second component of last analysis, the Assessment Team will *autonomously* assess for each site of interest the probability of the threat, using the same threat scale of 7 levels of the method. In this last case the evaluation will be conduct basing on the Team experience only.

This proposed method allows to the *Assessment Teams* to complete in an ordered and comprehensive way the building threat assessment phase.

To make the description of the method more tangible and interesting, we will focus our attention in the following specific evaluations only on *three threats* of the many proposed in the method as potential possible threats and on three specific and real sites/buildings. Under these hypotheses Three different Case Studies will be analyzed in the: *a commercial center*, *a government building*, *a little hospital* of an Italian town

The essential characteristics of the three different *sites/building* are herein essentially described.

Commercial Center

Situated in an important town, peripherical position, with an average number of people present in the Commercial Center during the day assessed to 500, considering both customers and workers of the Commercial Center. The Center is surrounded by a small park and many residential buildings, for an average of 6000 inhabitants within 0.5 km within the Center. The building was built in the 1970 and is not particularly relevant from a symbolic viewpoint. The Center is used by clerks and local family. The building value is, today, 3.5 million euros and the amount of weekly business is of 1.9 million euros. The external parking area of the Center is open access to all, with unprotected air and consumable entry. vehicles park without any specific policy. Even the access to the building is free for all the customers and for consumable supply. No specific internal security monitoring center operation exists, bland policies for the protection of critical and essential service energy, ICT, HVAC, no specific business/operation continuity plan applied for the majority of the shops in the Center.

Government Building

Situated in the same town of the Commercial Center, central position, with an average number of people in the building during the day assessed to 2000, considering both many national politicians, public workers and advisors. The building is surrounded by very large roads and squares, with shops and some residential buildings, for an average of 1500 people within 0.3 km from the building. The building was built between the 15th and 16th century and is one of the most important icons of the town and the nation. The building value is, today, more than 50 millions euros and the amount of weekly business around the building is more of 3 millions euros. The external parking area of the building is controlled with access by Pass Only. No vehicle can park within 50 meters, Presence of fenced, guarded and protected air/consumable entry. At the two entries of the building a severe controlled access is applied with an identification policy of visitors and non-staff personnel at the building. Badge are used for identification and registration for personnel access. Presence of a video controlled access area.

Internal security monitoring center with full day operation, specific and update policies for the protection of critical and essential services (energy, ICT, HVAC services), update and adequate operation continuity plan applied to the building.

Hospital

Situated in the same town of the other two buildings, in peripherical position, with an average number of people in the little public Hospital during the day assessed to 150, considering both health service workers and patients. The building is surrounded by a very large parking area with a garden and few residential buildings, for an average of 500 people within 0.3 km from the hospital. The building was built in the 1951 and is one of the three hospitals in the district. The building updated value is roughly 7 millions euros and the amount of weekly business around 0.3 km within the building is not relevant. The external parking area of the hospital is controlled by a private Security service. No vehicle can park within 10 meters to the hospital entry, access with cars to the structure only for health system operators,

Bland controlled access of visitors at the building, unprotected air/consumable. Presence of video controlled access area.

Internal security monitoring center with minimal policies for the protection of critical and essential service, and operation continuity plan existing.

2.1 Step 1 – List of the possible sites/buildings

The first point of the method to face for the Assessment Team is to establish the perimeter of the area of the sites/buildings to be analyzed. The considered area can vary in dependence of the different cases, target and interested stakeholders. The sites/buildings can be useful distinct in categories, following for example, this starting list: Government buildings, Administrative buildings, Diplomatic buildings, Symbolic and Iconic sites, Police and Intelligence centers, Healthcare-Hospital buildings, Cultural sites, University and School buildings, Commercial centers, Financial/Bank buildings, Productive/Utility centers and infrastructures, Office buildings, other high asset value infrastructures/sites.

In the following, for the application of the method, we will focus our attention on the Case Studies above introduced: *a commercial center*, *a government building*, *a hospital.*

2.2 Step 2 – List of the possible threats

In the attempt to evaluate *terrorist threats*, it is fundamental to understand which are the objectives of the aggressors. Typically, the terrorists are violent people and they seek publicity for their cause, monetary or political gain through their actions. These actions can be very different in practice and include injuring or killing people, destroying or damaging facilities, property, equipment, resources, or stealing equipment, material, or sensitive information. In some cases, the threat may originate from more than one person or group, and we can reveal differing action-methods and rationales.

So, to face the complex task to imagine and characterize a terrorist possible threat we can build, starting form the result in [4, 5], a *basic* and *flexible list of threats*, including for the purposes of this work, at least these different categories of terrorist attacks:

1. *Improvised Explosive Device attack* – such as moving vehicle bombs; stationary vehicle bombs; bombs delivered by persons (suicide bombers); exterior attacks (thrown objects like rocks, Molotov cocktails, hand grenades, or hand-placed bombs); covert entries (gaining entry by false credentials or circumventing security with or without weapons); mail bombs (delivered to individuals); supply bombs (larger bombs processed through shipping offices);
2. *CBR attack* – such as airborne contamination with CBR agents (used for example to contaminate the air supply of a building), waterborne contamination with CBR agents injected into the water supply or similar applications with indoor and outdoor CBR attacks.

In Table 1 we provide a possible list [5] of specific threats that can be considered as a *starting point* for the threat assessment process. The list can be integrated and modified taking into account the Assessment Team opinions for the specific situation.

As above discussed, for the Case Studies we will focus our attention only on three different specific *threats* extracted from Table 1. The threats considered in the following evaluation will be:

- the explosion of a van-bomb;
- the explosion of a suicide belt-bomb;
- the explosion of a Cesium-137 Dirty Bomb.

2.3 Step 3 – Adopt parameters for the evaluation of Attractiveness and Terrorist Capability

The terrorist attack of last decades shows [3,4,10] that terrorist cells continually evaluate new plans, and seek to exploit all the possible weakness and fragility of the enemy assets, in particular for buildings, taking into account the protective structural features and the site management security procedures.

For this reason, it becomes for every stakeholder impossible, both from a technical and benefit/cost point, *to try to protect everything from every type of attack*. The Assessment Team has the responsibility to determine what kind of threat is primary for the building to be protected and what level of protection the building stakeholders can afford. As the terrorist threat changes over time, the Assessment Team should revisit periodically all the threat assessment process, evaluating possible new imminent threats.

To select the *primary sites/buildings* and the *potential primary threats* of the starting list proposed in Step 2, we need to identify some *parameters*. These parameters have to be possibly objectives and based on the potential *attractiveness of the target* and on the *terrorist supposed capabilities*. In particular, in this step of the analysis we are interested in evaluating some specific characteristics of the *site*, the intrinsic economic and symbolic value, the general activities and high level functions internally carried out, the number of people operating in the building and in the surrounding of the building, and the terrorist capability to access and manage explosive and/or CBR agents.

Table 1. Starting list of possible specific threats for the assessment process [5]

Starting List of Threats
Improvised Explosive Device (Bomb)
- Stationary and Moving Vehicle
• Car bomb (50-200 kg TNT)
• Van bomb (200-1500 kg TNT)
• Trunk bomb (1500-30000 kg TNT)
• Small, medium and large aircraft
• Ship
- Mail
• Mail bomb (0,05-0,4 kg TNT)
- Supply
• Various dimensions
- Thrown
• Grenade (0,1-0,5 kg TNT)
- Placed
• Various dimensions
• Briefcase/Suitcase bomb (10-25 kg TNT)
- Suicide Bomber
• Pipe bomb (1-4 kg TNT)
• Suicide belt bomb (3-10 kg TNT)
• Suicide vest bomb (5-15 kg TNT)
• Satchel bomb (5-20 kg TNT)
Chemical Agent (agent example)
- Blister (Lewisite, Mustard)
- Blood (Hydrogen Cyanide)
- Choking/Lung /Pulmonary (Clorine, Phosgene)
- Incapacitating (BZ)
- Nerve (Tabun, Sarin, Soman, VX)
- Riot Control/Tear Gas (Mace)
- Vomiting
Biological Agent/Desease (group and category)
- Anthrax (bacteria, Cat.A)
- Botulism (toxin, Cat. A)
- Brucellosis (bacteria, Cat.B)
- Plague (bacteria, Cat.A)
- Smallpox (virus, Cat. A)
- Tularemia (bacteria, Cat. A)
- Viral Hemorrhagic Fevers (virus, Cat.A)
- Ebola (virus, Cat. A)
- other Toxins: Ricin, Staphylococcal Enterotoxin type B, T-2 Mycotoxins (toxin,Cat. B)
Radiological Attack/Agent
- R agent generic dispersion (Alpha, Beta, Gamma)
- Radiological Dispersal Device (RDD) - Dirty bomb
- Radiological agent storage
- Spent nuclear fuel storage
- Nuclear plant

The starting *basic parameters* proposed in this work for evaluating the *Attractiveness* of the target and *Terrorist Capability* indexes are collected in three distinct categories:

A. parameters for evaluating the *Asset Attractiveness* for a target, denoted by Att_A, focalized on the assets characterizing the site;

B. parameters for evaluating the *Vulnerabilities Attractiveness* for a target, denoted by Att_V, focalized on the weakness and fragility of the structures and of the security organization vulnerabilities, applied to the physical aspects, technical solutions and defense measures;

C. parameters for evaluating the *Terrorist Capabilities*, denoted by Ter_C, intending the terrorist capability to access, organize and manage Explosive/CBR agents-weapons.

In fact, in the case of a malicious attack due to an organized, skilled and adequately-financed terroristic group, the aggressor take into account in determining the site/building target of an attack, fundamentally, these three different aspects:

- the relevance of the asset to be attacked;
- the possible exploitable vulnerabilities characterizing the structure and the security organization;
- the capabilities to access and manage the necessary weapons.

Taking into account these analyses, we describe in detail eleven possible parameters collected in these three above introduced categories.

Category A - Parameters for evaluating the Asset Attractiveness of a target

As far as the Asset Attractiveness category is concerned *five* basic different parameters are introduced. It's important to stress that all these parameters are *site-dependent* and *threat-independent*. The objective of these parameters is to characterize in an adequately way, independently of the threat, the value of the assets (i.e. number of people exposed, economic and cultural values, political and iconic relevance). The proposed parameters are listed in the following.

A1. *Site Population Capacity* - The statistical population of the site/building (typical worst case occupancy).

A2. *Surrounding Population Capacity* - The statistical population of the surrounding area (for example within 0.3 km, typical worst case surrounding occupancy).

A3. *Building Relevance/Symbolic value* - The administrative, government, cultural and iconic relevance of the building for the State, Region, Town.

A4. *Political/administrative/socio-cultural importance of the occupants of the building* - The knowledge of building occupants and visitors can strength influence the choice of the target by the terrorists.

A5. *Economical value of the site* – Intrinsic economic value of the building added to the amount of business and revenue weekly generated by the activities managed in the site and in the collateral surrounding area (for example within 0.3 km [7] around the main target), both in direct and indirect ways.

Category B - Parameters for evaluating the Vulnerability Attractiveness of a target

As far as the Vulnerability Attractiveness is concerned, in this method are introduced *three* general different parameters for the evaluation. It's important to stress that even these parameters are *site-dependent* and *threat-independent* at this stage of the analysis. These parameters characterize, independently of the threat, the *general* vulnerability of different parts of the site, starting from the more external zone, up to the internal part of the building, taking a cue from the layers of defence approach [4]. The proposed parameters are listed in the following.

B1. *External vulnerability of the site* (external security) – Take into account and evaluate the control of external parking, vehicle and pedestrian external control points, the presence of Closed Circuit Television CCT monitoring, physical perimeter barriers, lighting with emergency power backup.

B2. *Entry vulnerability of the building* (building perimeter security) – Take into account and evaluate the procedures for people identification and access control facilities (X ray and magnetometer equipment, internal CCT monitoring, badge readers), receiving/shipping procedures, vehicle internal access, primary and secondary points of entry of utilities as electric power, water, gas, fuel, Information Technology and telecommunications infrastructure, Heat Ventilation and Air Conditioning (HVAC) peripheral systems, the structural building blast robustness, the window glass resistance (safety window film).

B3. *Internal vulnerability of the building* (internal security) – Take into account and evaluate the security internal control and monitoring center; the presence of a specific control for core infrastructures (energy, water, alarms, radio and wired emergency communications, ICT facilities, HVAC facilities, plumbing and gas systems, hub and terminal equipments) and specific essential functions (day care, administration, engineering, data center, security, food service, …) [4].

Category C - Parameters for evaluating the Terrorist Capabilities

As far as the third category, *Terrorist Capability*, is concerned, *three* different parameters are introduced for the evaluation. It's important to stress that these last parameters are, at this stage of the analysis, *threat-dependent* and *site-independent*. The parameters characterize, independently of the site, the capability of terrorists to access and manipulate the agents/weapons, and the organizational and technical skill. The proposed parameters are listed in the following.

C1. *Access to Explosive/CBR Agents* – This parameter evaluates the ease by which the source material for the attack can be acquired/make available to carry out the terrorist action. Consideration includes explosive/CBR agent provisioning, the local materials of HazMat inventory, farm and mining supplies, major chemical or manufacturing plants, university and commercial specific laboratories.

C2. *Expertise on weapons of the terrorists* – The parameter focuses the attention on the general level of skill and training to manage and create the weapon or arm a CBR agent. The evaluation of the parameter considers even the implemented past similar terroristic attacks, taking into account, where available, how many times a similar agent/weapon was used in the past.

C3. *Organizational skill and infrastructure knowledge of the terrorists* - The final parameter focuses the attention on the terrorist organizational skill and technical infrastructure knowledge in terms of service infrastructures and functions (as heating, ventilation, and air conditioning - HVAC-, water distribution pipe, electrical network, ICT network, fire alarm systems,...). In this case too, the evaluation of the parameters must consider even the implemented past similar terroristic scenarios, taking into account, where available, the organization applied and how many times the threat was realized in such a way.

In Appendix are proposed by the authors possible reference Rating Tables for evaluating all the *eleven* parameters above introduced. Every parameter is evaluated with a score based on 7-levels, in a semi-quantitative approach [10, 17, 18], denoting with the value 1 the less critical situation in the evaluation and with the value 7 the most critical one. Where the evaluation is related to numbers and range of numbers, a logarithm-based intervals for the different levels of the scale is proposed. Advantages of scales based on logarithm intervals are discussed in the study [10]. The list of parameters proposed and analyzed in this work must be considered 'open and flexible'. This means that is possible for the Assessment Team integrate and modify the numbers and the definition of the parameters, avoiding to use some of them if considered 'not of interest' or 'not applicable'.

2.4 Step 4 – Evaluation and rank of the general attractiveness index

The evaluation of the parameters of Category A and B discussed in Step 3 is conducted within the Assessment Team in the Step 4. For each parameter a single score is assigned by the Team, using the tables proposed in Appendix of this work for the two components, *Asset* and *Vulnerability Attractiveness*.

The parameters are processed by the Team in order, one by one, for category, separately, to obtain the assessed values of the two sub-indexes:

- Asset Attractiveness Att_A;
- Vulnerability Attractiveness Att_V.

In this paper, the authors propose as first possible fast approach for the evaluation of these last two values to simply add the single scores obtained for the parameters of the same Category of Step 3. In such a way, the two sub-indexes are defined as follows:

$$Att_{\text{A}} = \sum_{i=1}^{5} ai \qquad (2)$$

$$Att_{\text{V}} = \sum_{i=1}^{3} bi \qquad (3)$$

where, the variables a_i and b_i represent the different parameter scores in the two different categories.

Recalling relation (1), the general Attractiveness *Att* value can be easily evaluated adding the two sub-indexes of the Attractiveness for Asset and for Vulnerability, calculated by relations (2) and (3).

To understand the application of the method here described and generate a rank of sites for the attractiveness, in Table 2 and 3 is shown an example of the application of the procedure described in Step 4 to evaluate relations (2) and (3). The analysis is focused on the evaluation of three different Case Studies, *a commercial centre*, *a government building* and *a hospital*, above characterized in a certain detail. The analysis, as already specified, is in this stage of the method *threat-independent*.

Table 2. Example of application of Step 4 for evaluating the Category A parameters for asset attractiveness

Asset Attractiveness (Att_A)		**Commercial Center**	**Government building**	**Hospital**
Parameters	*var.*	*Score*	*Score*	*Score*
A1–Site population	a_1	5	6	4
A2- Surrounding population	a_2	5	4	3
A3-Building relevance	a_3	2	7	4
A4-Importance of the occupants	a_4	2	7	2
A5-Economic value	a_5	5	7	6
Total Score (Att_A sub-index)		**19**	**31**	**19**

Table 3. Example of application of Step 4 for evaluating the Category B parameters for vulnerability attractiveness

Vulnerability Attractiveness (Att_V)		**Commercial Center**	**Government building**	**Hospital**
Parameters	*var.*	*Score*	*Score*	*Score*
B1-External vulnerability	b_1	7	1	5
B2-Entry vulnerability	b_2	6	1	5
B3-Internal vulnerability	b_3	6	2	4
Total Score (Att_V sub-index)		**19**	**4**	**14**

Starting from the Asset and Vulnerability Attractiveness sub-indexes evaluated, applying relation (1) for the general Attractiveness *Att* index, we obtain for this example the results reported in Table 4.

Table 4. Evaluation of general Attractiveness *Att* index for the example

Attractiveness indexes	**Commercial Center**	**Government building**	**Hospital**
Asset Attractiveness (Att_A)	19	31	19
Vulnerability Attractiveness (Att_V)	19	4	14
General Attractiveness (*Att* index)	**38**	**35**	**33**

From the Table 4 numerical results is possible to generate a rank for the sites, as shows in Table 5.

Table 5. Example of rank for the site general Attractiveness

Rank	**Sites**	***Att* index**
1	**Commercial Center**	38
2	**Government building**	35
3	**Hospital**	33

The results of Table 5 rank show as, considering the main characteristics of the three different sites evaluated by the eight values of the parameters proposed in the example, the Commercial Center can be assessed, from a terrorist viewpoint, as the potential more attractive target among the analyzed sites. This final result here discussed is coherent with last decade statistical analyses for terrorist attacks [3, 4]. These last statistical results confirm the evidence that 'soft targets' are in practical cases preferred by the terrorists, typically for the reduced measures implemented in the structure to mitigate the risk of an attack.

2.5 Step 5 – Evaluation of the terrorist capability index

Similarly to Step 4, the evaluation of the Category C parameters discussed in Step 3 is conducted within the Assessment Team. For each parameter, a single score is assigned by the Team, using the table proposed in Appendix for the evaluation of the terrorist capability parameters, to obtain the final values of the *Terrorist Capability* index.

As for Step 4, the authors propose, as first possible fast approach for the evaluation of this last value, to simply *add* the single scores obtained for the parameters of the Category C of

Step 3. In such a way the Terrorist Capability Ter_C index is defined as follow:

$$Ter_C = \sum_{i=1}^{3} ci \tag{4}$$

As discussed in Step 3, the parameters herein introduced are evaluated *independently of the site/building characteristics*, and describe the general *skill* and *capability* supposed for the terrorists.

The analysis, in this work, is focused on the evaluation of only three different specific threats extracted from Table 1. The selected threats, already indicated in section 2.2, are: the explosion of a van-bomb; the explosion of a suicide belt-bomb; the explosion of a Cesium-137 Dirty Bomb.

In Table 6 is reported the application of the method proposed for evaluating the Terrorist Capability to the three selected threats. The specific values have to be indicated taking into account intelligence available information on the Terrorist groups existing, their capabilities to access to agents/materials, the possible expertise on weapons and the skill in organize and manage the attack.

The results of Table 7 show as, considering the main public characteristics of terrorist organizations known by Italian intelligence [19] and the selected threats, the *suicide belt bomb* appears the general threat easily applicable for the aggressors, followed by the *van-bomb* and, last in the rank, the *dirty bomb*.

From the Table 6 numerical results is possible to generate a *rank for the threats* (*primary threat selection*), as shows in Table 7.

Table 6. Example of application of the method proposed for evaluating the terrorist capability

Terrorist capability ($Terc$)		*Analyzed Threats*		
Parameters	*var.*	*Van bomb*	*Suicide belt bomb*	*Cesium 137 Dirty Bomb*
C1-Access to agents	c_1	4	5	3
C2- Expertise on weapons	c_2	5	6	4
C3 - Organizational skill / infrastructure knowledge	c_3	7	7	4
Total Score (Ter_C)	-	**16**	**18**	**11**

Table 7. Example rank for the analyzed threats

Rank	Threats	Ter_C index
1	**Suicide belt bomb**	18
2	**Van Bomb**	16
3	**Cesium 137 Dirty Bomb**	11

2.6 Step 6 – Evaluation of the Threat Probability Level

The last step of the method here proposed consists in the evaluation, for each site/building ordered in the rank generate in the Step 4, of the level of the *probability of any specific threat* of interest. This evaluation is carried out by the Assessment Team taking into account the results obtained in the previous steps for the general Attractiveness and the Terrorist Capability, together with the fundamental evaluations, typically classified, of *intelligence and law-enforcing institutional experts* and of *reliable intelligence information available*. This means that all the threats considered in the analysis, and in particular the selected primary threats in the rank of Step 5, are now further analyzed both for evaluating their applicability in the specific site/building considered (at this stage of the method we finally apply, at the same time, *site and threat dependent analysis*) and for evaluating the law-enforcing perspective and the intelligence viewpoint. At the end of these 'site-threat oriented' and 'intelligence' analyses, the Assessment Team can decide the final Threat Probability Level, using a threat probability scale of 7 levels proposed in Table 8, herein reported.

The Table 8 provides, for each level of the scale, the qualitative and quantitative definitions, other than a description in natural language of the meaning of the level in the scale. The scale proposed is, in some principles, similar to the scale discussed in [4, 5], with important differences.

- a quantitative reference value for any level of the scale is proposed;
- the proposed scale adopts a logarithm approach [10] for the range definition of the levels.

In practice, the Assessment Team approaches the analysis in this step in an ordered mode, starting from the site/building at the *top of the rank* (Step 4) and applying to this target all the *selected primary threats* beginning from the threat in *first position* in the rank (Step 5), up to the *last selected threat* in the rank.

Table 8. Threat probability scale

Level	**Qualitative/ Quantitative** (probability over a given period of time)	**Level description**
7	Very High from 2^0 to 2^{-1} (from 1 to 1/2)	The probability of a threat, weapon, and tactic being used against the site or building is *imminent*. The threat is credible.
6	High from 2^{-1} to 2^{-2} (from 1/2 to 1/4)	The probability of a threat, weapon, and tactic being used against the site or building is *expected*. The threat is credible.
5	Medium High from 2^{-2} to 2^{-3} (from 1/4 to 1/8)	The probability of a threat, weapon, and tactic being used against the site or building is *probable*. The threat is credible.
4	Medium from 2^{-3} to 2^{-4} (from 1/8 to 1/16)	The probability of a threat, weapon, and tactic being used against the site or building is *possible*. The threat is known, but is not verified.
3	Medium Low from 2^{-4} to 2^{-5} (from 1/16 to 1/32)	The probability of a threat, weapon, and tactic being used in the *region* is *probable*. The threat is known, but is not likely.
2	Low from 2^{-5} to 2^{-6} (from 1/32 to 1/64)	The probability of a threat, weapon, and tactic being used in the *region* is *possible*. The threat exists, but is not likely.
1	Very Low < 2^{-6} (< 1/64)	The probability of a threat, weapon, and tactic being used in the *region* or against the site or building is *very negligible*. The threat is non-existent or extremely unlikely.

3. CONCLUSIONS

The essential features of an original Threat Assessment Method for sites and buildings for the case of terrorist attacks with Explosive/CBR agents were described. The proposed method is based on an approach in six Steps and provides a structured guide useful to the Assessment Team in charge to evaluate the terrorist risks in a site/building. The general Attractiveness of a target and the Terrorist Capability indexes were introduced and defined, and practical application examples of the indexes were presented in three Case Studies. Finally, the evaluation of the Threat Probability Level, adopting a scale of 7-levels based on logarithm ranges, was analyzed for possible application in a Risk Assessment Methodology for sites/buildings in the case of terrorist attack.

REFERENCES

[1] US Department of Justice - National Criminal Justice (NCJ) NCJ181200. (1999). Fiscal Year 1999 State Domestic Preparedness Equipment Program, Assessment and Strategy Development Tool Kit.

[2] US Department of Veterans Affairs - Physical Security Assessment for the Department of Veterans Affairs Facilities (2002). Recommendations of the National Institute of Building Sciences Task Group to the Department of Veterans Affairs. https://www.hsdl.org/?view&did=449080.

[3] US Federal Emergency Management Agency (2003). Reference Manual to Mitigate Potential Terrorist Attacks against Buildings, Risk Management Series, FEMA 426. https://www.fema.gov/media-library-data/20130726-1455-20490-6222/fema426.pdf.

[4] US Federal Emergency Management Agency (2005). Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings, Risk Management Series, FEMA 452, p.1-3, p.1-24, p.2-2. https://www.fema.gov/media-library-data/20130726-1524-20490-7395/fema452_01_05.pdf.

[5] US Federal Emergency Management Agency (2011). Reference manual to Mitigate Potential Terrorist Attacks against Buildings, FEMA 426/BIP06, p.1-7/10, p.1-19. https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf.

[6] US Federal Emergency Management Agency (2008). Incremental Protection for Existing Commercial Buildings from Terrorist Attack, FEMA 459. https://www.fema.gov/sites/default/files/2020-08/fema459_complete.pdf.

[7] US Federal Emergency Management Agency (2009). Handbook for Rapid Visual Screening of Buildings to Evaluate Terrorism Risks, FEMA 455. https://www.fema.gov/sites/default/files/2020-08/fema_455_handbook_rapid_visual_screening.pdf.

[8] US Department of Commerce (1998). Critical Infrastructure Assurance Office (DOC CIAO) Vulnerability Assessment Framework 1.1. https://www.hsdl.org/?view&did=2250.

[9] US Department of Defense (DoD) (2002). Minimum Antiterrorism Standards for Buildings, Unified Facilities Criteria (UFC), UFC 4-010-01.

[10] Carbonelli, M. (2019). Terrorist attacks and natural/anthropic disasters: risk analysis methodologies for supporting security decision making actors, Aracne CBRN Series, Rome (Italy).

[11] US Department of Homeland Security (DHS) (2010). Risk Lexicon, Risk Steering Committee, p.11. https://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf.

[12] European Commission staff Working Paper (2010). Risk Assessment and Mapping Guidelines for Disaster Management, Brussels. https://ec.europa.eu/echo/files/about/COMM_PDF_SEC_2010_1626_F_staff_working_document_en.pdf.

[13] International Organization for Standardization (2009). ISO Guide 73 Risk management – Vocabulary, International Organization for Standardization.

[14] Craighead, G. (2009). High-rise security and fire life safety. Butterworth-Heinemann.

[15] Biringer, B.E., Rudolph, V., Matalucci, R.V., Sharon, L., O'Connor, S.L. (2007). Security Risk Assessment and Management: A Professional Practice Guide for Protecting Buildings and Infrastructures. John Wiley & Son Inc.

[16] Dusenberry, D.O. (2010). Handbook for Blast Resistant Design of Buildings. John Wiley & Son Inc.

[17] International Organization for Standardization (2018). ISO 31000 Risk management -- Principles and guidelines.

[18] International Organization for Standardization (2009). ISO 31010 Risk management - Risk assessment techniques.

[19] DIS, Italian Intelligence Service. Relazione annuale sulle politiche per l'Informazione per la Sicurezza (2020). https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2021/02/RELAZIONE-ANNUALE-2020.pdf.

GLOSSARY

CBR = Chemical, Biological, Radiological
CCT = Closed Circuit Television
EU = European Union
HazMat = Hazard Material
HVAC = Heating, Ventilation, and Air Conditioning
ICT = Information and Communication Technology
US = United States

NOMENCLATURE

Att	Attractiveness (dimentionless)
Att_A	Asset Attractivenes (dimentionless)
Att_V	Vulnerability Attractiveness (dimentionless)
Ter_C	Terrorist Capability (dimemtionless)

APPENDIX

Rating tables (A, B, C) for the evaluation of Attractiveness and Terrorist Capability indexes.

Table A1. Site population capacity

Rating Value	Number of people
7	>2430
6	811 to 2430
5	271 to 810
4	91 to 270
3	31-to 90
2	11 to 30
1	0 to 10

Table A2. Surrounding population capacity

Rating Value	Number of people
7	>24300
6	8101 to 24300
5	2701 to 8100
4	901 to 2700
3	301 to 900
2	101 to 300
1	0 to 100

Table A3. Building relevance/symbolic value

Rating Value	Building Relevance
7	Very high
6	High
5	Medium high
4	Medium
3	Medium low
2	Low
1	Very low

Table A4. Political/administrative/socio-cultural importance of the occupants of the building

Rating Value	Importance of the occupants
7	Very high
6	High
5	Medium high
4	Medium
3	Medium low
2	Low
1	Very low

Table A5. Economical value of the building

Rating Value	**Range (Euro)** Revenue per week	Note
7	>24.3M	Very high
6	8.1 M to 24.3M	High
5	2.7 M to 8.1 M	Medium high
4	900 k to 2.7 M	Medium
3	300k to 900k	Medium low
2	100k to 300k	Low
1	1 to 100k	Very low

Table B1. External/perimeter vulnerability of the site

Rating Value	Vulnerability	Example for application
7	Very high	Open Access in the parking external area to all, unprotected air and consumable entry, vehicle parking without any specific policy
6	High	Open access to all, Unprotected Air/Consumable Entry, No Unauthorized Vehicle Parking within the designated minimum distance
5	Medium high	No Unauthorized Vehicle Parking within the designated minimum distance, Controlled Access of Visitors before parking, Unprotected Air/Consumable Entry
4	Medium	No Unauthorized Vehicle Parking within the designated minimum distance, Controlled Access of Visitors and non staff Personnel before parking, Unprotected Air/Consumable Entry
3	Medium low	Controlled parking Access of Visitors and Non-Staff Personnel, No Unauthorized Vehicle Parking within the designated minimum distance, Protected Air/ Consumable Entry
2	Low	Controlled Access of Visitors and Non-Staff Personnel, No Vehicle Parking within the designated minimum distance, Guarded, Protected Air/Consumable Entry
1	Very low	Controlled parking Access by Pass Only, No Vehicle Parking within a designated minimum distance, Fenced, Guarded, Protected Air/Consumable Entry

Table B2. Entry vulnerability of the building

Rating Value	Vulnerability	Example for application
7	Very high	Open Access to all without identification procedure at the building, no control at the entry for receiving/shipping,
6	High	Open access at the building to all, Unprotected Air/Consumable entry
5	Medium high	Controlled Access of Visitors at the building, Unprotected Air/Consumable entry
4	Medium	Controlled Access of Visitors and non staff Personnel at the building, Unprotected Air/Consumable entry
3	Medium low	Protected Air/Consumable Entry, Controlled Access of Visitors and Non-Staff Personnel at the building
2	Low	Controlled Access of Visitors and Non-Staff Personnel at the building, simple badge for personnel access, Controlled shipping area
1	Very low	Controlled Access and identification of Visitors and Non-Staff Personnel at the building, Badge and biometric identification for personnel access, very stringent controlled shipping area

Table B3. Internal vulnerability of the building

Rating Value	Vulnerability	Example for application
7	Very high	No internal security monitoring center operation, absence of specific policies for the protection of critical and essential service
6	High	No internal security monitoring center operation, bland policies for the protection of critical and essential service (energy, ICT, HVAC services),
5	Medium high	Bland internal security monitoring center operation, bland policies for the protection of critical and essential service (energy, ICT, HVAC services),
4	Medium	Internal security monitoring center operation, minimal policies for the protection of critical and essential service
3	Medium low	Diurnal operation of the internal security monitoring center, specific policies for the protection of main critical services
2	Low	Full day operation of the internal security monitoring center, specific policies for the protection of critical services
1	Very low	Full day operation of the internal security monitoring center, specific and update policies for the protection of critical and essential services (, update and adequate business/operation continuity plan applied

Table C1. Access to explosive/CBR agents

Rating Value	Access capability
7	Very high
6	High
5	Medium high
4	Medium
3	Medium low
2	Low
1	Very low

Table C2. Expertise on weapons of the terrorists

Rating Value	Expertise on weapons
7	Very high
6	High
5	Medium high
4	Medium
3	Medium low
2	Low
1	Very low

Table C3. Organizational skill and Infrastructure knowledge of the terrorists

Rating Value	Skill and knowledge
7	Very high
6	High
5	Medium high
4	Medium
3	Medium low
2	Low
1	Very low